T.C.
TRAKYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI
DOKTORA TEZİ

21. YÜZYILDA ULUSLARARASI İLİŞKİLERDE YENİ GÜÇ REKABET SAHASI: SİBER UZAY

TOLGA ERDEM

TEZ DANIŞMANI
PROF. DR. SİBEL TURAN

EDİRNE 2020

T.C.

TRAKYA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

DOĞRULUK BEYANI

Trakya Üniversitesi Sosyal Bilimler Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

20/07/2020

TOLGA ERDEM



Tezin Adı: **21. Yüzyılda Uluslararası İlişkilerde Yeni Güç Rekabet Sahası: Siber Uzay**

Hazırlayan: **Tolga ERDEM**

ÖZET

Siber uzay sahası, 21. yüzyılın en dikkat çeken söylemlerinden biri olarak kabul edilmektedir. Bilimsel bilgi ve teknolojik ilerlemelerle birlikte değişen Uluslararası İlişkiler, hızla genişleyen bu dijital alana dâhil olmaktadır. Geleneksel Uluslararası İlişkilerdeki güç mücadelesi, bu yüzyılın dinamik koşullarından dolayı fiziksel sınırları aşmak zorunda kalmıştır. Sınırları olmayan, tamamıyla yapay ve belirsizlikler dolu bu karmaşık sahadaki aktör fazlalığı, Siber Uluslararası İlişkilerde güç mücadelesini çok daha karmaşık ve zorlu kılmaktadır. Artan siber yeteneklerin yarattığı güvensizlik ortamı, daha saldırgan siber yeteneklerin geliştirilmesine neden olmaktadır. Bundan dolayı siber alanda daima güçlü kalabilmek mümkün olmamaktadır. Aynı zamanda da siber alanın bir aktörün egemenliği altına girebilmesi zorlaşmaktadır. Bu çalışma üç ana bölümden oluşmaktadır ve Siber Uluslararası İlişkiler tüm boyutlarıyla ele alınmıştır. Birinci bölümde Uluslararası İlişkilerdeki teknolojik dönüşüm, kavramsal ve kuramsal çerçeve içerisinde ele alınmıştır. İkinci bölümde siber uzay ile Uluslararası İlişkiler teknik ve hukuki olarak incelenmiştir. Üçüncü bölümde ise 21. yüzyılın öne çıkan Siber Uluslararası İlişkiler örnek olaylarının sonuçlarına ve etki boyutlarına dikkat çekilmiştir.

Anahtar Kelimeler: Uluslararası İlişkiler, Siber Uzay, Siberpolitik, Siber Saldırı, Siber Savaş

Name of Thesis: **New Competition Domain in International Relations in the 21st Century: Cyberspace**

Prepared by: **Tolga ERDEM**

ABSTRACT

Cyberspace domain is considered as one of the most remarkable discourses of the 21st century. International Relations, changing with scientific knowledge and technological advances, is included in this expanding digital field rapidly. The struggle for power in traditional International Relations had to transcend physical boundaries due to the dynamic conditions of this century. Actor diversity in this complex field, which has no boundaries, is completely artificial and full of ambiguities, makes the power struggle in Cyber International Relations much more complex and challenging. The insecurity created by increased cyber abilities causes much more aggressive cyber abilities. Therefore, it is not always possible to remain powerful in the cyberspace. At the same time, it becomes difficult for the cyber domain to come under the domination of one actor. This study consists of three main sections and Cyber International Relations is dealt with in all its dimensions. In the first section, the technological transformation in International Relations is discussed within the conceptual and theoretical framework. In the second part, cyberspace and International Relations are examined technically and legally. In the third section, attention is drawn to the results and impacts of the 21st century prominent Cyber International Relations case studies.

Keywords: International Relations, Cyberspace, Cyberpolitics, Cyber Attack, Cyber War

ÖNSÖZ

Lisansüstü eğitim hayatım boyunca bilgisinden, tecrübesinden ve yol göstericiliğinden çok şey öğrendiğim değerli hocam Prof. Dr. Sibel TURAN'a en içten teşekkürlerimi ve şükranlarımı sunuyorum. Tez İzleme Komitesinin değerli üyeleri Prof. Dr. Burak GÜMÜŞ ve Dr. Öğr. Üyesi Emre KALAY'a samimi yaklaşımları, sağlamış oldukları akademik destek ve yardımlar adına ayrıca teşekkür ediyorum. Son olarak, akademik ve profesyonel anlamda eğitim kültürünü aldığım Trakya Üniversitesi Uluslararası İlişkiler Bölümünün tüm öğretim üyelerine ayrı ayrı teşekkürlerimi iletiyorum.

Temmuz, 2020 / EDİRNE

İÇİNDEKİLER

ÖZET i
ABSTRACT ii
ÖNSÖZ iii
İÇİNDEKİLER iv
TABLOLAR vii
KISALTMALAR ix
1. Giriş 1
1.1. Çalışmanın Analitik Yapısı 3
1.2. Literatür 7
1.3. Yöntem 12

BİRİNCİ BÖLÜM
KAVRAMSAL VE KURAMSAL ÇERÇEVE: ULUSLARARASI İLİŞKİLERDE "TEKNOLOJİK DÖNÜŞÜM"

1. Bilim, Teknoloji ve Uluslararası İlişkiler 15
2. Bilgi ve İletişim Devriminden Küresel Bilgi Çağına 24
2.1. Matbaa 25
2.2. Elektrikli Telgraf 27
2.3. Telefon 32
2.4. Radyo ve Televizyon 36
2.5. Uydu 44
3. Sanayi Devrimleri: Endüstri 1.0'dan Endüstri 4.0'a 50
3.1. Endüstri 1.0 52
3.2. Endüstri 2.0 56
3.3. Endüstri 3.0 60
3.4. Endüstri 4.0 65
4. Kuramsal Yaklaşım 75
4.1. Karmaşık Uluslararası İlişkiler Teorisinin Ortaya Çıkışı: Beşinci Büyük Tartışma 77
4.2. Karmaşıklık Teorisi: Karmaşıklığın Tanımlanması 85
4.3. Karmaşık Uluslararası İlişkiler Teorisi 93

İKİNCİ BÖLÜM
SİBER UZAY VE ULUSLARARASI İLİŞKİLER

1. Uzay Sahası 103
1.1. Dış Uzay Sahası 104
1.2. Siber Uzay Sahası 106
2. Siber Uzaya Dair Temel Kavramlar 114
2.1. İnternet 114
2.2. Siber Tehdit ve Siber Saldırı 121
2.3. Siber Casusluk ve Siber Suç 127
2.4. Siber Terör ve Siber Savaş 133
2.5. Siber Güvenlik 139
3. Siber Uluslararası İlişkiler 145
3.1. Siberpolitik 148
3.2. Dijital Diplomasi / Siber Diplomasi 153
3.3. Siber Güç 159
4. Siber Uzayda Hukukun ve İşbirliğinin Uygulanabilirliği 165
4.1. Uluslararası Hukuk ve Siber Uzay 167
4.1.1. Avrupa Konseyi Siber Suçlar Sözleşmesi (2001) 173
4.1.2. Siber Savaşa Uygulanacak Uluslararası Hukuk Hakkında Tallinn El Kitabı (2013) 176
4.2. Uluslararası İşbirliği ve Siber Uzay 180
4.2.1. Uluslararası Telekomünikasyon Birliği (*The International Telecommunication Union*, ITU) 183
4.2.2. İnternet Tahsisli Sayılar ve İsimler Kurumu (*The International Corporation for Assigned Names and Numbers*, ICANN) 185
4.2.3. İnternet Yönetişim Forumu (*The Internet Governance Forum*, IGF)……...187

ÜÇÜNCÜ BÖLÜM
SİBER ULUSLARARASI İLİŞKİLER ÖRNEK OLAYLARI

1. Kötü Amaçlı Yazılımlar (*Malwares*) 192
1.1. Virüsler (*Viruses*) 194
1.2. Solucanlar (*Worms*) 196
1.3. Truva Atları (*Trojan Horses/Trojans*) 198
1.4. Botlar ve Botnetler (*Bots & Botnets*) 199
1.5. Casus Yazılımları (*Spywares*) 201
2. Siber Olayların Sınıflandırılması 203
2.1. Keşif Saldırıları (*Reconnaissance Attacks*) 205
2.2. Erişim Saldırıları (*Access Attacks*) 206
2.3. Hizmet Engelleme Saldırıları (*Denial of Service Attacks*, DoS) ve Dağıtılmış Hizmet Engelleme Saldırıları (*Distributed Denial of Service Attacks*, DDoS) 208
3. Siber Olaylar Tarihinin Aşamaları 212
3.1. Gerçekleşme Aşaması 214
3.2. Yükseliş Aşaması 217
3.3. Militarizasyon Aşaması 220
4. 21. Yüzyılın Öne Çıkan Siber Uluslararası İlişkiler Örnek Olayları 232
4.1. Titan Rain Operasyonu (2003) 233
4.2. Estonya Saldırıları (2007) 237
4.3. Gürcistan Saldırıları (2008) 243
4.4. Stuxnet Saldırısı (2010) 248
4.5. WikiLeaks (2010) 256
4.6. Snowden (2013) 265
4.7. Ukrayna Saldırıları (2017) 274
SONUÇ 280
KAYNAKÇA 296
Kitaplar / Raporlar: 296
Makaleler / Kitap Bölümleri: 312
İnternet Kaynakları: 355
Belgeseller: 389

TABLOLAR

Tablo-1: Bilim-Teknoloji-Uluslararası İlişkiler Üçgen Modelleme……...22
Tablo-2: Telefon Bağlantıları ve Gerekli Hatlar…….33
Tablo-3: İngiliz Sanayileşmesi Sırasında Ekonomik Büyüme Yönleri……..54
Tablo-4: Sanayi Devrimleri ve Sürücüleri (*Drivers*): İletişim ve Enerji Kaynakları……...64
Tablo-5: Sanayi Devrimlerinin Etkileri……..66
Tablo-6: Siber-Fiziksel Sistemlerde İnsan ve Makine Etkileşim Modellemesi……..68
Tablo-7: Endüstriyel İletişim ve İlgili Teknoloji Alanlarının Gelişimindeki Kilometre Taşları…….71
Tablo-8: Sanayi Devrimlerinin Temel Parametrelerinin Kıyaslanması…….74
Tablo-9: Uluslararası İlişkilerde Büyük Tartışmalar……..82
Tablo-10: Karmaşık Uyarlamalı Sistem Modellemesi……...92
Tablo-11: Karmaşık Uluslararası İlişkiler Fenomeni…….97
Tablo-12: Siber Uzayın Özellikleri……...109
Tablo-13: Siber Uzayın Evrimi…….111
Tablo-14: ARPANET: Aralık 1969 (ÜST) ve Temmuz 1977 (ALT)……..116
Tablo-15: Dünya Bölgelerine Göre İnternet Kullanıcı Miktarları (1990-2015)…...120
Tablo-16: Dünyada Dijital Ortam…….……120
Tablo-17: Aktörlere ve Kritik Altyapılara Yönelik Siber Tehditler…….122
Tablo-18: Güvenlik İhlalleri ve Etkileri……...125
Tablo-19: Altyapı Tehdit Matrisi…….…….126
Tablo-20: Terörizm ile Suç Arasındaki Korelasyon…….……135
Tablo-21: Dinamik Siber Terörizm Çerçevesi…….…….136
Tablo-22: Siber Güvenlik Kapsamındaki Güvenlik Kavramları……..141
Tablo-23: Bilgi ve İletişim Teknolojileri (BİT) Güvenliğini Evrimi……142
Tablo-24: Siberpolitiğin Tezahür Şekli……150
Tablo-25: Siber Alanda Gücün Üç Yüzü…….…….162
Tablo-26: Siber Uzay Operasyonları Spektrumu……..191
Tablo-27: Casus Yazılımların İşleyişi……..201

Tablo-28: Siber Saldırı Diyagramı……203
Tablo-29: Keşif Saldırıları (*Reconnaissance Attacks*)……..205
Tablo-30: DoS Saldırısı……209
Tablo-31: DDoS Saldırıları……...210
Tablo-32: Gerçekleşme Aşamasındaki Siber Olaylar (1980-1998)…..…….216
Tablo-33: Yükseliş Aşamasındaki Siber Olaylar (1998-2003)…….……219
Tablo-34: Militarizasyon Aşamasındaki Siber Olaylar (2003-Günümüz)…….....222
Tablo-35: Siber Saldırıların Motivasyonel Boyutları……...235
Tablo-36: Saldırı Sayıları……..238
Tablo-37: Stuxnet Saldırı Diyagramı……253

KISALTMALAR

A-1	:	Aggregat 1 / Assembly 1
AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
ACA	:	Arms Control Association
ACT	:	Allied Command Transformation
AHCI	:	Arts and Humanities Citation Index
AHİM	:	Avrupa İnsan Hakları Mahkemesi
AMP	:	Advanced Manufacturing Partnership
APT	:	Advanced Persistent Threat
APCERT	:	Asia Pacific Computer Emergency Response Team
ARPA	:	Advanced Research Projects Agency
ARPANET	:	The Advanced Research Projects Agency Network
AR-GE	:	Araştırma ve Geliştirme
AT&T	:	American Telephone and Telegraph
B.B.C.	:	The British Broadcasting Corporation
BİT	:	Bilgi ve İletişim Teknolojileri
BNP	:	British National Party
C&C	:	The Command and Control Servers
CAS	:	Complex Adaptive Systems
CCD-CoE	:	Cooperative Cyber Defence Centre of Excellence
CCSP	:	Cisco Certified Security Professional Certification
CCT	:	Computational Complexity Theory
CERN	:	Conseil Européen pour la Recherche Nucléaire
CIR	:	Complex International Relations Theory
CISPs	:	Commercial Internet Service Providers
CNSA	:	The China National Space Administration
CO2	:	Karbondioksit
COE	:	The Council of Europe
CPPS	:	Cyber-Physical Production Systems

CPS	:	Cyber-Physical Systems
CRT	:	Cathod Ray Tube
CT	:	Complexity Theory
ÇHC	:	Çin Halk Cumhuriyeti
DARPA	:	Defense Advanced Research Projects Agency
DDoS	:	Distributed Denial of Service
DEC	:	Digital Equipment Corporation
DIA	:	U.S. Defense Intelligence Agency
DISA	:	Defense Information Systems Agency
DMS	:	Distribution Management System
DNS	:	Domain Name System
DoD	:	U.S. Department of Defense
DoS	:	Denial of Service
EARN	:	European Academic and Research Network
EMS	:	Energy Management System
ENISA	:	European Union Agency for Network and Information Security
ESA	:	European Space Agency
EUNet	:	European UNIX Network
FCC	:	The Federal Communications Commission
FoR	:	Factories of the Future
GCA	:	The ITU Global Cybersecurity Agenda
GPS	:	Global Positioning System
GSYİH	:	Gayri Safi Yurtiçi Hasıla
HF	:	High Frequency
HTML	:	Hypertext Markup Language
HTTP	:	Hypertext Transfer Protocol
IAEA	:	International Atomic Energy Agency
IANA	:	Internet Assigned Numbers Authority
IC	:	Integrated Circuits
ICANN	:	Internet Corporation for Assigned Names and Numbers

IC-CNCI	:	Intelligence Community Comprehensive National Cyber-security Initiative
ICRC	:	The International Committe of the Red Cross
IGF	:	The United Nations Internet Governance Forum
IGY	:	International Geophysical Year
IIC	:	Industrial Internet Consortium
IIoT	:	Industrial Internet of Things
INTELSAT	:	International Telecommunications Satellite Consortium
IoT	:	Internet of Things
IP	:	Internet Protocol
IS	:	Internet Society
ISC	:	Industrial Control Systems
ISOC	:	Internet Society
ISRO	:	Indian Space Research Organisation
ITU	:	International Telecommunication Union
ITU-D	:	The Telecommunication Development Sector
ITU-R	:	The Radiocommunication Sector
ITU-T	:	The Telecommunication Standardization Sector
İTÜBİDB	:	İTÜ Bilgi İşlem Daire Başkanlığı
JAXA	:	The Japan Aerospace Exploration Agency
KM	:	Kilometre
LANs	:	Local Area Networks
LF	:	Low Frequency
MAP	:	Membership Action Plan
MF	:	Medium Frequency
MIT	:	Massachusetts Institute of Technology
MILNET	:	Military Network
MMS	:	Multimedia Messaging Service
MNC	:	Multinational Corporations
MoD	:	British Ministry of Defense
MOOC	:	Massive Open Online Courses
MOSSAD	:	İsrail İstihbarat ve Özel Operasyonlar Enstitüsü

M.Ö.	:	Milattan Önce
M.S.	:	Milattan Sonra
NASA	:	The National Aeronautics and Space Administration
NATO	:	The North Atlantic Treaty Organization
NCCIC	:	National Cybersecurity & Communications Integration Center
NCSC	:	National Cyber Security Centre
NGO	:	Non-Govermental Organization
NJE	:	Network Job Entry
NMT	:	The Nordic Mobile Telephone
NORSAR	:	Norwegian Seismic Array
NPT	:	Nuclear Non-Proliferation Treaty
NSA	:	The National Security Agency
NSF	:	The US National Science Foundation
NSFNET	:	National Science Foundation Network
OECD	:	Ekonomik Kalkınma ve İşbirliği Örgütü
OS	:	Operating Systems
OST	:	The Outer Space Treaty
PLCs	:	Programmable Logic Controllers
PTT	:	Posta, Telgraf ve Telefon İdareleri
R&D	:	Research and Development
RF	:	Rusya Federasyonu
ROSCOSMOS	:	The Roscosmos State Corporation for Space Activities
SCADA	:	Supervisory Control and Data Acquisition
SCI	:	Science Citation Index
SCIE	:	Science Citation Index Expanded
SMS	:	Short Message Service
SNL	:	Sandia National Laboratory
SPACEX	:	Space Exploration Technologies Corporation
SSCB	:	Sovyet Sosyalist Cumhuriyetler Birliği
SSCI	:	Social Sciences Citation Index
STK	:	Sivil Toplum Kuruluşu

TCP	:	Transmission Control Protocol
TDK	:	Türk Dil Kurumu
TIR	:	The Third Industrial Revolution
UAD	:	Uluslararası Adalet Divanı
UK-GCHQ	:	UK Government Communications Headquarters
UN-COPUOS	:	UN Committee on the Peaceful Uses of Outer Space
UN-GA	:	United Nations General Assembly
UN-SC	:	United Nations Security Council
USAISEC	:	U.S. Army Information Systems Engineering Command
USB	:	Universal Serial Bus
USCYBERCOM	:	The United States Cyber Command
USNA	:	The United States Naval Academy
USOM	:	Ulusal Siber Olaylara Müdahale Merkezi
UUCP	:	The UNIX to UNIX Copy Protocol
V-2	:	Vergeltungswaffe-2
VB.	:	Ve Benzer
VHF	:	Very High Frequency
VLF	:	Very Low Frequency
VLSI	:	Very Large-Scale Integration
VS.	:	Vesaire
WEB (WWW)	:	World Wide Web
WEF	:	World Economic Forum
WSIS	:	The World Summit on the Information Society

21. YÜZYILDA ULUSLARARASI İLİŞKİLERDE YENİ GÜÇ REKABET SAHASI: SİBER UZAY

1. Giriş

Tarih boyunca "güç" kavramı, hem Sosyal Bilimlerde hem de Doğa Bilimlerinde son derece önemli kabul edilmekle beraber bu doğrultuda çok sayıda ve farklı perspektiflerde bilimsel çalışmaların gerçekleştirilmesine vesile olmuştur. Uluslararası İlişkiler disiplini içerisindeki tartışmalara bakıldığında ise odak noktasını yine güce yönelik sorgulamaların oluşturduğu yaygın olarak görülmektedir. Bu kadar yoğun ilgiye rağmen güç kavramının spesifik tanımı, özellikleri ve alanları hususundaki akademik tartışmalarda ortak bir paydanın oluşturulamaması, söz konusu kavrama ait karmaşıklığı ve belirsizliği derinleştirmekle birlikte bu doğrultuda yapılan çalışmaların zenginleşmesini de sağlamaktadır.

20. yüzyıl içerisinde disipline olan Uluslararası İlişkiler alanı, bu dönem içerisinde iki büyük dünya savaşı geçirmiş ve bu savaşların ulusal, uluslararası ve insani boyutlardaki katastrofik neden ve sonuçlarını analiz etmeye, anlamlandırmaya ve buna bağlı olarak da kısa-orta-uzun vadeli öngörülerde bulunmaya çalışmıştır. Milyonlarca insanın hayatına mal olan ve tahayyül edilmesi oldukça zor çok sayıda dramı beraberinde getiren bu iki büyük savaşın ardından oluşan konjonktürde "soğuk" olarak nitelendirilen bir başka savaş hali daha gerçekleşmiştir. "Soğuk" sıfatıyla; iki büyük savaşın yaşandığı Uluslararası İlişkiler periyoduna kıyasla nispeten gerilimin daha az olduğu, anlaşmazlık ya da çatışma hallerinin doğrudan ve kapsayıcı savaşlara evrilmediği kastedilmiş olsa da yine söz konusu dönem içerisinde ortaya çıkan "dehşet dengesi" ile dünyanın önceki iki büyük savaş dönemine kıyasla çok daha kapsayıcı, daha büyük kayıplara ve yıkımlara neden olabilecek nükleer savaş tehlikesine son derece yakın olduğu görülmüştür. 20. yüzyılın sonlarına doğru Sovyet Sosyalist Cumhuriyetler Birliği'nin (SSCB) dağılmasıyla birlikte o döneme kadar "iki kutuplu" olarak addedilen Uluslararası İlişkilerde önemli bir kırılma noktası yaşanmış ve kutuplardan biri ortadan kalkarak "tek kutupluluk" ortaya çıkmıştır. 21. yüzyılın başlangıcıyla beraber yaşanan "11 Eylül (9/11) Terör Saldırıları" neticesinde Amerika Birleşik Devletleri (ABD) tarafından geliştirilen

asimetrik tehdit olarak "küresel terörizm" kavramı ve bu bağlamda ABD'nin gerçekleştirmiş olduğu saldırgan tutumun yanı sıra yine bu yüzyıl içerisinde Çin Halk Cumhuriyeti (ÇHC), Avrupa Birliği (AB), Japonya ve Rusya Federasyonu (RF) gibi diğer uluslararası aktörlerin çeşitli güç sahalarında göstermiş olduğu ilerleme ve gelişmeler doğrultusunda "tek kutupluluk" sorgulanır olmuştur. Bunun yerine "çok kutupluluk" ya da "kutupsuzluk" şeklinde yeni tartışmalar akademik çevreler içerisinde ön plana çıkmıştır.

Yukarıda kısaca bahsedilen 20. ve 21. yüzyıl Uluslararası İlişkiler gelişmeleri dikkate alındığında; yaşanan tüm gerilimlerin, savaşların, çatışmaların, yıkımların ve geri adımların özünde "güç" kavramıyla ilişkilendirilebilecek temel faktörlerin olduğu ileri sürülebilmektedir. Çıkar çatışmalarına bağlı olarak geliştirilen "güç dengesi" ya da "güç maksimizasyonu" hamleleri, oluşan "güvenlik ikilemi" veya "dehşet dengesi" söylemleri ve literatürde kullanılan "büyük güç", "süper güç", "hegemon güç" gibi ifadelerin yoğunluğu da yukarıda ileri sürülen savı destekler niteliktedir. Dolayısıyla farklı perspektif ve bağlamları içerisinde barındıran, odak unsuru olarak "güç" üzerinden rekabeti ve mücadeleyi ön plana çıkaran geniş kapsamlı bir Uluslararası İlişkiler sahasından söz etmek mümkündür. Diğer taraftan bu yüzyıllardaki güç rekabetine yönelik öne çıkan güç sahalarının çoğunlukla askeri, ekonomik ve siyasi alanlarda olduğu görülmektedir; ancak Uluslararası İlişkiler disiplininin dinamik karakteristiği göz önüne alındığında; hem güce dair kavramsallaştırmaların hem de güç rekabet sahalarının sürekli ve çok boyutlu olarak geliştiği, değiştiği ve hatta dönüştüğü söylenebilmektedir. İşte bu noktada 20. yüzyılın ortalarından itibaren ön plana çıkmaya başlayan ve özellikle 21. yüzyılda büyük bir ivme kazanan yeni teknolojilerin geliştirilmesi çalışmaları, Uluslararası İlişkilerdeki dinamik dönüşümü ve oluşan bu yeni Uluslararası İlişkiler çevresi içerisindeki gücün yeniden tanımlanması ve dağıtılmasını, yaratılan yeni sahalar doğrultusunda doğrudan etkilemiştir. Uluslararası İlişkiler içerisindeki bu "teknolojik dönüşüm" rüzgârının güçlü etkisiyle Uluslararası İlişkiler aktörlerinin ilgisini çekmeye ve hâkimiyet mücadelesi vermeye başladığı yepyeni bir güç rekabet sahası ortaya çıkmıştır: Uzay.

Askeri güç sahası kapsamında üstünlük gayesiyle 20. yüzyıl ortalarından itibaren ABD ve SSCB kutupları arasında rekabete dönüşen uzay çalışmaları, aynı

yüzyılın sonlarına doğru artan çok yönlü teknolojik gelişmelere bağlı olarak bilgisayar sistemlerini birbirine bağlayan İnternet ağını geliştirmiş ve söz konusu ağ, dünyayı ve dolayısıyla uluslararası sistemi tümüyle kapsayacak şekilde hızla genişletilmiştir. 21. yüzyılın başlangıcıyla birlikte ise uluslararası sistemin askeri, ekonomik ve siyasi güç sahalarının enformasyon altyapılarının büyük çoğunluğu dünyayı tamamen saran bu teknolojik ağa bağımlı hale gelmiştir. Öte taraftan, uzay çalışmalarına bağlı olarak gelişen, devinim kazanan ve çeşitlenen yeni teknolojiler sayesinde uzay alanı, kendi içerisinde etkileşim halinde iki farklı alt alan oluşturmuştur: "Siber Uzay" ve "Dış Uzay". Birbiri ile benzer ve farklı özelliklere sahip bu iki boyut arasında doğrudan ve sürekli bir etkileşim hali söz konusudur. Günümüz Uluslararası İlişkiler aktörlerinin çeşitli güç sahalarındaki altyapılarının ve üstyapılarının siber uzay ve dış uzay alanlarına çeşitli şekillerde eklemlenmesi, aktörlerin güvenlik endişelerine farklı boyutlar katmaktadır. Buna ek olarak; hem siber uzayın hem de dış uzayın sınırlarının olmaması hali, uluslararası aktörlerin artan güvenlik endişelerini söz konusu bu yeni alanlarda güç rekabetine girerek giderme ihtiyaçlarını da beraberinde getirmektedir.

Bu çalışmanın konusunu; 20. yüzyılın ortalarında başlayan uzay çalışmalarına yönelik teknolojik gelişmeler neticesinde 21. yüzyıl Uluslararası İlişkilerinde yeni güç rekabet sahası olarak ortaya çıkan siber uzayın, çalışmanın analitik yapısı bölümünde ortaya konulan sorular ve hipotezler doğrultusunda çözümlenmesi oluşturmaktadır. Yazarın bu konuya ilgisi lisansüstü eğitim sürecinde almış olduğu dersler doğrultusunda yapmış olduğu araştırmalar ve güncel Uluslararası İlişkiler gelişmelerine yönelik gözlemlerine bağlı olarak şekillenmeye başlamıştır.

1.1. Çalışmanın Analitik Yapısı

Uzay alanı –siber uzay ve dış uzay– evrensel ortak varlıklar (*global commons*) kapsamında ele alınmaktadır. Bunun nedeni olarak ise enformasyon, iletişim ve bilgisayar teknolojileri alanlarındaki hızlı ve derin gelişmelerin, devletlerin ulusal güvenliklerinden insanların gündelik yaşamlarına kadar her alandaki doğrudan etkilerinin geleneksel coğrafi temelli yaklaşımlardan oldukça farklı olması gösterilmektedir. Bu çalışma, uzay sahalarından "siber uzay" üzerine

odaklanmakta ancak gerekli görülen kısımlarda "dış uzay" ile ilgilenmekte ve "siber uzay" alanını, 21. yüzyıl Uluslararası İlişkilerinde yeni bir güç rekabet sahası olarak ortaya koymayı amaçlamaktadır. Bunun gerçekleştirebilmesi için öncelikli olarak bilim ve teknolojinin bilgisi sorgulanmalı ve yapılan araştırmalarda elde edilen veriler doğrultusunda Uluslararası İlişkiler alanı ile olan etkileşiminin güç ve güvenlik anlayışı üzerinden derinlemesine çözümlenmesi gerekli görülmektedir. Ardından bilgi, iletişim ve endüstriyel anlamdaki devrimsel gelişmelerin analizi yapılıp, kuramsal çözümlemeyle pekiştirilmesi ve nihayetinde de genel uzay kavramından siber uzay ayrımı yapılarak modern Uluslararası İlişkiler anlayışındaki pozisyonunun yeni bir güç rekabet sahası olarak detaylı olarak tartışılması istenmektedir. İşte bu çerçevede şu araştırma soruları irdelenecektir: Bilim, Teknoloji ve Uluslararası İlişkilerin güç anlayışı nasıldır ve bu anlayış üzerinden birbirlerini nasıl etkilemektedirler? Bilgi ve İletişim Devrimi nasıl gerçekleşmiştir, önemli aşamaları nelerdir? Endüstri Devrimlerinin bilimsel ve teknolojik gelişmeler ile bağı nasıl yorumlanmalıdır? Uluslararası aktörler modern Uluslararası İlişkilerde hangi güç alanlarında rekabet etmektedirler? 21. yüzyıl Uluslararası İlişkilerinde güç rekabet sahalarında değişim ya da dönüşüm söz konusu mudur? Eğer söz konusuysa ne şekilde gerçekleşmektedir? Modern Uluslararası İlişkilerdeki aktörler ve sistemler açısından siber uzay ne ifade etmektedir ve kuramsal bir yaklaşım söz konusu mudur? Siber uzay sahasının uluslararası hukuki boyutu nasıldır? Siber uzayda güçlü olmak, modern Uluslararası İlişkiler aktörlerinin güvenlik algılarını nasıl etkilemektedir? Bu bağlamda verilebilecek örnek olaylar nelerdir, küresel ve bölgesel etkileri nasıl olmuştur?

Bu soruların incelenmesiyle amaçlanan şey; 21. yüzyıl Uluslararası İlişkiler disiplininde uzayın gerçekten de klasik Uluslararası İlişkiler güç rekabet sahalarına –askeri, ekonomik ve siyasi– alternatif olup olamayacağının siber uzay boyutundan incelenerek anlaşılabilmesi hususunda fikir verebilmektir; ancak uzayın alt alanları olan siber uzay ile dış uzayın arasındaki etkileşimin yoğun olduğunu ve bu iki alan arasında keskin bir ayrım yapılmasının oldukça zor olduğunu belirtmekte fayda vardır. Öyle ki söz konusu etkileşim, iki alan arasındaki karşılıklı bağımlılık (*interdependence*) ve karşılıklı bağıntılılık (*interconnectedness*) halini gün geçtikçe giderek artırmaktadır. Örneğin; uydular ve baz istasyonları gibi dış uzay sistemi

bileşenleri, siber uzayın birer dahili parçaları haline gelirken, her gün çok büyük miktarlarda veriler uydular tarafından üretilip iletilmektedir. Bu eğilimin öneminin ülkeler tarafından kabul görmesiyle uydu tasarım ve geliştirme çalışmaları istikrarlı şekilde gelişmekte ve netice olarak da dış uzaydaki yörünge yuvaları ve sınırlı sayıdaki iletim frekansına erişim için aktörler arası rekabet giderek artmaktadır. Siber uzay ile dış uzay arasında artan bu bağımlılık hali, özellikle de dış uzay varlıklarının çoğunluğunun siber ağlara bağımlı hale gelmesiyle birlikte uluslararası aktörler açısından yeni güvenlik açıklarını da beraberinde getirmektedir. Özellikle 21. yüzyılda üretilen uyduların daha eski dönemki uydulara kıyasla uzaktan yeniden yapılandırılabilir ve yükseltilebilir özellikte olan yerleşik bilgisayarlarla donatılmış olması, onları siber saldırılara açık hale getirmektedir. Dolayısıyla bu durum özellikle devletlerin düşük izlenilebilirlikteki ulusal altyapılarını etkileyebilecek son derece tehlikeli bir araca dönüşebilmektedir.

Bu çalışmanın amacı; evrensel ortak varlıklardan kabul edilen uzayın, özellikle siber uzay bağlamında yeni bir güç rekabet sahası olup olmadığını göstermekle sınırlı değildir. Buna ek olarak, bu alanın görece büyüklüğünün de hesaba katılarak uluslararası güvenlik perspektifinden algılanışını ortaya koyabilmek ve uluslararası hukuk bağlamında bu alanın uluslararası aktörlerce kullanımının hangi şartlar doğrultusunda taahhüt altına alındığı hususlarının analizi de çalışmanın amacı kapsamındadır. Bundan dolayı Uluslararası İlişkilerde siber uzaya dair yapılan uluslararası mutabakatlar, anlaşmalar, sözleşmeler, bildiri ve ilke tanzimleri çalışmanın içerisindeki konulara ait alt başlıklarında detaylı olarak ele alınacaktır. Diğer taraftan çalışmanın muhteviyatı, uzay sahasının siber uzay alt alanını güç perspektifi bağlamında sınırlandırmıştır. Zaman sınırlaması olarak ise 21. yüzyıl ön plana çıkarılmakla beraber bu yüzyıldaki gelişmelerin daha iyi idrak edilebilmesi ve herhangi bir soru işaretine mahal vermemek adına 20. yüzyıl ortalarındaki siber uzay çalışmalarına yönelik gerçekleştirilen teknolojik yeniliklerin başlangıcı da kapsama dâhil edilmiştir. Böylelikle enformasyon, iletişim ve bilgisayar teknolojileri alanlarındaki gelişmelerin siber uzay sahasını nasıl oluşturduğu ve bu sahanın uluslararası aktörlerin askeri, ekonomik ve siyasi güç alanlarına etkileri ve bu etkilere bağlı olarak güvenlik algılarının nasıl değiştiği gözlemlenebilecektir.

Bu çalışmada, uzaya dair yukarıda da kısaca sunulan teknolojik gelişmeler ışığında, siber uzayın Uluslararası İlişkilerin güç rekabet sahalarından biri olarak kabul edilip edilemeyeceği sorusu araştırılacaktır. Bu soruyla bağlantılı olarak çalışmanın hipotezi şu şekilde oluşturulmuştur: "Soğuk Savaş dönemi Uluslararası İlişkilerinde ortaya çıkan uzay çalışmaları rekabeti ve geliştirilen yeni teknolojiler, 21. yüzyıl Uluslararası İlişkiler bilgisinde 'teknolojik dönüşüm' yaratarak siber uzayı Uluslararası İlişkilerin karmaşık çerçevesi içerisinde yeni güç rekabet sahalarından biri haline getirmiştir." Küresel ilişkilerin her geçen gün siber uzay sahasına eklemlenmesi ve siber faaliyetlerin küresel ilişkilerdeki etkilerinin ve belirleyiciliklerinin giderek derinleşmesinden dolayı; kavramsal, kuramsal ve teknik boyutlara ek olarak uluslararası hukuk ve güncel örnek olay analizleri açısından irdelenmesinin söz konusu hipotezin çok boyutlu olarak test edilebilmesine imkân sağlayacağı düşünülmektedir.

Söz konusu hipotezin ve araştırma sorularının ele alınmasının Siyaset Bilimi ve Uluslararası İlişkiler açısından önemi; askeri güç maksimizasyonu gayesiyle başlatılan uzay teknolojileri çalışmalarının, sürekli olarak değişen ve gelişen dinamik ve karmaşık Uluslararası İlişkilerin içerisinde güç odaklı olarak değişiminin ve konumlanışının ele alınmasıdır. Siber uzay sahasını Uluslararası İlişkiler kapsamında güç rekabet sahası olarak ele alan çalışmaların çok fazla olmaması, söz konusu alana yönelik Uluslararası İlişkiler ilgisinin oldukça yeni olması ve bu konuyla ilgili Türkçe literatürün azlığı da hesaba katıldığında bu çalışmanın söz konusu boşlukların doldurulmasına bir parça da olsa katkı sağlayacağı düşünülmektedir.

Bu çalışmada ortaya konan hipotezin çözümlenmesi için aşağıda açıklanan yol haritası incelenecektir:

Birinci bölümde sorunsalın derinlemesine kavramsal ve kuramsal analizi yapılacaktır. Bu doğrultuda öncelikle leksikografik olarak bilim ve teknoloji sorgulanacak, bu iki alanın Uluslararası İlişkiler alanı ile olan etkileşimi analiz edilecektir. Ardından bilginin ve iletişimin küresel bağlamda gelişimine yönelik devrimsel süreçler önemli aşamalarıyla ele alınacaktır. Söz konusu gelişmelerin üretim ve ihtiyaçlar açısından yarattığı endüstriyel devrimlerin küresel boyutu detaylandırılacak ve nihayetinde Uluslararası İlişkiler disiplininin bütün bu gelişmelere yönelik geliştirdiği yeni kuramsal yaklaşım, "Beşinci Büyük Tartışma"

bağlamında da sunulan Karmaşık Uluslararası İlişkiler Teorisine giden süreç "Sosyal Bilimlerde Teknolojik Dönüşüm" temelinde ele alınacaktır.

İkinci bölümde ise birinci bölümde sunulan kavramsal ve kuramsal çerçeve ile bağlantılı olacak şekilde geliştirilecek teknik bir analiz ile çalışma pekiştirilecektir. Bu bağlamda çalışmanın ana unsuru olan siber uzay sahası, genel uzay tanımlamasından ayrılarak mevcut tüm teknik boyutları ve kavramlarıyla birlikte açıklanmaya çalışılacaktır. Özellikle Uluslararası İlişkiler disiplini içerisinde son dönemde kullanımı giderek artan "siber saldırı", "siber güç" ya da "siber terör" gibi pek çok ifade türü detaylandırılacaktır. Ek olarak ise siber uzay sahasına yönelik uluslararası hukuk kapsamında yapılmış ve yapılması planlanan her türlü düzenleme, hukuki perspektiften aktarılacaktır. Dahası, uluslararası işbirliğinin siber alanda uygulanabilirliği, öne çıkan organizasyon ve girişimler üzerinden analiz edilecektir.

Üçüncü bölümde ise çalışmanın birinci ve ikinci bölümlerinde sunulan kavramsal, kuramsal, teknik ve hukuki yaklaşımların örnek olay analizleri üzerinde bütünleşmesi sağlanacaktır. Çalışmanın zaman sınırlaması her ne kadar 21. yüzyıl olsa da, 20. yüzyıl ortalarından itibaren siber uzay sahasının alt yapısını inşa eden yaşanmış küresel örnek olaylardan tarihsel arka plan oluşturularak 21. yüzyıl küresel ilişkilerini derinden etkileyen örnek olaylar detaylı olarak ele alınacaktır. Böylelikle Siber Uluslararası İlişkilerin uluslararası güç rekabetine etkisi çok yönlü olarak gözlemlenebilecektir.

Son bölümde ise çalışmanın Giriş bölümünde ortaya atılan hipotezin ve araştırma sorularının çözümlenmesi sonucunda elde edilen neticeler, konu bütünlüğü içerisinde tekrar ele alınarak çalışmanın hipotezini sağlayıp sağlamadığının analizi yapılacak ve genel bir değerlendirme ile çalışma sonlandırılacaktır.

1.2. Literatür

Bu çalışmanın planlaması toplamda beş bölüm üzerine yapılmıştır. Giriş ve Sonuç bölümleri hariç tutulduğunda üç ana bölüm bulunmaktadır. Dolayısıyla literatürün üç bölüm esasına göre ele alınması yerinde olacaktır. Birinci bölümün başlığı "Kavramsal ve Kuramsal Çerçeve: Uluslararası İlişkilerde 'Teknolojik Dönüşüm'" olarak belirlenmiştir. Bu bölümde bilim ve teknoloji üzerine araştırmalar

ve tanımlamalar yapılacak, ardından da bu alanların Uluslararası İlişkiler alanı üzerine olan etkileri incelenecektir. Ardından Bilgi ve İletişim Devrimi ile Sanayi Devrimleri ele alınacak ve nihayetinde de Karmaşıklık Teorisi ve Karmaşık Uluslararası İlişkiler Teorisi ile kuramsal perspektif sunulacaktır. Bu doğrultuda literatüre bakıldığında, çok disiplinli ve çapraz disiplinli yaklaşımlar içeren bilimsel çalışmaların gerçekleştirildiği görülmektedir. Uluslararası İlişkiler alanında teknolojik dönüşüm vurgusu yapan konulara dair Türkçe yazında fazla çalışma olmamakla birlikte yeni yeni gelişmeler yaşanmakta ancak yazının merkezini İngilizce kaynaklar oluşturmaktadır. Bilim, Teknoloji ve Uluslararası İlişkiler alanlarının karşılıklı etkileşimleri üzerine öne çıkan başlıca isim, Georgetown Üniversitesi Bilim, Teknoloji ve Uluslararası İlişkiler kürsüsünden emekli Prof. Dr. Charless Weiss olmuştur. Weiss'in "*Science, Technology and International Relations*"[1] ile "*How Do Science and Technology Affect International Affairs?*"[2] başlıklı çalışmaları, bilim ve teknoloji araştırmaları yapmakta ve Uluslararası İlişkiler-Bilim-Teknoloji arasında üçlü ve işteş bir etkileşim hali olduğunu savunmaktadır. Öte taraftan Massachusetts Teknoloji Enstitüsü (*Massachusetts Institute of Technology*, MIT) Siyaset Bilimi bölümü profesörü Eugene B. Skolnikoff "*The Elusive Transformation: Science, Technology, and the Evolution of International Relations*"[3] isimli çalışmasıyla Uluslararası İlişkiler içerisinde yaşanan teknolojik dönüşümü derinlemesine ele almaktadır. Diğer taraftan Connecticut Üniversitesi Siyaset Bilimi kürsüsünden Prof. Dr. Elizabeth Crump Hanson'un "*The Information Revolution and World Politics*"[4] başlıklı eseri, Bilgi ve İletişim Devriminin aşamalarını teknolojik gelişmeler ışığında kapsamlı olarak araştırmaktadır. Sanayi Devrimleri üzerine ise öne çıkan isimler Arnold Toynbee ile Pat Hudson olmaktadır. Toynbee'nin "*Lectures on the Industrial Revolution of the*

[1] Charles Weiss, "Science, Technology and International Relations", *Technology in Society*, Cilt 27, Sayı 3, Ağustos 2005, ss. 295-313.
[2] Charles Weiss, "How Do Science and Technology Affect International Affairs?", *Minerva*, Cilt 53, Sayı 4, Kasım 2015, ss. 411-430.
[3] Eugene B. Skolnikoff, *The Elusive Transformation: Science, Technology, and the Evolution of International Relations*, 1. Basım, Princeton University Press, New Jersey 1993.
[4] Elizabeth C. Hanson, *The Information Revolution and World Politics*, Rowman & Littlefield Publishers, Inc., Maryland 2008.

18th Century in England: Popular Adresses, Notes and Other Fragments"[5] isimli çalışması Sanayi Devrimlerinin çıkışına ışık tutmakta, Hudson ise "*The Industrial Revolution*"[6] isimli çalışmasıyla sürecin güncel perspektiflerden anlaşılabilmesini kolaylaştırmaktadır. Kuramsal açıdan ise Prof. Dr. Emilian Kavalski'nin "Beşinci Büyük Tartışma" söylemini ortaya attığı "*The Fifth Debate and The Emergence of Complex International Relations Theory: Notes on The Application of Complexity Theory to The Study of International Life*"[7] başlıklı makalesi, karmaşıklığın Uluslararası İlişkiler disiplinine uyarlanması adına son derece önemli bir kaynak niteliği taşımaktadır. Ek olarak, karmaşıklığın anlaşılabilmesi açısından ise Seva Gunitsky, Antoine Bousquet ve Robert R. Geyer isimleri öne çıkmaktadır. Gunitsky'nin "*Complexity and Theories of Change in International Politics"*[8]*,* Bousquet'in "*The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*"[9] ve Geyer'in "*Beyond The Third Way: The Science of Complexity and The Politics of Choice*"[10] isimli çalışmaları hem karmaşıklık kavramının hem de Karmaşıklık Teorisinin anlaşılması adına son derece faydalı olmaktadır.

İkinci bölümün başlığı "Siber Uzay ve Uluslararası İlişkiler" olarak tespit edilmiştir. Bu bağlamda siber uzaya dair her kavram ve kullanım, teknik olarak detaylı bir şekilde ele alınacaktır. Ayrıca siber uzaya yönelik uluslararası hukuk bağlamında yapılmış ve yapılması planan her türlü düzenleme ve anlaşma da yine bu bölümün kapsamı içerisinde olacaktır. Bu doğrultuda literatürde öne çıkan çalışmalar şu şekildedir: MIT'de Siyaset Bilimi kürsüsünde görev yapmakta olan Prof. Dr. Nazli Choucri, siber uzay ve Uluslararası İlişkiler üzerine yaptığı çalışmalarla "Siber Uluslararası İlişkiler" söylemini geliştirmiş, siber-güvenlik, siber-politika ve siber-terör kavramları üzerine çeşitli çalışmalarda bulunmuştur. Choucri'nin "*Cyber*

---

[5] Arnold Toynbee, *Lectures on the Industrial Revolution of the 18th Century in England: Popular Adresses, Notes and Other Fragments*, 4. Basım, Longmans, Green and Co., Londra 1894.
[6] Pat Hudson, *The Industrial Revolution*, Hodder Arnold, New York 1992.
[7] Emilian Kavalski, "The Fifth Debate and The Emergence of Complex International Relations Theory: Notes on The Application of Complexity Theory to The Study of International Life", *Cambridge Review of International Affairs*, Cilt 20, Sayı 3, Eylül 2007, ss. 435-454.
[8] Seva Gunitsky, "Complexity and Theories of Change in International Politics*", International Theory*, Cilt 5, Sayı 1, 2013, ss. 35-63.
[9] Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, 2. Basım, Columbia University Press, New York 2009.
[10] Robert R. Geyer, "Beyond The Third Way: The Science of Complexity and The Politics of Choice", *British Jorunal of Politics and International Relations*, Cilt 5, Sayı 2, Mayıs 2003, ss. 237-257.

Politics in International Relations"[11] isimli çalışması bu bağlamda en fazla dikkat çeken çalışma niteliğindedir. Diğer taraftan editörlüğünü Jan-Frederik Kremer ile Benedikt Müller'in yaptığı "*Cyberspace and International Relations: Theory, Prospects and Challenges*"[12] başlıklı çalışmada siber uzaya dair kavramsal ve teorik bilgiler derinlemesine sunulmakta olup Estonya, Stuxnet ve Ukrayna saldırıları gibi güncel siber saldırı örneklerinden uluslararası aktörlerin davranış analizleri yapılmaktadır. David J. Betz & Tim Stevens tarafından yazılmış olan "*Cyberspace and The State: Toward A Strategy For Cyber-Power*"[13] başlıklı çalışmada ise güç kavramının siber uzay alanına evrilmesi ve güç sahası oluşturmasına temas edilmekte olup siber uzay gücünün bağımsızlık ve savaş kavramlarıyla ilişkileri ele alınmaktadır. Siber uzaya dair bir başka önemli çalışma ise editörlüklerini Maxmillian Mayer, Mariana Carpes ve Ruth Knoblich'in yaptığı "*The Global Politics of Science and Technology*"[14] isimli iki ciltlik eserdir. Bu eserde siber uzaya yönelik nükleer bilimden nanoteknolojiye kadar çok farklı açılardan yaklaşımlar Uluslararası İlişkiler bağlamında ele alınmaktadır. Türkçe yazına bakıldığında ise, Vahit Güntay'ın "*Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu: Siber Savaş Örneği*"[15] başlıklı makalesi siber uzay alanını güvenlik açısından ele alarak siber savaşı açıklamaktadır. "*Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler*"[16] başlıklı bir başka çalışmada ise Muharrem Gürkaynak ve Adem Ali İren tarafından siber uzay alanındaki Uluslararası İlişkiler tartışılmaktadır.

Üçüncü bölümün başlığı ise "Siber Uluslararası İlişkiler Örnek Olayları" şeklinde oluşturulmuştur. Buna göre bu bölümde, birinci ve ikinci bölümlerde sunulan kavramsal, kuramsal, teknik ve hukuki bilgiler, örnek olaylar üzerinde

---

[11] Nazli Choucri, *Cyber Politics in International Relations*, The MIT Press, Cambridge, MA 2012.
[12] Jan-Frederik Kremer & Benedikt Müller (Editörler), *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer-Verlag Berlin Heidelberg, 2014.
[13] David J. Betz & Tim Stevens, *Cyberspace and The State: Toward A Strategy For Cyber-Power*, Routledge, Oxon 2011.
[14] Maxmillian Mayer, Mariana Carpes & Ruth Knoblich (Editörler), *The Global Politics of Science and Technology: Concepts From International Relations and Other Disciplines*, Springer-Verlag Berlin Heidelberg, 2014.
[15] Vahit Güntay, "Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu: Siber Savaş Örneği", *Güvenlik Bilimleri Dergisi*, Cilt 6, Sayı 2, Kasım 2017, ss. 81-108.
[16] Muharrem Gürkaynak & Adem Ali İren, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, Cilt 16, Sayı 2, 2011, ss. 263-279.

birleştirilecektir. Bu bölümde kullanılan kaynakların çoğunluğunu basın ve yayın enstrümanları ile güncel akademik yayınlar oluşturacaktır. Bu doğrultuda örnek olaylardan bazıları adına literatürde öne çıkan çalışmalar şu şekildedir: 1999 yılında ABD'de gerçekleşen *Moonlight Maze* saldırısına ve siber saldırıların altyapısına dair detaylı bilgilerin verildiği Fred Kaplan'ın "*Dark Territory: The Secret History of Cyber War*"[17] isimli çalışması öne çıkmaktadır. James A. Green'in editörlüğünü yaptığı "*Cyber Warfare: A Multidisciplinary Analysis*"[18] başlıklı eseri, siber saldırıların ve siber savaşların niteliklerine yönelik analizleri barındıran ve 2003 yılında Çin kaynaklı olarak ABD bilgisayar sistemlerine yapılan *Titan Rain* saldırısına dair önemli bilgileri paylaşmaktadır. Siber uzayda ilk ciddi ve sistemik saldırı olarak kabul edilen ve siber saldırıların gündelik yaşama doğrudan etkisinin ne kadar ciddi boyutlara ulaşabileceğini gözler önüne seren 2007 Estonya Saldırılarına yönelik Aviram Jenik tarafından kaleme alınan "*Cyberwar in Estonia and the Middle East*"[19] ile Stephen Herzog'un "*Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*"[20] başlıklı çalışmaları son derece dikkat çekicidir. 2010 yılında İran'a yapılan ABD ve İsrail kaynaklı Stuxnet Saldırısı, saldırının nükleer çalışmalar üzerinde yarattığı tahribat ve bölge ülkeleri üzerinden küresel boyutlara ulaşan derin etkileriyle Uluslararası İlişkiler disiplini içerisindeki güvenlik anlayışına yeni boyutlar kazandırmıştır. Bu saldırıya dair Kim Zetter'in "*Countdown to Zero Day: Stuxnet and The Launch of the World's First Digital Weapon*"[21] adını taşıyan eseri ile Thomas Rid'in "*Cyber War Will Not Take Place*"[22] ve James P. Farwell & Rafal Rohozinski'nin "*Stuxnet and the Future of Cyber War*"[23] başlıklı makaleleri, söz konusu olayın sistematiğine, ilerleyişine ve

---

[17] Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, 1. Basım, Simon & Schuster, NEw York 2016.
[18] James A. Green (Editör), *Cyber Warfare: A Multidisciplinary Analysis*, 1. Basım, Routledge, New York 2015.
[19] Aviram Jenik, "Cyberwar in Estonia and the Middle East", *Network Society*, Cilt 2009, Sayı 4, Nisan 2009, ss. 4-6.
[20] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, Cilt 4, Sayı 2, Yaz 2011, ss. 49-60.
[21] Kim Zetter, *Countdown to Zero Day: Stuxnet and The Launch of the World's First Digital Weapon*, 1. Basım, Crown Publishers, New York 2014.
[22] Thomas Rid, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Cilt 35, Sayı 1, 2012, ss. 5-32.
[23] James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival: Global Politics and Strategy*, Cilt 53, Sayı 1, 2011, ss. 23-40.

ekonomik ve küresel zararlarının verilerine kadar çok önemli bilgileri araştırmacıların dikkatine sunmaktadırlar. Son olarak Jason Andress & Steve Winterfeld tarafından yazılan "*Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*"[24] başlıklı çalışma, güvenlik üzerine çalışan araştırmacılara, yaşanan örnek siber olaylar üzerinden teknik açıklamalar sunmakta ve araçlar geliştirmektedir.

1.3. Yöntem

Bu çalışmanın üzerine inşa edilmesi planlanan Giriş ve Sonuç hariç üç ana bölümlü yapısı göz önünde bulundurulduğunda; metodolojik olarak birincil, ikincil ve üçüncül kaynaklardan doğrudan yararlanılacağı öngörülmektedir. Çalışmanın kavramsal, kuramsal, hukuki ve teknik çerçevesini oluşturan birinci ve ikinci bölümlerde; çoğunlukla matbu akademik kitaplar, süreli yayınlar, sözlükler, ansiklopediler, eleştirel çalışmalar ve araştırmaların yanı sıra SCI (*Science Citation Index*), SCIE (*Science Citation Index Expanded*), SSCI (*Social Sciences Citation Index*), AHCI (*Arts and Humanities Citation Index*) gibi uluslararası, bilimsel ve saygın indeksler tarafından taranmakta olan akademik dergilere başvurulacak olup çeşitli veritabanları ve çevrimiçi sayfalar gibi elektronik kaynaklardan da yararlanılacaktır. Çalışmanın yine ikinci bölümünde hukuki boyut da söz konusu olacağından uluslararası aktörler arasında yapılmış ve yapılması planlanan hukuki düzenlemeler, anlaşma metinleri ve kurumsal sözleşmeler de tercih unsuru olacaktır. Çalışmanın üçüncü bölümünün ise daha çok teknolojik karakterli örnek olay analizlerinden oluşturulması planlandığından dolayı doğal olarak elektronik nitelikli ikincil kaynaklara ve güvenilir basın ve yayın kuruluşlarının haberlerine başvurulacaktır. Akademik ve bilimsel saygınlığı yüksek, geçerliliği ve güvenilirliği bulunan ulusal ve uluslararası kurumların –T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Ulusal Siber Olaylara Müdahale Merkezi (USOM), Ulusal Havacılık ve Uzay Dairesi (*The National Aeronautics and Space Administration – NASA*), Avrupa Uzay Ajansı (*European Space Agency –*

[24] Jason Andress & Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* 2. Basım, Elsevier, Massachusetts 2014.

ESA), Rusya Devlet Uzay Etkinlikleri Kuruluşu (*The Roscosmos State Corporation for Space Activities – ROSCOSMOS*), Çin Ulusal Uzay İdaresi (*The China National Space Administration – CNSA*), Hindistan Uzay Araştırma Organizasyonu (*Indian Space Research Organisation* – ISRO), Japonya Uzay Araştırma Ajansı (*The Japan Aerospace Exploration Agency* – JAXA), Uzay Keşif Teknolojileri Şirketi (*Space Exploration Technologies Corporation* – SPACEX), Kuzey Atlantik Antlaşması Örgütü (*The North Atlantic Treaty Organization* – NATO), Avrupa Konseyi (*The Council of Europe* – COE), Birleşmiş Milletler İnternet Yönetişim Forumu (*The United Nations Internet Governance Forum* – IGF), Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (*European Union Agency for Network and Information Security – ENISA*), İnternet Derneği (*Internet Society* – ISOC), Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (*National Cybersecurity & Communications Integration Center* – NCCIC) vb.– çevrimiçi sayfaları detaylı olarak incelenecek olup paylaşılan veriler, raporlar, grafikler, tablolar, görseller gibi çeşitli kaynaklar veri toplama araçlarından olacaktır. Diğer taraftan çalışmanın içeriğine ve dolayısıyla sonucuna etki edebilecek her türlü güncel olay ve gelişmeler, gözlem yöntemi kullanılarak takip edilecek ve analize tabi tutulacaktır. Bunlara ek olarak; çalışmanın üçüncü bölümünde incelencek olan Siber Uluslararası İlişkiler örnek olaylarına konu olan devletlerin ya da kurumların resmi çevrimiçi kaynaklarına başvurulacak, servis edilen belgelerin gerçekliğine yönelik basın ve yayında çıkan resmi sorumlulara ait söylemlere bakılacak ve örnek olaya konu olan kişilerin yer aldığı belgeseller izlenecektir. Ayrıca çalışma süreci boyunca Yükseköğretim Kurulu Başkanlığı Ulusal Tez Merkezi üzerinden yayınlanmış ve konuyla ilgisi olan yüksek lisans ve doktora tezleri incelenecek olup başta Trakya Üniversitesi Kütüphanesi, Boğaziçi Üniversitesi Kütüphanesi, İstanbul Teknik Üniversitesi Kütüphanesi olmak üzere çeşitli üniversitelerin zengin kütüphanelerinde yoğun araştırmalar gerçekleştirilecektir.

BİRİNCİ BÖLÜM

KAVRAMSAL VE KURAMSAL ÇERÇEVE: ULUSLARARASI İLİŞKİLERDE "TEKNOLOJİK DÖNÜŞÜM"

"...Herkesi her an izliyor da olabilirlerdi. Ama size istedikleri zaman bağlanabildikleri açıktı. Çıkardığınız her sesin duyulduğunu, karanlıkta olmadığınız sürece her hareketinizin gözetlendiğini varsayarak yaşamak zorundaydınız; zorunda olmak ne söz, artık içgüdüye dönüşmüş bir alışkanlıkla öyle yaşıyordunuz..."[25]

Her geçen gün artan teknolojik gelişmeler, yaşanan hızlı değişimler ve ortaya çıkan yenilikler neticesinde bilim ve teknoloji, yaşamın her alanıyla doğrudan/dolaylı ve oldukça güçlü bağlara sahip bir tür karmaşık gerçeklik halini almıştır. İnsan yaşamının her alanına etki edebilirliğinden kaynaklanan teknolojinin devrimsel gücü sayesinde hayata dair algı unsurları yeniden ele alınmaya ve bugünün dünyasının gerçeklikleriyle uyumlu hale getirilmeye çalışılmaktadır. Sosyal Bilimler açısından bakıldığında ise belki de en fazla güncelleme ihtiyacının hâsıl olduğu alan Uluslararası İlişkiler[26] disiplini olarak göze çarpmaktadır. Bunun nedeni, uluslararası ilişkiler içerisinde meydana gelen her gelişme, hiç şüphesiz geçmişte meydana gelen herhangi bir olay ya da etkinlik ile ilişkilendirilerek anlamlandırılabilirken, bilhassa 20. yüzyılın sonlarından itibaren hızla artan teknolojik gelişmelerin devrimsel gücü de dikkate alındığında, küresel düzeyde daha önce hiç bu kadar geniş kapsamlı ve hızlı bir değişim yaşanmamıştır. Uluslararası ilişkilerin yapısal olarak yaşamakta olduğu bu küresel başkalaşım süreci, uluslararası politikada meydana gelen tektonik kaymaların tarihsel ana faktörlerinden olan savaşlar ve ekonomik bunalımlardan ziyade bilim ve teknolojide meydana gelen küresel boyutlu gelişmelerden kaynaklanmaktadır. Öyle ki 21. yüzyıl uluslararası ilişkilerinde bilim ve teknoloji alanında yaşanan geniş kapsamlı gelişmeler, artık uluslararası ekonomik gelişmelerin ve ulusal/uluslararası güvenliğin temel belirleyici faktörü konumuna gelmiştir.

---

[25] George Orwell, *1984*, Çeviren: Celal Üster, 44. Basım, Can Sanat Yayınları, İstanbul 2014, s. 27.

[26] Çalışma içerisinde disiplin adı, bilim alanı ve vurgunun öne çıkarıldığı kısımlarda "Uluslararası İlişkiler", genel ilişkilerin kastedildiği ve genel anlamın öne çıkarıldığı kısımlarda ise "uluslararası ilişkiler" yazımı tercih edilmiştir.

Bilgisayar, internet, kitle iletişim araçları, gerçek zamanlı uydu bağlantıları, telefon ve türevleri, e-mail, video konferans, küresel konumlama sistemi (*Global Positioning System*-GPS), hava durumu vb. çok sayıda yeni teknolojik gelişmenin insan yaşamında belirleyiciliğinin ve doğrudan etki edebilme gücünün giderek artması neticesinde toplumsal dönüşüm ihtiyacı hem organik olarak tabandan tavana hem de uluslararası ilişkilerdeki başkalaşımın doğası gereği tavandan tabana doğru çift yönlü vuku bulmuştur. Temel gerçeklik haline gelen bu toplumsal dönüşüm durumu, uluslararası ilişkilere yönelik yeni beklentilerin, yaklaşımların ve seçeneklerin oluşmasına vesile olmuştur. Uluslararası ilişkiler prosedürleri değişimden etkilendikçe; aktörler, aktörlerin içinde yer aldığı sistemler, aktörlerin çıkar algıları, beklentileri ve motivasyonları da değişim ihtiyacından etkilenmiştir. Çok boyutlu teknolojik dönüşüme dayanan küresel başkalaşımın neticesinde ortaya çıkmaya başlayan bu yeni dijital dünyada, özellikle devletler gibi geleneksel egemen aktörlerin kendi yapısal sistemleri içerisinde engelsiz çalışabilmeleri giderek zorlaşmaktadır. Hükümet dışı örgütlerin (*non-govermental organizations*-NGOs) ve çok uluslu şirketlerin (*multinational corporations*-MNCs) uluslararası ilişkilerdeki bu dönüşümden faydalanarak çok daha güçlü uluslararası ilişkiler aktörleri haline gelmeleri, nitelikli ve hızlı teknolojik benimseme ve ilerleme gösteren ülkelerin uluslararası ilişkilerin yeni belirleyici aktörleri pozisyonuna dönüşmesi gibi durumlar da göz önünde bulundurulduğunda alışılagelen geleneksel egemenlik ve klasik Uluslararası İlişkiler anlayışının bilim ve teknoloji bağlamında güncellenerek geliştirilmesi ve daha verimli hale getirilmesi gerekmektedir.

1. Bilim, Teknoloji ve Uluslararası İlişkiler

Bilim ve teknoloji, farklı anlamları olan birbiriyle ilişkili kavramlardır. Büyük Oxford Sözlüğü'nde bilime dair birden fazla tanımlama yapıldığı görülmektedir: "*I) Bir şeyin durumu ya da gerçekliği; belirtilen veya ima edilen bir şeyin idrakı ya da bilgisi. II) Çalışma ile edinilen bilgi; herhangi bir öğrenim bölümüyle edinilen ustalık. III) Belirli bir bilgi ya da çalışma dalı; kabul edilmiş ve tanınmış bir öğrenim bölümü. IV) Gözlemlenen gerçekler ile sistematik olarak sınıflandırılmış ve genel yasalar altında ele alınmak suretiyle az da olsa uyuşan ve kendi alanında yeni hakikatlerin keşfedilmesi için güvenilir yöntemler içeren bir çalışma dalı. V)*

'Bilimlerin'in örnekleri olan bilgi ya da entelektüel faaliyetler."[27] Türk Dil Kurumu'na (TDK) göre ise bilim; "*1. Evrenin veya olayların bir bölümünü konu olarak seçen, deneye dayanan yöntemler ve gerçeklikten yararlanarak sonuç çıkarmaya çalışan düzenli bilgi, ilim. 2. Genel geçerlik ve kesinlik nitelikleri gösteren yöntemli ve dizgesel bilgi. 3. Belli bir konuyu bilme isteğinden yola çıkan, belli bir amaca yönelen bir bilgi edinme ve yöntemli araştırma sürecidir.*"[28] Aynı kaynaklar üzerinden teknoloji tanımlamasına bakıldığında; "*I) Bir sanat dalı ya da sanatlar üzerine bir söylem veya bilimsel inceleme; pratik veya endüstriyel sanatların bilimsel çalışması. II) Belirli bir sanat ya da öznenin terminolojisi; teknik isimlendirme.*"[29] TDK'ya göre ise; "*1. Bir sanayi dalı ile ilgili yapım yöntemlerini, kullanılan araç, gereç ve aletleri, bunların kullanım biçimlerini kapsayan uygulama bilgisi, uygulayım bilimi. 2. İnsanın maddi çevresini denetlemek ve değiştirmek amacıyla geliştirdiği araç gereçlerle bunlara ilişkin bilgilerin tümü.*"[30]

Yukarıda sunulan açıklamalar doğrultusunda bilim ve teknoloji kavramlarının sözlükbilimsel anlamlarının "bilgi" odağına dayandığı görülmektedir. "Bilgi ve İletişim Devrimi", "Küresel Bilgi Çağı" gibi ifadelerin özellikle 21. yüzyıl Sosyal Bilimlerinde sıklıkla kullanılıyor oluşu ve bilginin mahiyetine yönelik yapılan vurguların giderek artmasından dolayı "bilgi" kavramının da sözlükbilimsel açıdan anlamının sunulmasını gerekli kılmaktadır. Buna göre bilgi şu şekilde tanımlanmaktadır; "*I) Bilgilendirme eylemi; eğitim, öğretim; öğretici bilginin iletişimi. II) Bazı aktif ya da temel niteliklerle bilgilendirme eylemi; ilham, canlandırma.*[31] *III) Genel kabul görmüş gerçeklik.*"[32] TDK'ya göre ise; "*1. İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat. 2. Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf. 3. İnsan zekâsının*

---

[27] William Little, H. W. Fowler & J. Coulson, *The Oxford Universal Dictionary Illustrated: An Illustrated Edition of The Shorter Oxford English Dictionary*, Editör: C. T. Onions, 3. Basım, Oxford At The Clarendon Press, Londra 1965, s. 1806.
[28] Türk Dil Kurumu, Büyük Türkçe Sözlük, *http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5bb924c4932158.33702650*, (Erişim Tarihi: 7 Ekim 2018).
[29] William Little, H. W. Fowler & J. Coulson, *a.g.e.*, s. 2140.
[30] Türk Dil Kurumu, Büyük Türkçe Sözlük, *http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5bb924c4932158.33702650*, (Erişim Tarihi: 7 Ekim 2018).
[31] William Little, H. W. Fowler & J. Coulson, *a.g.e.*, s. 1003.
[32] *A.g.e.*, s. 1093.

çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf. 4. Genel olarak ve ilk sezi durumunda zihnin kavradığı temel düşünceler. 5. Doğa bilgisi. 6. Kurallardan yararlanarak kişinin veriye yönelttiği anlam."[33]

Özü insan aklının alabileceği bilgiye dayanan bilim ve teknoloji kavramlarının belirtilen sözlükbilimsel anlamları, Uluslararası İlişkiler alanına indirgenerek modern yaklaşımla adapte edilmelidir. Buna göre deneylere, gözlemlere ve kuramsal analizlere dayanan doğal dünyanın bilgisi olan bilimin, modern bilim toplumunun güncel çalışmalarını da kapsayacak şekilde Uluslararası İlişkiler bağlamında genişletilmesi gerekmektedir. Bu genişleme, bilim insanlarının güvenlik, istihbarat ya da uluslararası ilişkilerin diğer yönlerine katılımından, bilim insanları arasındaki iletişim, işbirliği ve rekabet süreçlerine ve bilim insanlarının bireysel ya da kurumsal olarak danışmanlık ve savunuculuk faaliyetlerine kadar çok yönlü olmalıdır.[34] Aynı şekilde doğal dünya hakkındaki sistemli teknik bilgilerin pratik amaçlar için uygulanışı teknoloji ile vuku bulurken, teknolojinin en belirleyici özelliği olarak da "kamusal bilgiyi"[35] (*public knowledge*) ön plana çıkarmaktadır. Buna göre "şeyler"in neden ve nasıl oldukları konusundaki bilgiden ziyade, insani amaçların tanımlanabilir ve tekrarlanabilir şekilde nasıl yerine getirileceğinin bilinmesi sayesinde bilginin kamusallaşması sağlanmaktadır. Kamusal bilginin karakteristik özelliği olarak ise iletilebilirliği ve tekrarlanabilirliğinin yanı sıra ilke olarak tanımlanabilir algoritmalarla yeniden yapılandırılabilmesi ön plana çıkmaktadır.[36] Bundan dolayı teknolojinin geliştirilme ve kullanım kapasitelerinin de sürekli değişen dünya şartlarını kapsayacak şekilde genişletilmesi gerekmektedir. Bu bağlamda birey ve devlet yaşamında doğrudan etkili ve belirleyici olan en basit teknoloji pratiklerinden –tuvalet, uyuşturucu ve türevleri, bomba yüklü araçlar vb.– tutun da en gelişmiş teknoloji pratiklerine –uzay araçları, hızlı enformasyon

[33] Türk Dil Kurumu, Büyük Türkçe Sözlük, *http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5bb924c4932158.33702650*, (Erişim Tarihi: 7 Ekim 2018).
[34] Charles Weiss, "How Do Science and Technology Affect International Affairs?", *Minerva*, Cilt 53, Sayı 4, Kasım 2015, s. 412.
[35] John Michael Ziman, *Public Knowledge: An Essay Concerning The Social Dimension of Science*, 2. Basım, Cambridge University Press, Londra 1974, ss. 8-12.
[36] Harvey Brooks, "Technology, Evolution, and Purpose", *Daedalus*, Cilt 109, Sayı 1, Kış 1980, s. 66.

enstrümanları, biyoteknolojik uygulamalar vs.– kadar pek çok teknolojik uygulama Uluslararası İlişkiler kapsamında değerlendirilmektedir.[37]

Bilimsel gelişmelerin ve teknoloji uygulamalarının uluslararası ilişkilerin yapısını ya da toplumsal unsurları bütünüyle değiştirdiğini iddia etmekten ziyade uluslararası ilişkilerin çeşitli yönlerini etkileyerek dönüşüme yol açtığını belirtmek daha yerinde görünmektedir.[38] Bu gelişmelerin ve uygulamaların sosyal yapılar içerisinde şekillendirilmesiyle ortaya çıkan etkiler, yapısal faktörler arasındaki ilişkileri değiştirebilir ve yeni aktörleri ön plana çıkararak politik oyundaki katılımcı sayısını arttırabilir. Ayrıca politika konularının çerçevesini ve politika müdahalelerinin algılanan maliyet ve faydalarını etkileyerek yapı ve bağlam içerisindeki diğer değişikliklere yol açabilmektedir; ancak bu değişiklikler bilimsel bilginin ya da teknolojik kabiliyetlerin varlığı nedeniyle kendi kendine ortaya çıkmazlar. Politik ve ekonomik sistemlerdeki aktörlerin eylemleriyle, yaptıkları seçimlerle ve toplumun kümülatif tepkileriyle gerçekleşirler.[39]

Bilim alanındaki ilerlemelerin uluslararası ilişkilerin doğası üzerindeki dönüşümsel etkisinin daha iyi anlaşılabilmesi adına teknolojik değişimin Uluslararası İlişkilere yansıması incelenmelidir. Bilimsel gelişmeler, teknolojik uygulamaların gelişmesine vesile olarak sayılarının ve çeşitlerinin artmasını sağlamaktadırlar. Dolayısıyla bilimsel bilginin pratik boyutuna karşılık gelen teknolojik uygulamalar da kendi içerisinde sürekli bir değişim ve dönüşüm halinde bulunmaktadırlar. Söz konusu bu teknolojik değişim ve dönüşüm süreci, alışılagelen klasik uluslararası ilişkiler sistemi dışında faaliyet gösteren caydırıcı bir unsur olarak, ülkeler arası çıkar ilişkilerinde en dikkatli şekilde yapılmış olan planlara dahi kaçınılmaz olarak zarar verebilecek değişken ve düzensiz güç boyutlarına ulaşabilmektedir. Bununla birlikte aynı teknolojik değişim ve dönüşüm süreci, mevcut küresel sistemin içerisinde doğabilecek ve sistemin istikrarsızlığına yol açabilecek her türlü olasılığı minimize etmek için de kullanılabilmektedir. Teknolojinin karakteristik gelişim modellerine

---

[37] Charles Weiss, *a.g.m.*, s. 412.
[38] Karl W. Deutsch, "The Impact of Science and Technology on International Politics", *Daedalus,* Cilt 88, Sayı 4, Güz 1959, s. 669.
[39] Eugene B. Skolnikoff, *The Elusive Transformation: Science, Technology, and the Evolution of International Relations*, 1. Basım, Princeton University Press, New Jersey 1993, ss. 10-11.

sahip olan kavramsallaştırma–gelişim–onay–dağıtım döngüsü[40] ile ülkelerin geliştirdikleri teknolojilere karşı önlem teknolojilerinin geliştirilebilmesi için uygun fırsatlar ve zaman dilimi oluşabilmektedir. Özellikle çeşitlendirilme bağlamında gücün yapısının uygun tasarlanması, diğer tarafta bulunan aktörlerin savunmasızlığını azaltan faktörlerden olabilmektedir. Bu sebeple Uluslararası İlişkiler içerisinde –özellikle askeri ve stratejik kavramlardaki– devrimsel nitelikli değişimler istikrarsız ya da düzensiz geçişlerle gerçekleşebilmektedir. Dolayısıyla teknolojik değişim ve dönüşümün uluslararası ilişkiler üzerine etkileri son derece büyüktür ve kapsayıcıdır; ancak bu etkiler, sistem içerisindeki aktörlerin gerekli iradeye ve bilgeliğe sahip olmalarıyla doğru orantılı olarak kontrol ve manipüle edilebilir olmaktadır.[41]

Bilim ve teknolojinin insanlığın küresel refahının ileri seviyelere yükselmesini sağlayan yapıcı gücüyle, küresel yıkımları doğurabilecek karanlık ve ıstıraplı gücü eş zamanlı ve en net olarak 21. yüzyılda tecrübe edilmektedir. Bilim ve teknoloji, küresel toplumun ekonomik, siyasi, askeri ve kültürel gelişiminde her zaman güçlü bir değişimin ve dönüşümün itici gücü olmuştur. Süreklilik arz eden ve iyileştirilen üretim seçenekleri ile iletişim ve ulaşım teknolojilerindeki ilerlemeler sayesinde benzeri görülmemiş bir ekonomik refah sağlanmış ve küresel ekonomik sistem içerisinde çeşitli ve sayısız yolla çok sayıda insanın yaşam koşullarının iyileştirilmesine doğrudan katkıda bulunulmuştur. Diğer taraftan ise nükleer silahlar ve siber savaşlar örneklerinde olduğu üzere silahlı çatışmanın küresel erişiminin ve yıkıcılığının artışını da beraberinde getirmiştir. Birçok teknolojik yenilik neticesinde artan çevre kirliliği, küresel iklim değişikliği, biyoçeşitliliğin azalması gibi dramatik ve çoğu zaman istenmeyen olumsuz yan etkiler de ortaya çıkmaktadır.[42] Devletler ve hükümetlerarası örgütler tarafından alınan kararlar her ne kadar temelde siyasi süreçlere dayanıyor olsalar da, belirtilen bu olumlu ve olumsuz yan etkiler göz önünde bulundurularak, alınan bu kararlar için –bilim ve teknoloji odaklı 21. yüzyıl dünyasında– hem yerel hem de küresel fayda maksimizasyonu bağlamında bilim ve

---

[40] Arnold M. Kuzmack, "Technological Change and Stable Deterrence", *Journal of Conflict Resolution*, Cilt 9, Sayı 3, Eylül 1965, s. 317.
[41] Aynı yerde.
[42] Stefan Fritsch, "Technology and Global Affairs", *International Studies Perspectives*, Cilt 12, Sayı 1, 2011, s. 27.

teknoloji danışmanlığı elzemdir.[43] Yeni yüzyılın bu yeni vitrini içerisinde toplanan keşif verilerinin etkin ve faydacı olarak yorumlanmasında, teknik kabiliyetlerin doğru değerlendirilerek sistem içerisindeki mevcut kuvvet konuşlandırmalarının doğru şekilde anlamlandırılmasında bilim ve teknolojinin rolü ve etkisi son derece önemlidir.

Bilimsel bilgi ve teknolojik ilerlemelerin neticesinde uluslararası ilişkiler kapsamında ortaya çıkan sorunlar, riskler ve belirsizliklere yönelik Charles Weiss tarafından bilim ve teknoloji tabanlı altı model tespiti yapılmıştır:

1) Uluslararası sistemde köklü bir değişim yaratacak kadar hızlı ve geniş yelpazeye sahip bilim ve teknoloji,
2) Oyun-değiştirici olarak bilim ve teknoloji,
3) Uluslararası toplum tarafından ele alınması gereken konuların, risklerin ve sorunların kaynağı veya kilit boyutu olarak bilim ve teknoloji,
4) Uluslararası makro sorunların temel boyutları olarak ya da yeni uluslararası makro fenomenin anlaşılmasını kolaylaştırıcı kaynaklar olarak bilim ve teknoloji,
5) Dış politikanın araçları olarak veya süregelen bir uluslararası rejimin ya da problemin yönetimine girdi olarak teknik bilgi sağlayıcıları bağlamında bilim ve teknoloji,
6) Uluslararası İlişkiler ve diplomasi açısından menfaat sağlayan işbirlikçi projelerin ve kurumların doğrudan öznesi olarak bilim ve teknoloji.[44]

Birinci modelin en bariz örnekleri olarak atomik silahlar ve bilgi teknolojileri ön plana çıkmaktadır. Bilhassa nükleer silahların ortaya çıkmasıyla birlikte uluslararası ilişkilerde devletlerin ulusal güç anlayışlarının temelini nükleer teknoloji yetkinliği doldurmaya başlamıştır. Nükleer güç sahibi olmak, aktörlere uluslararası ilişkiler içerisinde belirleyicilik ve caydırıcılık anlamında ciddi avantajlar sağlamıştır.[45] Sosyal bağlamın ve insan eylemlerinin etkisine maruz kaldığından nükleer teknoloji

[43] Norman P. Neureiter, "Science and Technology in Foreign Policy", *Issues in Science and Technology*, Cilt 19, Sayı 2, Kış 2003, s. 23.
[44] Charles Weiss, *a.g.m.*, ss. 413-414.
[45] John Krige & Kai-Henrik Barth, "Introduction: Science, Technology, and International Affairs", *Osiris*, Cilt 21, Sayı 1, 2006, s. 6.

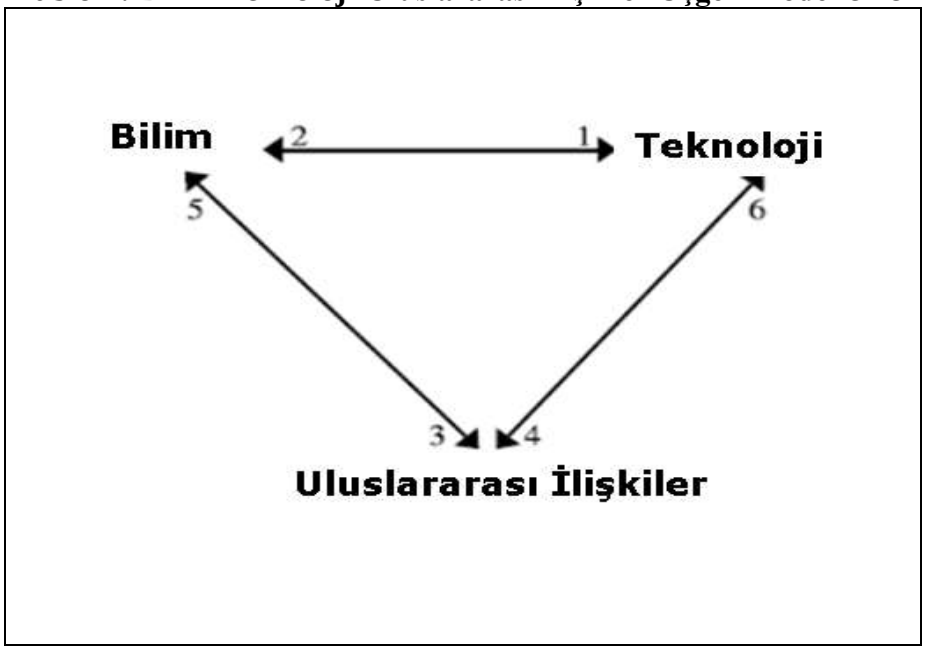
ve bilgi teknolojileri sosyal yapının öznesi konumundadır. Buna örnek olarak ise basınçlı su reaktörlerinin, nükleer denizaltılarda başarılı testlerinin ardından sivil amaçlı nükleer enerji santrallerinde baskın teknoloji haline gelmesi gösterilmiştir.[46] İkinci model kapsamında bilim ve teknoloji, uluslararası sistemdeki aksiyonların değişkeni, uluslararası sistem dâhilindeki farklı aktörlere avantajlar ve dezavantajlar sağlayan ve Uluslararası İlişkiler kuramında daha önceden açıklanmış kavramsal ayrımların bulanıklığını teknolojik ilerlemelerin yeni güç rekabet alanları içinde yeni yetenekler yaratmasıyla netleştirmeye çalışan temel unsurlar olarak sunulmaktadır.[47] Üçüncü modelde ise Uluslararası İlişkiler ile bilimsel gerçeklik arasındaki bağlantının göründüğünden çok daha karmaşık bir yapıya haiz olduğu belirtilmektedir. Buna göre bir bilim insanı açısından gerçekler, kabul edilen bilimsel metotlar ile oluşturulan ve kabul edilen otorite tarafından da doğrulanan olgulardır. Buna karşın, bu olguların çoğunluğunu uluslararası meseleler –örneğin İran'ın atom bombası üretebilme hızı gibi– oluşturmuyorsa ve özellikle yetersiz verilere ya da kaçınılmaz olarak tamamlanamamış matematiksel modellere dayanıyorsa ciddi anlamda belirsizlik içermektedir. İyi yapılandırılmış ve tarihsel olarak geniş kabul görmüş bilimsel kuramların bile geniş ölçekli farklı gözlemleri, ikame ettikleri fikirlerin sıklıkla küçük boşluklarından ve henüz çözülmemiş sorunlarından beslendiklerinden ve gelecekteki araştırmalar neticesinde çözüleceğine duyulan inançtan dolayı ikna edici bulunmaktadır.[48] Dördüncü modelde bilim ve teknoloji, küreselleşme gibi bir makro fenomenin teknik temelini sağlamaktadır. Fakat bu noktada ekonomik, siyasi, hukuki ve kültürel güçlerle uyumlu şekilde hareket eden bilim ve teknolojinin temel rolü belirsizleşebilir ve bu durumdan kaynaklı kamuoyunun, araştırmacıların ve akademik uzmanların söz konusu fenomenin bilimsel ve teknolojik yönüne yeterince dikkat vermemelerine neden olabilmektedir.[49] Beşinci ve altıncı modellerde ise bilim ve teknoloji, oturmuş uluslararası sistem içerisinde veya ikili ilişkiler kapsamında açıkça tanımlanmış çıkarların realize edilmesi gayesiyle oluşturulan temel amaçlar için istihdam

[46] Charles Weiss, *a.g.m.*, s. 414.
[47] *A.g.m.*, s. 415.
[48] Thomas S. Kuhn, *The Structure of Scientific Revolutions: Volume II*, 2. Basım, The University of Chicago Press, Chicago 1970, s. 147.
[49] Charles Weiss, *a.g.m.*, s. 420.

edilebilecek en güçlü araçlar olarak sunulmaktadır. Bu kapsamda geliştirilen yoğun bilim ve teknoloji tabanlı projeler; uluslararası müzakereler ile mutlaka çözülmesi gereken uluslararası sorunların –konum, maliyet, tedarik, fikri mülkiyet, yönetim, teknik destek vb.– artışını da beraberinde getirmektedir.[50]

Bilim ve teknolojinin hem karşılıklı hem de Uluslararası İlişkiler üzerindeki etkilerinin ötesinde, bilim ve teknolojinin de Uluslararası İlişkilerden doğrudan ya da dolaylı olarak etkilendiği üçüncü bir boyut daha bulunmaktadır. Buna göre bilim, teknoloji ve Uluslararası İlişkilerin karşılıklı ve eş zamanlı bağımlılığı bulunmaktadır. Söz konusu bağımlılık yine Charles Weiss tarafından oluşturulan üçgen modellemeyle ifade edilmiştir.[51]

Tablo-1: Bilim-Teknoloji-Uluslararası İlişkiler Üçgen Modelleme



Kaynak: Charles Weiss, "Science, Technology and International Relations", *Technology in Society*, Cilt 27, Sayı 3, Ağustos 2005, s. 298.

Bu modellemeye göre 1 numaralı ok yönünde; artan bilimsel bilgi birikiminin pratik amaçlar için düzenlenmesi ve uygulanması sayesinde teknolojik ilerlemeler söz konusu olmaktadır. Bunun en iyi örneği lazerin icadıdır: 1900'lü yıllarda Max Planck, termodinamik ile ilgili olarak ışığın tüm dalga boylarını emen kara cisim

[50] *A.g.m.*, ss. 421-423.
[51] Charles Weiss, "Science, Technology and International Relations", *Technology in Society*, Cilt 27, Sayı 3, Ağustos 2005, s. 298.

ışımasının (*blackbody radiation*) ısı aldığında neden tüm ışık frekanslarını eşit şekilde yaymadığı üzerine çalışırken enerji ile radyasyonun frekansı arasındaki ilişkiyi açıklamış, 1905 yılında ise Albert Einstein bu bilgiyi geliştirerek ışığın kendi enerjisini 'foton' adı verilen ayrık kuantum parçacık yığınlarıyla ilettiğini tespit etmiştir. Böylelikle teorize edilen bilgiler ışığında öncelikli olarak lazer, ardından ise lazer üzerine geliştirilen bilgiler ışığında kompakt diskler geliştirilmiştir.[52] 2 numaralı ok yönüne bakıldığında ise teknolojik ilerlemelerin de bilimsel ilerlemelere yol açtığı belirtilmektedir. Buna gösterilebilecek en iyi örneklerden başlıcası Hubble Uzay Teleskobu'dur. 1990 yılında uzaya gönderilen Hubble Uzay Teleskobu, 1993 yılına kadar süren hata onarım çalışmalarının ardından 1994 yılında ilk fotoğrafları göndermeye başlamasıyla birlikte kozmoloji alanında evrenin yapısına ve kökenine dair araştırmaların derinleşmesine ve mevcut bilimsel bilgilerin daha da ilerlemesine vesile olmuştur.[53] 3 numaralı ok yönüyle bilimin Uluslararası İlişkiler üzerindeki etkileri ortaya konmaktadır. Bu etkiler Weiss'e göre iki şekilde gerçekleşmektedir: Birincisi, doğal dünya hakkındaki bilimsel bilginin artması, insanları yeni fenomenlerden haberdar ederek iklim değişikliği gibi yeni konuları uluslararası gündeme getirmektedir. İkincisi ise; bilimsel işbirliği, rekabet ve iletişim, kendi içlerinde az ya da çok bağımsız süreçler olmalarına rağmen Uluslararası İlişkileri – örneğin; bilimsel işbirliği anlaşmalarının devletler arasındaki daha geniş kapsamlı ikili ilişkilere zemin hazırlayabilmesi gibi– etkileyebilmektedir.[54] 4 numaralı ok yönünde ise teknolojinin Uluslararası İlişkileri etkilediği gösterilmektedir. 1945'ten itibaren nükleer silahların, Uluslararası İlişkilerde savaşın ve jeopolitiğin doğasını değiştirerek gücün dağılımında ve çatışma dinamiklerinde belirleyici olduğu gerçeği bu durumu destekler niteliktedir.[55] 5 ve 6 numaralı ok yönlerine göre ise Uluslararası İlişkilerin bilim ve teknoloji üzerine karşı etkileri vurgulanmaktadır. Buna göre dış politika hedefleri; ulusal öncelikleri, gündemleri ve farklı alanlardaki bilimsel ve teknolojik araştırma, geliştirme, eğitim ve öğretim için nispi bütçe tahsislerini

[52] Devaryan Gupta, "Laser Technology Applications: A Gift to Humanity", *International Journal of Applied Research*, Cilt 1, Sayı 7, 2015, ss. 476-479.
[53] Oli Usher & Lars Lindberg Christensen, *The Universe Through the Eyes of Hubble*, Springer International Pubslihing AG, Cham 2014, s. 101.
[54] Charles Weiss, "Science, Technology …", s. 298.
[55] Daniel S. Geller, "Nuclear Weapons, Deterrence, and Crisis Escalation", *The Journal of Conflict Resolution*, Cilt 34, Sayı 2, 1990, s. 291.

doğrudan etkilemektedir. Ayrıca kamuoyunun genel eğilimi, temel ve uygulamalı bilimsel araştırmalar ile bilim insanlarının eğitimi de dâhil olmak üzere her türlü bilimsel ve teknolojik ilerlemenin finansmanına yönelik kamu desteğini de doğrudan etkilemektedir. Örneğin; Hubble Uzay Teleskobu'nun hazırlanma süreci, uzaya fırlatıldıktan sonraki arıza onarım süreci ve sonrasındaki güncelleme süreci maliyetleri, o dönem Amerikan kamuoyunda ve Kongre kanadında tepkiye neden olmuş ve bütçe kesinti taleplerini beraberinde getirmiştir.[56] Diğer taraftan Uluslararası İlişkilerin bilim ve teknolojinin gelişimi üzerindeki dolaylı etkileri ekonomi, hukuk, siyaset ve kültür mekanizmaları aracılığıyla işlemektedir. Teknoloji ve uygulamalı bilimler, piyasanın taleplerini ve dolayısıyla teknoloji tabanlı mal ve hizmetler için yerel veya küresel pazarı etkileyen yanıtları –ekonomi politikaları, yönetmelikler, gelir seviyeleri ve dağılımı, kültürel ya da dini tercihler vb.– desteklemektedir.[57]

2. Bilgi ve İletişim Devriminden Küresel Bilgi Çağına

Bilgi ve İletişim Devrimi, teknolojik yeniliklerin ve değişimlerin uzun soluklu tarihsel evriminin neticesi olarak ele alınmaktadır. İnsanlığın sahip olduğu bilginin giderek genişlemesi, zamanın ve mekânın erişilebilirliğinin artması ve iletişimin demokratikleşmesi ve hızlanması göz önünde bulundurulduğunda tarihten günümüze dek bilgi bağlamında insanlık adına ilerleyici bir eğilim olduğu görülmektedir.[58] Bilginin ve bilgi kaynaklarının bollaşması, geçmiş ile içinde bulunulan an arasında keskin kırılmaları beraberinde getirerek bariz yaşamsal değişimlerin yaşanmasını sağlamıştır. Aynı şekilde önem arz eden bir diğer husus; iletişim kanallarının sayısının ve çeşidinin artarak herkese ulaşılabilir hale gelmesiyle büyük mesafeler arası iletişim maliyetinin ve zaman kaybının azalması yönünde olmuştur. Yani reel iletişim maliyetleri son derece düşük miktarlara inerken, etkili şekilde iletilebilecek bilgi miktarı sınırsız olarak nitelendirilebilecek boyutlara

---

[56] Andrew Lawler, "Rising Cost of Shuttle and Hubble Could Break NASA Budget", *Science*, Cilt 305, Sayı 5692, 24 Eylül 2004, ss. 1882-1883.
[57] Charles Weiss, "Science, Technology …", s. 299.
[58] Elizabeth C. Hanson, *The Information Revolution and World Politics*, Rowman & Littlefield Publishers, Inc., Maryland 2008, s. 13.

ulaşmıştır.[59] Uydu teknolojilerinin elektronik sinyalleri 0 ile 1 rakamlarına dönüştürerek oluşturduğu sayısallaştırma kombinasyonları sayesinde ise mesajlar, fotoğraflar, görüntüler, datalar ve her türlü bilgi formları, mevcut yer istasyon modülleri aracılığıyla dünyanın her yerinden çekilebilir hale gelmiştir.[60] Öyle ki, daha güçlü ve daha esnek bilgi teknolojileri etrafında düzenlenen yepyeni bir teknolojik paradigmanın ortaya çıkışı, bilginin kendisini üretim sürecinin ürünü haline getirmesini de mümkün kılmıştır.[61]

Bilgi ve İletişim Devriminin daha iyi idrak edilebilmesi adına kökenini oluşturan en önemli eklemlerinin –matbaa, telgraf, telefon, radyo ve televizyon yayını, uydular– hem bireysel yaşam hem de Uluslararası İlişkiler boyutunda ele alınarak derinleştirilmesi yerinde olacaktır:

2.1. Matbaa

Yazının ortaya çıkışı ve yayılması, şüphesiz insanlık tarihinde yaşanmış, yaşanan ve gelecekte de yaşanabilecek en önemli değişikliklerin mihenk taşını oluşturmaktadır. 15. yüzyılın sonlarına doğru yazım araçlarında yaşanan yenilenme ve yeniden üretim neticesinde yazı, yazıcının kopyalama masasından atölyelere geçmiştir. Yaşanan bu geçiş, bilginin tüm formlarını kapsayan devriminin başlangıcı olmuştur.[62] Elizabeth C. Hanson'a göre; hangi alanda olursa olsun, günümüze kadar ortaya çıkan hiçbir teknolojik gelişme, Johannes Gutenberg'in icadı olan metal taşınabilir tipteki matbaanın yarattığı sosyal ve siyasi etkiden daha büyüğünü yaratamamıştır; çünkü matbaanın icat edildiği 15. yüzyıl dönemine kadarki süreç kendi şartları bağlamında ele alındığında, bilginin büyük miktarlarda depolanabilmesinin ve yeniden üretilebilmesinin etkili bir yolunun olmadığı görülmektedir. Yazılı her tür belgenin üretilebilmesinin ve kopyalanabilmesinin maliyeti ve zorluğundan dolayı insanlık açısından bilgi ve belgelerin dönüşümü ve aktarımı oldukça sınırlı kalmıştır. Bilginin maliyetini düşüren, temin süresini zaman

---

[59] Robert O. Keohane & Joseph S. Nye, Jr., "Power and Interdependence in the Information Age", *Foreign Affairs*, Cilt 77, Sayı 5, Eylül/Ekim 1988, s. 83.
[60] Elizabeth C. Hanson, *a.g.e.*, ss. 1-2.
[61] Manuel Castells, *The Rise of the Network Society*, 2. Basım, Wiley-Blackwell, Singapur 2010, s. 78.
[62] Elizabeth L. Eisenstein, *The Printing Press As An Agent Of Change: Communications and Cultural Transformations in Early-Modern Europe (Complete in One Volume)*, Cambridge University Press, New York 1980, s. 3.

olarak hızlandıran ve miktarını artıran Gutenberg'in matbaası, bilgi devriminin özünü oluşturmuştur.[63]

Matbaanın icadının bilgi üzerinde sadece maliyet, zaman ve miktar bağlamında etkisi bulunmamaktadır. Matbaa, aynı zamanda bilgi tekelinin kırılmasının en önemli enstrümanlarından biri olmuştur. Söz konusu kırılma iki şekilde gerçekleşmiştir: 1) Farklı görüşlerin yayılmasını kolaylaştırmıştır (Örnek: Martin Luther ve diğer Protestan reformcular), 2) Avrupa'daki Latince hegemonyasının kırılarak çeşitli yerel dillerdeki yayınların sayısını artmıştır.[64] Benedict Anderson'ın Lucien Febvre ve Henri-Jean Martin'den aktararak belirttiğine göre; 16. yüzyıla kadar kutsallığından dolayı öğretilen yegâne dil olan Latince'nin pozisyonu, matbaayla beraber ortaya çıkan kapitalist yayıncılık mantığı sebebiyle hızla değişime uğramıştır.[65] Kapitalist yayıncılık olarak adlandırılan bakış açısına göre ticari değeri olan bilgi ve yetenekler teşvik edilerek, kitap satıcılarının daha fazla kâr elde edebilme motivasyonu ile en geniş piyasaya ulaşabilme hedefi ortaya çıkmıştır.[66] Bu durumu destekleyen istatistikî verilere bakıldığında; 1446 ila 1450 yılları arasında Almanya'nın Mainz şehrinde Guttenberg'in öncülüğünde icat edilerek geliştirilen matbaanın, 1450-1500 yılları arasındaki dönemde kitap fiyatlarını üçte iki (2/3) oranında düşürdüğü[67], 1500 yılından önce basılan kitapların %77'sinin Latinceyken %23'ünün diğer yerel dillerde olduğu, 1575'ten sonraki basımların çoğunun Fransızca ve 1640 sonrasında ise Latince kitapların en düşük seviyelere ulaşarak ulusal metin çeşitliliğinin pazarı belirler hale geldiği ve Avrupa'daki kitap ticaretinin birçok parçaya bölünerek eski kutsal dillerle bütünleştirilen kutsal cemaatlerin parçalanma, çoğullaşma ve bölgeselleşme sürecinin örneklendirilmesi olarak sunulmuştur.[68]

Hanson'ın bahsettiği bir diğer önemli husus ise modern devlet anlayışının yükselmesiyle alakalıdır. Buna göre matbaanın geliştirilmesiyle Latince

---

[63] Elizabeth C. Hanson, *a.g.e.*, s. 14.
[64] *A.g.e.*, s. 15.
[65] Benedict Anderson, *Hayali Cemaatler: Milliyetçiliğin Kökenleri ve Yayılması*, Çeviren: İskender Savaşır, 1. Basım, Metis Yayınları, İstanbul 1993, s. 32.
[66] Jeremiah E. Dittmar, "Information Technology and Economic Change: The Impact of the Printing Press", *The Quarterly Journal of Economics*, Cilt 126, Sayı 3, Ağustos 2011, s. 1134.
[67] *A.g.e.*, s. 1133.
[68] Benedict Anderson, *a.g.e.*, ss. 32-33.

hegemonyasının kırılarak daha çok insan tarafından konuşulan Fransızca ve Almanca gibi dillerin konsolide edilmesi ve bu dillerdeki yayın sayısının artması, modern devlet formasyonunu kolaylaştıran ve hızlandıran önemli faktörlerden biri olarak kabul edilmektedir. Kapitalist yayıncılık mantığı, Orta Çağ Avrupası'nda kullanılan çok sayıda yerel dilin ve lehçenin birtakım standartlar ve benzerlikler etrafında birleştirilerek düşük maliyet, geniş pazar ve maksimum kâr gayeleriyle Almanca, Fransızca gibi ulusal dillerin gelişmesine vesile olmuştur. Yerel dil ve lehçelerin temel ulusal diller etrafında konsolide olmasıyla geniş alanların yönetilmesi kolaylaşmıştır. Halkın çoğunluğunun konuştuğu ve anladığı ortak diller üzerinden hazırlanan ve standartlaştırılan belgeler ve kanunlar sayesinde geniş ve tanımlanmış topraklardaki yönetimsel kapasite gelişerek siyasal konsolidasyon ve gücün merkezileşmesi desteklenmiştir. Diğer taraftan ise geniş alanlarda yaşayan yerleşik halkların psikolojik bağının temeli oluşturularak feodal sadakatin zayıflaması sağlanmıştır. Paylaşılan bu grup psikolojisi ise zamanla milliyetçilik ideolojisine evrilmiştir.[69]

2.2. Elektrikli Telgraf

Uzun mesafeler arası organize haberleşme sistemi örneklerine insanlık tarihinin en eski kayıtlarında rastlanılmaktadır. Örneğin; Milattan Önce (M.Ö.) 6. yüzyılda Pers İmparatorluğu, günümüzdeki İran, Irak, Suriye ve Türkiye topraklarının bulunduğu alanı yaklaşık olarak kapsayan bir iletişim sistemi kurmuştur. Bu sistem; her 22,5 km'de bir ara duraktan oluşmakta olup İmparatorluğa bağlı atlı ulaklar bu istasyon dizisi içerisinde nöbetleşe çalışmışlardır. "*Cursus Publicus*"[70] olarak adlandırılan Roma sistemi de daha büyük bir alanda yine aynı prensiple çalışmış ve bu sistemin en verimli olduğu Milattan Sonra (M.S.) 4. ve 5. yüzyıl dönemlerinde sadece bir mesajın bir gün ve gece dâhilinde ulaşabileceği en uzak mesafe yaklaşık 275 km olmuştur. Bir başka dikkate değer örnek ise, Venedikli tüccarlar tarafından 15. yüzyılda Akdeniz'de geliştirilen posta güvercinlerine dayalı haberleşme sistemidir ve bu dönemin kullanımı en yaygın iletişim türü olarak

[69] Elizabeth C. Hanson, *a.g.e.*, ss. 15-16.
[70] Detaylı bilgi için bkz.: Lukas Lemcke, *Imperial Transportation and Communication from the Third to the Late Fourth Century: The Golden Age of the Cursus Publicus*, Collection Latomus 353, Edition Latomus, Bruxelles 2016.

görülmüştür.[71] Yukarıda sunulan örneklerden anlaşılacağı üzere uzun mesafeler arası iletişim arayışı, kadim insanlık tarihinin her döneminde temel ihtiyaç olarak tezahür etmiştir. Bu bağlamda telgrafın icadı ve geliştirilmesi, hem insanlık tarihi açısından hem de bilgi devrimi açısından son derece büyük önem arz etmektedir.

Telgraf, mesafelerin etkisini ortadan kaldıran ve neredeyse anlık iletişim sağlayabilen ilk iletişim şekli olarak kabul edilmektedir. Her ne kadar kullanılan bant genişliği paylaşım hacmi üzerinde kısıtlayıcı olsa da bilginin önceki pratiklere kıyasla çok daha kısa sürede hedefine ulaşabilmesi devrimsel niteliktedir.[72] Telgrafın bu devrimsel özelliği, optik (semafor) telgraftan elektrikli telgrafa geçilmesiyle, doğal olarak da elektriğin keşfi ve elektrik üzerine geliştirilen çalışmaların devrimsel etkisiyle alakalıdır. Elektrik bilgisinin keşfi ve tanımlanması, iletişim teknolojilerinin ilk modern inovasyonu olarak kabul edilmiştir. Bu bilgi, elektriğin iletişime uygulanması üzerine arayış içinde olan çoğu Batı Avrupalı ülkenin ve dünyanın çeşitli yerlerindeki bilim insanlarının birikimli kültürel tabanın bir parçası haline gelmiştir.[73] Elektrik itkilerinin kablo aracılığıyla nasıl iletilebileceği, manyetizma ve elektriğin sinyalizasyon sisteminde nasıl kullanılabileceği üzerine yapılan ilk statik elektrikli deneyler sayesinde 18. yüzyılda Fransız Claude Chappe tarafından işler hale getirilen optik mekanik sistemler ortaya çıkmış ve elektrikli telgrafın öncülü olan, işaret ve bayraklar aracılığıyla harflerin görüş mesafesinde bir taraftan diğer tarafa aktarılmasını sağlayan "optik (semafor) telgraf" geliştirilmiştir.[74] Optik telgrafın mümkün hale gelmesiyle telekomünikasyon filizlenmeye başlamış ve temel mekanik yapılar yeterli doğruluk oranıyla yapılabilir hale gelmiştir. Münferit haberleşmeler için çeşitli ülkelerde çok sayıda semafor telgraf hattı istasyonu – örneğin; 1825-55 yılları arasındaki Rus Çarı I. Nikolay, St. Petersburg'u Varşova, Moskova ve Alman sınırına, yaklaşık 8 ila 10'ar km arayla inşa edilen ve her birinde 6 kişinin bulunduğu toplam 220 semafor kulesiyle birbirine bağlamıştır[75]–

[71] Elizabeth C. Hanson, *a.g.e.*, s. 17.
[72] Byron Lew & Bruce Cater, "The Telegraph, Co-ordination of Tramp Shipping, and Growth in World Trade, 1870-1910", *European Review of Economic History*, Cilt 10, Sayı 2, 2006, s. 147.
[73] Annteresa Lubrano, *The Telegraph: How Technology Innovation Caused Social Change*, 1. Basım, Routledge, New York 2012, s. 6.
[74] Brian Winston, *Media, Technology and Society - A History: From The Telegraph to The Internet*, 1. Basım, Routledge, Londra 1998, s. 21.
[75] Aynı yerde.

kurulmuştur.[76] Buna karşın, optik (semafor) telgraf, daha iyi bir teknolojiyle (elektrikli telgraf) yer değiştirerek ortadan kalkan tek telekomünikasyon alanı olarak yorumlanmıştır. Özellikle elektromanyetizma teorisi ve hassas mekaniklerin gelişimi, dinamik elektriğin kullanıldığı elektrikli telgraf dalının büyümesini desteklemiştir. Elektrikli telgrafın çalışma prensibi, metaforsal olarak insan sinir sistemine benzetilmektedir. Kara ve deniz üzerine konumlandırılan kablolar, tıpkı insan yapısındaki sinirler gibi elektriksel mesajları ileri ve geri iletmektedirler. Mesajların alındığı, verildiği ve iletildiği ana telgraf istasyonu ise tıpkı beyin gibi çalışmaktadır.[77] Ana telgraf istasyonları, dinamik elektriğin yüksek hızını kablolar içerisinde efektif kullanarak aktarımlar sağlamakta ve mesafeleri anlık dilimlere indirmektedir. Telgraf ile iletişimin öne çıkan anlık olma özelliği, 1830'ların başında İngiliz bilim insanı Charles Wheatstone'un elektrik hızı üzerine yaptığı deneylere dayanmaktadır. Karmaşık aygıtlar kullanarak yaptığı deneylerde Wheatstone, elektrik akışının teorik olarak kablosuz ortamda saniyede 450.000 km mesafeden fazlasına yani ışık hızının çok üstüne çıkabildiği varsayımında bulunmuştur.[78] Kullanılan kablonun türü elektrik akış hızına ciddi anlamda düşürücü etki yapmasına rağmen mesafelerin insanlık adına anlık dilimlere düştüğü gerçeğini değiştirmemektedir. 1832 yılında Joseph Henry tarafından New Jersey Koleji'nde (sonrasında adı Princeton Üniversitesi olarak değiştirilmiştir) halka açık deneyde telgraf sistemiyle bir koluna zil bağlı olan mekanizmaya yeterince güçlü elektromanyetik çekme yaratarak hareket ettirmiş ve zilin çalmasını sağlamıştır. Samuel Finley Breese Morse isimli Amerikalı mucit, Henry'nin patentini almadığı deney aparatını kendi çalışmasına başlangıç noktası olarak kullanmış ve elektrik akımının dar bir kâğıt şerit üzerinde yarattığı nokta ve çizgi işeretlerinden geliştirdiği kod ile "Mors sistemi" olarak bilinen elektromıknatıslı telgrafı geliştirmiştir.[79] Ardından deniz ve kara üzerinde hizmet veren çeşitli telgraf ve kablo şirketleri oluşmaya başlamış, 1866 yılında ise ilk transatlantik telgraf kablosu yerleştirilerek

---

[76] Anton A. Huuderman, *The Worldwide History of Telecommunications*, Wiley-Interscience, New Jersey 2003, s.7.
[77] Iwan Rhys Morus, " 'The Nervous System of Britain': Space, time and the Electric Telegraph in the Victorian Age", *The British Journal of the History of Science*, On Time: History, Science and Commemoration, Cilt 33, Sayı 4, Aralık 2000, s. 457.
[78] *A.g.e.*, ss. 458-459.
[79] Brian Winston, *a.g.e.*, s. 26.

dakikada 5 kelimelik bir hıza sahip Mors kodunun telgraf kanalıyla diğer tarafa iletilebilmesi sağlanmıştır.[80] Özellikle denizaltı telgraf kablo üretimi giderek önemli bir endüstri haline gelmiş ve 1850'lerden 1920'lere kadar bu alanda İngiliz hegemonyası oluşmuştur. 1930'ların sonlarından itibaren ise dünya genelinde teknolojik çalışmalara ve gelişmelere verilen önemin artamasından dolayı uluslararası ticaret ve politikada ABD, Almanya gibi güçlü rakiplerin devreye girmesiyle bu hegemonya kırılmıştır. II. Dünya Savaşı'nın patlak vermesiyle birlikte ise kıtalararası telgraf ağları, denizaltı kabloları gibi ticari yatırımlar adeta savaş silahlarına dönüşmeye başlamıştır.[81]

Telgrafın efektif olarak bu derece gelişmesiyle birlikte dünya üzerinde uzun mesafeler arasındaki etkileşim ağları (kara yolları, tren yolları vb.) hem genişlemiş hem de çeşitlenmiştir. 1800'lü yılların başında bilinmeyen iki temel altyapı (demiryolu ve telgraf), 20. yüzyıla gelindiğinde kıtasal ve küresel boyutlara ulaşmıştır. İnsan ve yük aktarımı sağlayan demiryolları ile bilgi ve iletişim aktarımı sağlayan elektrikli telgraf ağları eklektik hale gelerek modernliğin ve ilerlemenin sembollerine dönüşmüştür. Dahası bu ağ teknolojileri, toplumları ilerleme ve dünya barışı hizmetine entegre etmek için kullanılabilecek araçlar olarak tanımlanmaya başlamışlardır.[82] Diğer taraftan elektrikli telgrafın yeni ve farklı bir üretim gücü olarak küresel ölçekte yayılması, ulusal ve uluslararası ticarette özel sektörün kontrolü ve etkinliğinin geliştirilebilmesi adına yeni yasalar, ekonomik teoriler, siyasal düzenlemeler, yönetim teknikleri, örgütsel yapılar ve bilimsel gerekçeler gibi ihtiyaçları beraberinde getirmiştir.[83] Bu çok yönlü ilişkilerin özellikle ekonomik bağlamda koordinasyonu, piyasaların kendi iç dinamikleri doğrultusunda görülmez el (*invisible hand*) ile sağlanmış olsa da devletler arası ilişkiler üzerindeki etkileri çok daha karmaşık ve derinden olmuştur.

Hristiyan olan ya da olmayan, Doğu ve Batı dâhil olmak üzere çeşitli coğrafyalardaki çeşitli ülkelerde ve kültürlerde geniş kitlelere hitap etmesi sebebiyle

---

[80] Anton A. Huuderman, *a.g.e.*, s. 10.
[81] Daniel R. Headrick & Pascal Griset, "Submarine Telegraph Cables: Business and Politics, 1838-1939", *The Business History Review*, Cilt 75, Sayı 3, Güz 2001, ss. 544-545.
[82] Erik van der Vleuten & Arne Kaijser, "Networking Europe", *History and Technology*, Cilt 21, Sayı 1, Mart 2005, s. 32.
[83] James W. Carey, *Communication as Culture: Essays on Media and Society*, Revised Edition, Routledge, New York 2008, s. 158.

oldukça ilgi gören elektrikli telgraf, sabit mekân kısıtlamasını aşan veri hareketliliği özelliği sayesinde ülkeler arası ilişkilerin işlerliğini geliştirmiştir.[84] Aynı dönemlerdeki diğer altyapısal gelişmelere kıyasla telgraf, devlet kapasitelerini arttırıcı geniş kapsamlı etki yaratmıştır. Örneğin; İngiltere ile Hindistan arasındaki iletişim baz alındığında, 1830'lu yıllarda yelkenli gemi ile yaklaşık altı ay sürerken, 1850'lilerde demiryolu ve buharlı gemilerle bir ayın altına inmiş, 1870'lerde ise elektrikli telgraf ağı sayesinde aynı günde sağlanır olmuştur.[85] Bilhassa Avrupalı devletler ile kolonileri arasındaki iletişim ağını derinleştiren elektrikli telgraf, koloniyal yönetim ve kontrolün daha efektif hal almasını sağlayan bir araç haline gelmiştir. Dolayısıyla Batı hegemonyasının Batılı olmayan dünya üzerindeki varlığı daha da pekişmiştir. Öte yandan elektrikli telgrafın ekonomik bağlamda yatırım eylemi şeklindeki küresel patlaması neticesindeki İngiliz özel sektörünün denizaltı kablo üretimindeki liderliği, İngilizlerin küresel iletişimin baskın gücü olmasını sağlayarak kuralları koyan ve uygulamalarıyla etki yaratan aktörel yapısını pekiştirmiştir. İngilizlerin enformatik dominantlığı, diğer büyük güçlerin endişelerini artırarak uluslararası rekabetin daha da kızışmasını sağlamıştır. Diğer taraftan elektrikli telgrafın iletişim hızı sayesinde ticari taahhütlerin daha elverişli ve öngörülebilir hale gelmesiyle beraber ülkeler arasındaki ticaret hacimleri artmış, ulus aşırı ekonomik eylemlerin teşviği geliştirilerek dünya ekonomilerinin birbirine entegrasyonu ivme kazanmıştır. Son olarak ise elektrikli telgraf, "haber" (*news*) kelimesine yeni anlamlar yükleyerek gelişen medyanın özellikle dış politikadaki karar alıcıların fayda-maliyet hesaplarının dikkat unsuru olarak önemli bir parçası haline gelmesini sağlamıştır.[86] Tüm bu detaylardan dolayı elektrikli telgraf, insanlık tarihi açısından pek çok önemli icadın ve inovasyonun ilk adımı olarak kabul edilmektedir. Telgraf sayesinde uzun mesafe veri aktarımının ve iletişimin operasyonel bir gerçekliğe dönüşmesi, teknolojik çalışmaların fiziksel kısıtlamaları aşabilme arayışını derinleştirerek bir sonraki aşama olan kablolardan bağımsız sesin

[84] Yakup Bektas, "Displaying the American Genius: The Electromagnetic Telegraph in the Wider World", *The British Journal for the History of Science*, Cilt 34, Sayı 2, Haziran 2001, s. 231.
[85] Barry Buzan & George Lawson, "The Global Transformation: The Nineteenth Century and the Making of Modern International Relations", *International Studies Quarterly*, Cilt 57, Sayı 3, 2013, s. 628.
[86] Elizabeth C. Hanson, *a.g.e.*, ss. 19-20.

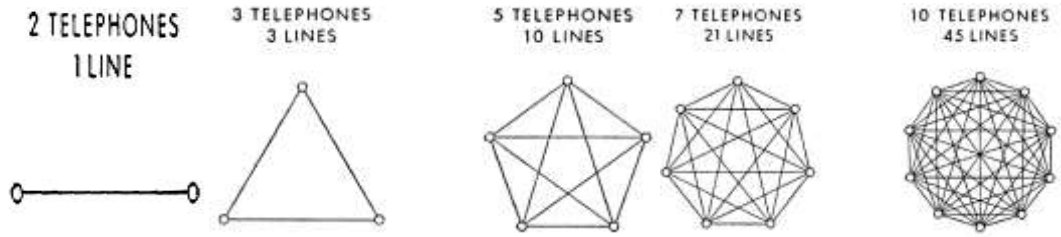
ve verilerin radyo dalgaları yoluyla iletilebilmesi deneysel çalışmalarını da beraberinde getirmiştir.

2.3. Telefon

Elektrikli telgrafın küresel anlamda gelişmesi, yayılması ve uluslararası ticaret unsuru haline gelmesiyle birlikte mevcut sistem içerisindeki bilim insanları, o zamana kadar geliştirilmiş mevcut ilkel cihazların ilerletilmesi yarışına girişmiş ve yatırımcılar tarafından endüstriyel bir imparatorluğun doğuşu öngörülerek gelişmeler dikkatle takip edilmiştir. Piyasa içerisindeki baskın aktörler pozisyonunu korumaya çalışırken, yeni aktörler ise oluşan bu yeni pazarda daha iyi konumlanabilme çabasına girişmişlerdir. Devletler açısından da uluslararası ticaret üzerinden ilişkilerin belirlenilebilirliği, yeni güç rekabet sahası olarak derinleşen bilim ve teknoloji alanına kaymıştır. Böyle bir ortamda kapsamı genişleyerek dünyanın küçülmesini sağlayan elektrikli telgraf ağlarının, çalışma prensibi revize edilerek sesin ara konumsuz doğrudan evden eve iletebilir hale gelmesi, ekonomik boyutunun yanı sıra derin toplumsal ve politik etkiler yaratan devrimsel bir gelişme olarak kabul edilmektedir. Yapılan çok sayıdaki evden eve ses iletimli telgraf türevi başarısız deneysel çalışmaların ardından, 1876 yılında Alexander Graham Bell'e ABD Patent Ofisi tarafından verilen "Telgrafta Gelişme" (*Improvement in Telegraph*) başlıklı patent ile yeni bir dönem başlamış ve şimdiye kadar yayınlanan en değerli patent olarak kabul edilmiştir.[87] 1877 yılında Gardiner Hubbard ve Thomas Sander ile birlikte Bell tarafından "Bell Telefon Şirketi" (*The Bell Telephone Company*) kurulmuş ve başlangıçta küçük ölçekli olarak yaklaşık 32 km'yi aşmayacak mesafe aralığındaki iki evi ya da bir işletme ile bir evi basit iki nokta iletişimli telefonlar üreterek, bunları kullanım amacına göre yıllık 20-40$ aralığında kiralamaya başlamışlardır. Gösterilen ilgiyle birlikte doğrudan telefon bağlantısı oluşturulan abone sayısının artışı, önemli bir sorunu da beraberinde getirmiştir: Büyük sayılardaki abone sayısının doğrudan bağlantı kurmasının imkânsız hale gelmesi.

[87] Lewis Coe, *The Telephone and Its Several Inventors: A History*, 1. Basım, McFarland & Company, Inc., Publishers, North Carolina 1995, s. 1.

Tablo-2: Telefon Bağlantıları ve Gerekli Hatlar



Kaynak: Arthur W. Page, The Bell Telephone System, Harper & Brothers Publishers, New York & Londra 1941, s. 120.

Yukarıdaki tabloda da görüldüğü üzere sadece iki abonenin birbirine bağlanması için tek hat yeterliyken, üç abonenin birbirine doğrudan bağlanması için 3 hat, beş abone için 10 hat, on abone için 45 hat, yüz abone için 4950 hat, bin abone için ise yaklaşık yarım milyon hat gerekmektedir.[88] Böylelikle çok sayıdaki abonenin doğrudan telefon bağlantılarının yapılabilmesi adına telefon santralleri ve telefon santralleri arasında da ana şebekeler oluşturulmuştur. 1878 yılında New Haven'da ilk telefon santralinin açılmasıyla artık bir abone diğerine sorunsuz şekilde bağlanabilir pozisyona gelmiştir.[89]

Telefonun küresel anlamda gelişip yayılması, elektrikli telgrafa kıyasla çok daha yavaş gerçekleşmiştir. Sesin iletilmesi, telgraf sinyali itkilerinin iletilmesinden çok daha karmaşık bir teknoloji gerektirmektedir. Zayıflamanın çok hızlı olması ve mesafenin sinyali zayıflatmasından dolayı sesin daha yüksek frekanslara ihtiyacı vardır. Dolayısıyla ses sinyallerinin zayıflamasını ve emilimini engelleyecek kabloların üretilmesi ve sistem altyapılarının oluşturulması gerekmektedir. Küresel anlamda çok daha düşük maliyetle oluşturulmuş ve yaygınlaştırılmış telgraf ağlarına kıyasla alternatif olarak çok daha yüksek maliyetli ve karmaşık teknoloji altyapısı gerektiren telefon ağlarının kurulup yaygınlaşması bu sebeple oldukça yavaş olmuştur. Öyle ki; 1920'li yıllara kadar Avrupalı devletlerin çoğunda telefon ağı bulunmamakla birlikte 1960'lara kadar da Avrupa'da uzun mesafeli ve hızlı iletişimin baskın formu olarak elektrikli telgraf devam etmiştir.[90] 1930'lu yıllarda

[88] Arthur W. Page, *The Bell Telephone System*, Harper & Brothers Publishers, New York & Londra 1941, s. 119.
[89] Claude S. Fischer, *America Calling: A Social History of the Telephone to 1940*, University of California Press, California 1992, s. 36.
[90] Elizabeth C. Hanson, *a.g.e.*, s. 21.

radyo ile telefon teknolojilerinin birleştirilmesi çalışmalarının ivme kazanmasıyla beraber ABD ile Avrupa arasında telefon bağlantıları kurulmaya başlamıştır. Taşınabilir telefonlar da yine bu dönemde özellikle devletler ya da endüstriler tarafından kullanılan iki yönlü telsizlerin, manuel olarak sabit hatlı telefon şebekelerine yerleştirilen çağrı yamalarıyla ortaya çıkmaya başlamıştır. Avrupa'nın yaşamış olduğu iki büyük savaş neticesinde yıkılan şehirler ve zarar gören altyapılar gibi teknik problemlerin yanı sıra, ülkelerin hükümet politikaları ve ulusal sınırlar arasında işbirliğine yönelik siyasi engeller neticesinde de Avrupa'da telefonun gelişimi ve ilerlemesi oldukça zor olmuştur. Avrupa'daki ülkelerde kurulan Posta, Telgraf ve Telefon İdareleri (PTT) ile özel telefon şirketleri, öncelikli olarak sabit telefon servisi sağlamaya odaklanmış, mobil radyo araştırma ve geliştirme çalışmalarını nispeten daha az önemsemiştir. Dolayısıyla Avrupalı devletler, hem kablolu hem de kablosuz taşınabilir telefonculukta uluslararası arenada ABD'nin oldukça gerisinde kalmışlardır.[91] Öyle ki bu durum, 1970'lere doğru Avrupa lehine değişim göstermeye başlamıştır.

1977 yılında ABD'de Federal İletişim Komisyonu (*The Federal Communications Commission*-FCC) tarafından ilk hücresel telefon sistemi kurulması için AT&T Bell Labortuvarları yetkilendirilmiş, bu Laboratuvarlar tarafından bir prototip hücresel analog sistemi kurulmuş, çalıştırılmış ve bir yıl sonrasında da yeni sistemin genel denemeleri başlamıştır. FCC, hücresel telsizin pratik faydası hususunda ikna olmasına rağmen ABD'nin coğrafi büyüklüğü, yaşanma olasılığı düşük problemleri yaşanır kılmıştır. Bu nedenle, hücresel telefonun ilk çalışma örneklerinin ABD'de ortaya çıkmasına rağmen, Danimarka, Norveç, İsveç ve Finlandiya gibi İskandinav ülkeleri hücresel telefonculukta işlevsel anlamda liderlik görevlerini zamanla üstlenmiş ve 1969 yılında da Nordik Mobil Telefon (*The Nordic Mobile Telephone*-NMT) Grubu etkili bir cep telefonu sistemi geliştirilmesi gayesiyle kurulmuştur. 1981 yılına gelindiğinde ise İsveç'te yaklaşık 20.000 cep telefonu kullanıcısı sayısına ulaşılmıştır ki bu sayı o dönem için Avrupa'nın en yüksek sayısı kabul edilmiştir. 1987 yılına kadar cep telefonları, kamyoncular ve inşaat işçileri için standart bir kit olarak satılmıştır. Almanya, Fransa, İtalya ve

[91] Tom Farley, "Mobile Telephone History", *Telektronikk*, Cilt 101, Sayı 3/4, 2005, s. 22.

İngiltere kendi sistemlerini tasarlamaya karar verirken; İspanya, Avusturya, Hollanda ve Belçika ise NMT Grubunun hizmetlerini takip ederek kendi ülkelerine sipariş vermişlerdir. 1990'lardan itibaren ise cep telefonu teknolojisindeki Avrupalı devletlerinin yatırımları daha da derinleşmiştir.[92]

Telefonun icadı ve gelişiminin uluslararası ilişkilere etkisi çok yönlü olmuştur. Devletler, telefonculuğun endüstrileşmesinde rekabet etmenin de ötesinde bu teknolojinin siyasileşmesini ve askerileşmesini sağlamışlardır. Uluslararası ilişkiler istihbaratının gizlilik içerisinde sağlanabilmesi açısından telefon teknolojisi son derece faydalı bir enstrüman işlevi görmüştür. Ortaya çıkan bu yeni bilgi teknolojisi sayesinde iletişim, ulaşımdan ayrılarak yeni casusluk ve savaş biçimleri yaratmıştır.[93] Yaşanan büyük savaşların yıkıcı sonuçları ve ülkelerin çıkarlarını maksimize etme gayeleri, telgraf ve telefon teknolojilerinde daha büyük gelişmelerin yaşanmasına vesile olmuştur. Gerçek zamanlı iletişimin devletler arası rekabet ve devletlerin dâhili nüfuzuna etkisi ne olursa olsun, hükümetlerin tepki sürelerini kısaltmakta ve merkezi karar vericiler üzerindeki baskıyı arttırmaktadır. Telefonun iletişim kurma yeteneğine olan müspet katkısı sayesinde yabancı elçilerin ve temsilcilerin devletler arası ilişkilerdeki belirleyici rolü nispeten azalmıştır. Diğer taraftan dile getirilen bir başka argümana göre; iletişimin telefonlar sayesinde anlık seviyelerinde hızlanması, uluslararası çatışma halini şiddetlendiren unsurların da başında gelmektedir. Buna göre dünyanın her yerindeki gerilimler anlık olarak iletilerek abartılmakta ve devlet liderleri tarafından bastırılması daha da zorlaşmaktadır. Anlık iletişim, manevralar adına diplomatik yolların etkisini azaltmakta ve olayların seyrini beklemek mümkün değilse çatışma maliyetlerinin görünürlüğünü kesinlikle arttırmaktadır.[94] Netice olarak telefon teknolojisinin gelişimi, devletler arası ilişkilerin dinamizmini arttırmış, gerçek zamanlı anlık etkileşimi mümkün kılmış, istihbarat akışını efektif hale getirmiş, ticari ve askeri

---

[92] Hazel Lacohée, Nina Wakeford & Ian Pearson, "A Social History of the Mobile Telephones With A View of Its Future", *BT Technology Journal*, Cilt 21, Sayı 3, 2003, ss. 204-205.

[93] Daniel R. Headrick, *The Tools of Empire: Technology and European Imperialism in the Nineteenth Century*, 1. Basım, Oxford University Press, Oxford & New York 1981, ss. 8-9.

[94] Cherie Steele & Arthur A. Stein, "Communications Revolutions and International Relations", *Technology, Development, and Democracy: International Comflict and Cooperation in the Information Age*, Editör: Juliann Emmons Allison, SUNY Series in Global Politics, University of New York Press, Albany 2002, s. 32.

rekabeti derinleştirerek devletler arası bağımlılığı ilerletmiş ve teknolojinin siyasallaşarak Uluslararası İlişkilerdeki belirleyiciliğini daha da pekiştirmiştir.

2.4. Radyo ve Televizyon

Elektrikli telgraf ve telefonun ortaya çıkış ve gelişme dönemleri dikkate alındığında, bu ağların kablolar üzerinden gerçekleşmesi sebebiyle bilgi ve iletişimin geçmişe kıyasla devrimsel nitelikte hızlanmasına rağmen yine kablolar sebebiyle sınırlı olduğu görülmüştür. Kablolar üzerinden sağlanan bilgi ve iletişimin, gemiden gemiye ya da gemiden kıyıya mümkün olamaması, kablo türevleri üzerinden telgraf sinyallerinin ve sesin aktarılabilme başarısı, telgraf ve telefon ağlarının küresel bağlamda karşılık bularak yayılması ve neticesinde de endüstrileşerek önemli pazarlar yaratması gerçekleri açısından rekabet eksikliğinin olduğu kablosuz bilgi aktarımı ve iletişimin sağlanabilmesi teknolojik çalışmalarının hız kazanmasını sağlamıştır.[95] Graham Bell'in elektrikli telgrafı ilerleterek geliştirdiği telefon sistemi, Thomas Edison tarafından icat edilen karbon mikrofon sayesinde yeterli yükseklikteki sesin belirli mesafeler arasında iletilmesini netleştirmiş, David Hughes kısa bir mesafeden ark etki aktarımını –temel olarak dönüştürülmemiş radyo sinyali– göstermiş, ardından Heinrich Hertz tarafından ark etkisinin iletimi daha uzun mesafeden sağlanmış ve söz konusu etkinin pratik iletişim için kullanılabilmesi adına vermiş olduğu ilham Edouard Branly tarafından kullanılarak metal uçları olan küçük bir cam tüp ve her bir uçta tel kontağı olan "*coherer*" adını verdiği ark etkisini algılayan bir cihaz geliştirmiş ve radyo sinyallerinin en ilkel formda tanımlanabilmesini sağlamıştır.[96] Yine aynı dönemlerdeki önemli bilim insanlarından Nikola Tesla ve Guglielmo Marconi, ark etkisi vericisinin iletebileceği mesafeyi geliştirmek için bağımsız olarak çalışmalar yapmışlar ve nihayetinde Marconi tarafından 1901 yılında Kanada'dan (St. John's, Newfoundland) Atlantik Okyanusu'nun ötesindeki Britanya'ya (Poldhu, Cornwall) zorlukla algılanabilir bir

[95] Cecilia Kiely, "Titans of Technology", *PassageMakers*, 1 Eylül 2018, *https://www.passagemaker.com/trawler-news/titans-of-technology*, (Erişim Tarihi: 16 Aralık 2018), s. 47.

[96] Jack Lander, "The Fascinating Invention of Radio, and How It Can Help You Become A More Successful Inventor", *Inventors' Digest*, Cilt 29, Sayı 5, Mayıs 2013, s. 39.

sinyal iletebilme başarısı gösterilmiştir.[97] Böylelikle elektromanyetik enerjinin dalgalar şeklindeki hareketi noktadan noktaya iletişim anlamında pratikte kabul edilmiş ve 1897 yılında dünyanın ilk radyo donanım şirketi olarak kurulan *The Wireless Telegraph and Signal Company* –1902 yılı sonrasında *The Marconi Company* adını almış, 1999 yılında *British Aerospace* ile birleşerek *BAE Systems* oluşturulmuştur– gemiler ile kıyı arasındaki bilgi iletişiminin sağlanabilmesi için Morse kodunu noktadan noktaya ileten kablosuz telgrafı üretmişlerdir.[98] Kablosuz telgraf öncesindeki bilgi ve iletişim teknolojilerinin kablolar aracılığıyla yapılıyor olması, söz konusu kablosuz telgraf icadının mantıksal olarak adının "kablosuz" (*wireless*) şeklinde konmasına vesile olmuş ve 1906 yılına kadar bu şekilde tanımlanmasını sağlamıştır. 1906 yılında Berlin'de gerçekleştirilen Uluslararası Radyo Telgraf Konvansiyonu'nda (*International Radio Telegraph Convention*) insanlık tarihi açısından son derece önemli olan bu icadın adındaki "kablosuz" kelimesi yerine "radyo" (*radio*) kelimesinin kullanımı tercih edilmiştir.[99] Latince "*radius*" –ışın ya da ışık hüzmesi– kelimesinden türetilen "radyo", merkezi bir noktadan çıkan elektromanyetik dalgaların radyasyonunu en doğru şekilde tanımlayabilecek yepyeni bir kelime olarak düşünülmüştür; ancak bilimsel araştırmalardaki alışagelmişlikten dolayı "radyo telgraf" terimi yerine "kablosuz telgraf" kullanımının bir süre daha devam ettiği görülmüştür.[100]

Radyo telgrafın erken zamanlarında, radyo sinyallerinin eş zamanlı alımlarının işlevsellik açısından önemli sorunlar yarattığı gözlenmiştir. Açık denizdeki iki ya da daha fazla gemiden –vericiden– çıkan radyo sinyalleri, karada kurulan alıcı radyo istasyonlarında eş zamanlı algılandığında iletişim açısından karmaşık ve pratiklikten oldukça uzak bir iletişim hali oluşturmuştur. Frekans sıklığının ayarlanması ile alıcı ve verici istasyonların muazzam derecede geliştirilmesi dahi deniz ile kara arasındaki iletişimi bir süre daha nokta ve çizgilerle

---

[97] John B.Williams, *The Electronics Revolution: Inventing the Future*, 1. Basım, *Springer Praxis Publishing*, Chichester Mayıs 2017, s. 1.
[98] Julian Newby, *Inside Broadcasting*, 1. Basım, Routledge, Londra 1997, s. 12.
[99] USA Washington Printing Office, *International Radio Telegraph Convention of Berlin: 1906 And Propositions For The International Radio Telegraph Conference of London*, Washington 1912, *https://archive.org/details/internationalrad00interich*, (Erişim Tarihi: 17 Aralık 2018).
[100] Lewis Coe, *Wireless Radio: A History*, 2. Basım, McFarland & Company, Inc., Publishers, North Carolina Şubat 2006, s. 3.

(Morse kodları) sınırlı tutmuştur. "Edison etkisi" olarak da adlandırılan elektron akışından dolayı bir vakum içerisinde iletimin sağlanabilmesi bilgisi, İngiliz Elektrik mühendisi John Ambrose Fleming tarafından –günümüzde diyot vakum tüpü olarak da bilinen– "valf"ın icadı ile pratik hale gelmiş ve sonrasında "radyonun babası" olarak da bilinen Amerikalı mucit Lee de Forest tarafından geliştirilen şebekenin, diyot tüpü içerisindeki verici ile toplayıcı arasına yerleştirilmesiyle elektron akışı kontrol edilebilir hale gelmiş ve ses iletimi tam olarak sağlanmıştır.[101] Radyo telgrafının işlevselliğinin her geçen gün ilerlemesiyle birlikte amatör bilim meraklılarının da ilgisi giderek artmış ve çok sayıda amatör radyo alıcı-verici istasyonları inşa edilmiştir. Diğer taraftan söz konusu icadın pratikliği, ordular açısından donanmanın faydasına görülmüş ve kablosuz iletişim, ulusal güvenliğin omurgası haline gelmiştir. Amatör meraklıların ordunun radyo iletişimine müdahale eder pozisyonlara gelmesi ve radyo iletişiminde gizliliğin zayıf olmasından dolayı, radyo dalgalarının kullanımına yönelik uluslararası düzenleyici kuralların oluşturulması ihtiyacı doğmuş ve daha önce de belirtilen 1906 yılındaki Berlin Konvansiyonu'nda bu amaca yönelik bir taslak anlaşma, yirmi yedi devlet[102] tarafından kabul edilmiştir. Bu anlaşmayla dalga boylarının paylaşımı ve daha faydalı olan dalgaların devletler tarafından kullanılması belirlenmiştir; ancak Avrupalı devletler tarafından hızla onaylanan bu anlaşma, ABD içerisinde özel sektör ile ordu –dolayısıyla devlet– arasında kaotik bir süreç oluşturmuştur. ABD'de pek çok resmi görevli, iletişimin yönetimsel bir fonksiyon olduğunu ve radyo telgraf iletişiminin devlet tarafından kontrol edilmesi gerektiğini savunmuştur. Buna karşılık amatör operatörler ve özel radyo telgraf şirketleri, havanın tüm insanlığa ait olduğunu ve kullanımının özgür olması gerektiğini savunmuşlardır.[103] 1912 yılında *Titanic* isimli geminin batması sonucunda 1500'den fazla insanın hayatını kaybetmesi, ABD açısından dönüm noktasını oluşturmuştur; çünkü *Titanic* kaza

---

[101] Jack Lander, *a.g.m.*, s. 40.

[102] Almanya, ABD, Arjantin, Avusturya, Macaristan, Belçika, Brezilya, Bulgaristan, Şili, Danimarka, İspanya, Fransa, Büyük Britanya, Yunanistan, İtalya, Japonya, Meksika, Monako, Norveç, Hollanda, İran, Portekiz, Romanya, Rusya, İsveç, Türkiye ve Uruguay. Detaylı bilgi için bkz.: USA Washington Printing Office, *International Radio Telegraph Convention of Berlin: 1906 And Propositions For The International Radio Telegraph Conference of London*, Washington 1912, *https://archive.org/details/internationalrad00interich*, (Erişim Tarihi: 17 Aralık 2018), s. 3.

[103] Elizabeth C. Hanson, *a.g.e.*, ss. 25-26.

yaptığı sırada *Marconi Company*'e ait radyo telgrafı kullanılarak SOS çağrısında bulunulmuş ve gelen yardım sayesinde çok sayıda insanın hayatı kurtulmuştur.[104] Bu trajedi neticesinde radyo iletişimin önemi daha iyi anlaşılarak bu olaydan sadece dört ay sonra oldukça katı bir Radyo Kanunu (*Radio Act, 1912*) Kongre tarafından kabul edilmiştir. Bu kanunla birlikte hava dalgalarına erişim, devlet kontrolü kapsamına alınmış, tüm amatör operatörlere lisans alma zorunluluğu ve 1906 Berlin Konvansiyonu'ndaki prensiplere uyma zorunluluğu getirilmiştir. Dahası elektromanyetik spektrumundaki radyo dalgalarının kısa dalga boyu bantları amatörlerce, orta dalga boyu bantları özel sektöre bağlı ticari istasyonlarca ve uzun dalga boyu bantlarının[105] ise devlet kullanımına ait olduğu belirlenmiştir.[106]

Radyo (kablosuz) telgrafın günümüzdeki anlamıyla bilinen radyo yayıncılığına evrilmesi ise, teknolojik ilerlemelerin ve sosyal uyumun karşılıklı etkileşimi yoluyla bir teknolojiyi nasıl şekillendirdiğinin en güzel örneğidir. 1920'lere kadar radyo teknolojisine yönelik deneysel çalışmalar, sürekli radyo dalga teknolojisinin bireysel amatörlerden kurumsal kontrole aktarılması, ordunun kablosuz iletişim teknolojilerinde rolünün artması, radyonun düzenlenmesi ve kullanılmasının meşru tabana oturtulması gibi çeşitli teknolojik ve altyapısal araştırmalarla geçmiştir.[107] 1920 yılından itibaren ABD'de ve Avrupa'da ilk radyo istasyonlarının açılmasıyla birlikte düzenli radyo yayıncılığı başlayarak bilgi ve iletişim akışının en hızlı yayılan kısmını oluşturmuştur. Uluslararası radyo

---

[104] John B.Williams, *a.g.e.*, ss. 1-2.

[105] Işık ve radyo dalgaları, aynı elektromanyetik spektrumda yer almalarına rağmen dalga boyları birbirinden farklıdır. Radyo dalgaları, elektromanyetik spektrumda en uzun ve en az enerjiye sahip olan dalgalardır. Bu dalgaların yayılım karakteri; kullanılan frekans, dalga boyu ve fazın belirli bant genişliklerindeki modülasyonuna bağlı olarak değişebilmektedir. Çok Düşük Frekans (*Very Low Frequency, VLF*), Düşük Frekans (*Low Frequency, LF*), Orta Frekans (*Medium Frequency, MF*), Yüksek Frekans (*High Frequency, HF*), Çok Yüksek Frekans (*Very High Frequency, VHF*) vb. frekans aralıklarına göre bantlar oluşturulmaktadır. Detaylı bilgi için bkz.: Paul Lorrain & Dale Corson, *Electromagnetic Fields and Waves*, 2. Basım, W. H. Freeman and Company, San Fransico 1970, ss. 459-503.; Donald E. Kerr, *Propagation of Short Radio Waves*, Dover Publications, Inc., New York 1965, *https://archive.org/details/PropagationOfShortRadioWaves/page/n15*, (Erişim tarihi: 17 Aralık 2018), ss. 1-8.

[106] Cees J. Hamelink, *The Politics of Communication: A Human Rights Perspective*, SAGE Publlications, Londra 1994, s. 10.

[107] Susan J. Douglas, *Inventing American Broadcasting: 1899-1922*, 3. Basım, The John Hopkins University Press, Maryland 1989, *https://archive.org/details/InventingAmericaBroadcasting1899-1922*, (Erişim Tarihi: 18 Aralık 2018), s. 240.

yayıncılığı, odaklanılması gerekilen bir alan halini alarak çok fazla sayıda dinleyiciye ve çok fazla sayıda ülkeye ulaşabilen bir kitle iletişim ortamına dönüşmüştür.[108]

1920'lerden itibaren hem yerel hem de uluslararası bağlamda ortaya çıkmaya başlayan kitlesel bilgi ve iletişim ortamının gelişmesine ve daha da genişlemesine önemli katkı sağlayan bir diğer önemli yeniliğin adıysa "televizyon" olmuştur. Televizyonun icadı de tıpkı kendisinden önceki teknolojik gelişmelerde olduğu gibi bilimsel ve teknolojik olaylar dizisine dayanmakla birlikte daha kapsayıcı ve karmaşık olma özelliğine de sahiptir. Öyle ki televizyonun çalışma prensibi; elektrik, telgraf, fotoğraf ve hareketli resimler ile radyodaki gelişmelerin bütünleştirilmesine dayanmaktadır.[109] Televizyon, muhtemelen farklı mekân ve zamanlarda yaşamış çok sayıda bilim insanının üretme isteğiyle ortaya koydukları çabaların neticesi olarak ortaya çıkan ve geçici görsel imgelerin elektriksel iletimini, kabulünü ve görsel yansıtılmasını sağlayan son derece fonksiyonel bir araçtır. Bir video sistemi kurulması yolunda ilk pratik adım, 1884 yılında Alman Paul Nipkow isimli genç bir mühendislik öğrencisi tarafından tasarlanan ancak realize edilemeyen mekanik bir görüntü tarama cihazı tasarımıyla başlamıştır. Nipkow'un görüntü tarama konsepti, tıpkı insan gözünün basılı bir sayfayı taraması gibi, bir sahnenin noktadan noktaya, soldan sağa ve yukarıdan aşağıya doğru şekilde denetlenmesi fikrini ortaya koymuştur. Buna göre tarama işlemi, ışık değerlerinin noktadan noktaya iletilebilen eşdeğer elektrik değerlerine dönüştürülmesine hizmet etmekte ve bir nesnenin bir ekranda görünmesini sağlayabilmek için uzak konumda bir kopya tarama diskinin bulunmasını ve görüntüleme birimiyle tam senkronizasyon halinde çalışma gerekliliğini ortaya çıkarmaktadır.[110] Bu prensiple ışık dönüştürücü olarak 1892 yılında Alman bilim insanları Julius Elster ile Hans Geitel tarafından fotoelektrik piller geliştirilmiş, 1906 yılında da Lee de Forest'ın geliştirdiği vakum tüpü ampflikatörü ile çok zayıf akımların güçlendirilerek katot ışın tüpü (*cathod ray tube,*

[108] Hamid Mowlana, *Global Information and World Communication: New Frontiers in International Relations*, 3. Basım, SAGE Publications, Londra 1998, s. 76.
[109] Raymond Williams, *Television: Technology and Cultural Form*, 1. Basım, Schocken Books, New York 1975, ss. 14-15.
[110] Richard C. Webb, *Tele-Visionaries: The People Behind The Invention of Television*, John Wiley & Sons, Inc., New Jersey 2005, ss. 6-8.

CRT)[111] adı verilen ışığı elektriğe ve yeniden ışığa dönüştürerek görüntü iletimi sağlanmıştır.[112] Buna karşın, işlevsel olarak görüntünün iletilebilme başarı Büyük Savaş sonrası dönemde gerçekleşmiş ve 1923 yılında Rus bilim insanı Vladimir K. Zworykin tarafından elektronik televizyon kamera tüpü tanıtılmıştır. Radyo endüstrisi içerisindeki televizyon araştırma ve geliştirme çalışmalarının ilerleme hızı, 1925 yılından itibaren radyo yayınlama sistemlerinin model olarak alınması gibi önemli teknik ilerlemeler sayesinde giderek artmıştır.[113] Öyle ki, radyonun popülaritesinin ticari, hukuki ve kamusal bağlamda çoktan yayılmış olduğu bu dönemde sunulan televizyon setlerindeki ilk görüntülerin kalitesinin oldukça düşük, maliyetlerin ise radyoya kıyasla oldukça yüksek olmasıyle birlikte Büyük Buhran'ın küresel ekonomik etkileri de dikkate alındığında yeterli ilgi ve talebin oluşmadığı görülmüştür. Öyle ki dünyanın ilk düzenli televizyon servisi (*Deutscher Fernseh-Rundfunk*) 1935 yılında Almanya'da hizmete girmesine rağmen görüntü kalitesinin düşüklüğü, programlamasının düzensizliği ve en önemlisi satış olmaması gibi nedenlerden dolayı aynı yıl içerisinde faaliyetlerini durdurmuştur.[114] Televizyon setlerinin küresel düzeyde ilgi uyandırması ve talep görmesi, II. Dünya Savaşı sonrası dönemde uydu çalışmalarındaki gelişmelerle birlikte başlamış, teknolojik altyapının geliştirilmesi ve maliyetlerin nispeten düşürülmesiyle birlikte 1960'lı yıllardan itibaren giderek artmıştır.

Radyo ve televizyonun icadının işlevsel hale gelerek yaygınlaşmasıyla birlikte gelişen radyo ve televizyon yayıncılığı, ulusların arasındaki ilişkiler üzerinde ani ve dinamik bir etki yaratmıştır. Uygarlık tarihinde yaşanan daha önceki bilimsel başarılara kıyasla radyo ve televizyon alanındaki ilerlemeler oldukça çabuk gerçekleşerek büyümüştür. Radyo ve televizyon yayıncılığının etkisi ulusal ve

---

[111] Katot ışın tüpü (CRT), bir veya birden fazla elektron tabancası içeren bir vakum tüpüdür ve imgeleri görüntülemek için kullanılan bir floresan ekran içerir. Görüntüleri oluşturmak için elektron ışınlarını hızlandırmaya ve yansıtmaya yarayan bir aracı vardır. Görüntüler; elektriksel dalga formlarını (osiloskop yani salınımölçer), fotoğrafları (televizyon, bilgisayar monitörü) ve radar hedeflerini temsil edebilmektedir. Katot ışın tüpleri (CRT), ayrıca bellek cihazları şeklinde fonksiyonel olarak da kullanılmıştır. Detaylı bilgi için bkz.: Shubham Gupta, Vishal Sharma & Parshant Sharma, "Cathode Ray Tube and Its Applications", *International Journal of Innovative Research in Technology*, Cilt 1, Sayı 6, 2014, ss. 1731-1733.

[112] Albert Abramson, "The Invention of Television", *Television: An International History*, Editör: Anthony Smith, 2. Basım, Oxford University Press, New York 1998, ss. 11-12.

[113] Raymond Williams, *a.g.e.*, s. 18.

[114] Elizabeth C. Hanson, *a.g.e.*, s. 35.

uluslararası bağlamda eşit gibi görünse de bazı özelliklerinden dolayı uluslararası alandaki etkileri daha ağır basmaktadır. Radyo dalgalarının yapısal özelliklerinden dolayı yayınların ulusal sınırlar içerisinde tutulamaması, iki istasyonun birbiriyle etkileşime girmeden etere/esire[115] aynı frekansta dalgalar gönderememesi ve bu özelliklerinden dolayı radyo ve televizyonun kaçınılmaz olarak hem uluslararası iyi niyetlerin hem de uluslararası kötü iradelerin yayılmasında araç olarak kullanılır hale getirmiştir.[116] Noktadan noktaya iletişim fikrinin ötesine geçilmesi, I. Dünya Savaşı'ndan sonrasına kadar kablosuz iletişimin potansiyelini baskılayan gerçek engelleyici olmuştur. Radyo yayını esasen sinyallerin nereden alınacağını önceden bilmemekle ilgili olup kitlelerin çok yönlü ve daha fazla sömürülebilmesinin, teknolojinin algılanabilen büyük bir hatasının yani herkes tarafından dinlenilebilir olmasına bağlılığını daha da güçlendirmiştir.[117] Özellikle II. Dünya Savaşı döneminde en etkili propaganda yöntemlerinden biri olarak radyo, dış politikada kabul gören diplomasi, ekonomik baskı ve askeri güç araçlarıyla birlikte yer almıştır.[118] Radyolar aynı zamanda toplumsal istikrar ve moral inşa enstrümanı olarak da devletlerce tercih edilmiştir. Öyle ki bu dönemde Fransız hükümetine bağlı istasyonlar halka sakin olma tavsiyelerini, İngiliz Yayın Kuruluşu (*The British Broadcasting Corporation*, B.B.C.) eğlenceyle birlikte acil durum talimatlarını, Alman *Deutscher Fernseh-Rundfunk* ise Polonya'nın kolaylıkla elde ediliş

---

[115] Fizikte boş alan kavramı, tamamen farklı alt alanlara ait iki düşünce alanına ayrılabilmektedir. Bir tarafta boşluğun hiçbir zaman parçacıklardan ya da alanlardan yoksun olmadığı görüşünü çeşitli formlarda savunan kuantum alan teorileri ve türevleri yer alırken, diğer tarafta ise Albert Einstein'ın genel görelilik kuramı bağlamında uzay-zamanın içsel metrik yapısının spesifik bir belirteci olarak varlığı ileri sürülen ve Türkçe'de "Eter" ya da "Esir" (İng.: *Ether* / *Aether*; Alm: *Äther*) olarak adı geçen maddenin varlığı yer almaktadır. Her iki düşünce alanı da boşluğun esasen bir madde formu ya da formlarıyla dolu olduğunu savunmaktadır. Boş alan maddesinin literatür içerisinde kavramsallaşması da "eter/esir" üzerinden gerçekleşmiştir. Eter/esir maddesi, sadece dış uzay alanını değil, iç uzay alanı olan atmosferik dünya boş alanını da kapsamaktadır. Detaylı bilgi için bkz.: Joseph Larmor, *Aether and Matter: A Development of the Dynamical Relations of the Aether to Material Systems On The Basis of The Atomic Constitution of Matter*, Cambridge University Press, Cambridge 1900.; Albert Einstein, "Ether and The Theory of Relativity", *The Collected Papers of Albert Einstein, Volume 7: The Berlin Years: Writings, 1918-1921 (English Translation Supplement by Alfred Engel)*, Princeton University Press, New Jersey 2002, ss. 160-183.; Matjaž Ličer, "The Concept of Aether in Classical Electrodynamics and Einstein's Relativity", *Filozofski Vestnik*, Cilt 34, Sayı 2, 2013, ss. 61-77.

[116] Joseph J. Mathews, "The Radio and International Relations", *The Southwestern Social Science Quarterly*, Cilt 20, Sayı 2, Eylül 1939, s. 140.

[117] Brian Winston, *a.g.e.*, ss. 75-76.

[118] John B. Whitton, "War by Radio", *Foreign Affairs*, Cilt 19, Sayı 3, Nisan 1941, s. 584.

hikâyelerini radyolar üzerinden milyonlara duyurmuşlardır.[119] Hatta radyo, gerçek savaş ortamında aktif bir araç olarak da kullanılmıştır. Örneğin; Naziler tarafından radyo, saldırı ve işgaller öncesinde karşı tarafın moral olarak çökertilmesini sağlayan –"*Alman ajanları her yerde, her şeyi bilir, görür ve raporlar*" şeklindeki propaganda yayınlarıyla– dinamik bir silah olarak kullanılmıştır.[120] Propagandanın bir tür saldırı silahı olarak kullanılması, savaşların tarihi kadar eskilere dayanmakla birlikte yeni olan nokta, devletin en sert güç olduğu ve bunun geliştirilip etkili şekilde uygulanması için resmi devlet organlarının kullanıldığı ve çeşitlendirildiği gerçeğidir. Devletler tarafından da radyonun gücünün –her eve ulaşabilir olması– ve olanaklarının genişliğinin –sınırlandırılamazlığı– farkına varılması, onu en tehlikeli propaganda araçlarından biri haline getirmiştir.[121]

Diğer taraftan televizyon yayıncılığına geçiş, II. Dünya Savaşı'nın ve televizyon alıcı fiyatlarının yüksekliğinden kaynaklı yavaş gerçekleşmiş olsa da özellikle Amerikan siyasetindeki etkisi oldukça güçlü olmuştur. Örneğin 1952 yılındaki ABD Başkanlık Seçimlerinde Cumhuriyetçi stratejistler, yeni yeni gelişen televizyon yayıncılığının etkisine güvenerek Dwight Eisenhower'ın konuşmalarının bir kısmını televizyon üzerinden yayınlayarak seçim kampanyasını oluşturmuşlardır. Bu durum, gerek politikacılar gerekse de gazeteciler açısından ortaya çıkan bu yeni medya türünün ilk ciddi deneyimi olmuştur.[122] Televizyon yayıncılığı sayesinde siyasi elitler, politikalarını vatandaşlarına doğrudan yüz yüze aktarabilme imkânına sahip olurken, kitlelerin manipülasyonu daha kolaylaşarak nüfuz alanı genişlemiştir. Televizyon teknolojisindeki ilerlemeler –kablolu televizyon, siyah-beyaz küçük ekranlar, renkli ekranlar, büyük ekran televizyonlar, ses ve görüntü kalitesi iyileştirilmiş televizyonlar gibi– radyo yayıncılığındaki ilerlemelerle doğru orantılı olarak uluslararası yayıncılığın[123] gelişmesini sağlamıştır. Böylelikle devletler

---

[119] Harold N. Graves, "European Radio and the War", *The Annals of the American Academy of Political and Social Science*, Cilt 213, New Horizons in Radio, Ocak 1941, s. 75.
[120] John B. Whitton, *a.g.m.*, ss. 584-585.
[121] John B. Whitton, "Radio After The War", *Foreign Affairs*, Cilt 22, Sayı 2, Ocak 1944, s. 315.
[122] Lee Edwards, *Mediapolitik: How the Mass Media Have Transformed World Politics*, 1. Basım, The Catholic University of America Press, Washington D.C. 2001, s. 43.
[123] Uluslararası yayıncılık (*International broadcasting*): Sponsor devletin sınırları dışındaki bir nüfusa yönelik devlet destekli haber, bilgi ve eğlencenin karmaşık birleşimidir. Detaylı bilgi için bkz.: Monroe E. Price, Susan Haas & Drew Margolin, "New Technologies and International Broadcasting:

arasındaki etkileşimlerde birbirlerinin medyalarını etkileyerek, halklarının ve karar vericilerinin fikirlerinin şekillendirilmesi gibi stratejik hedefler ön plana çıkmaya başlamıştır. Özellikle politikacılar ve gazeteciler, uluslararası yayıncılığın etki boyutunun derinleşmesiyle birlikte siyaset ve iletişimde meydana gelen devrim niteliğindeki değişimlerin yakınsamasının medyaya egemen olan yeni bir küresel yönetim sistemi yarattığını öne sürmüşlerdir. Diplomasi, siyaset ve küresel iletişimde meydana gelen bu önemli değişimler neticesinde diplomasi ile medya arasındaki etkileşim biçimlerinde çeşitlilik oluşmaya başlamıştır. Medyanın ve kitle iletişiminin diplomasi alanındaki genişleyen rolü sayesinde iç ve dış ilişkilerdeki politik iletişimin önemi çok daha iyi anlaşılır hale gelmiştir.[124]

2.5. Uydu

Devletlerin egemenliği hakkındaki klasik literatür incelendiğinde, egemenlik anlayışının tarihsel ve coğrafi olarak değişkenlik gösterebilen uygulamaların bir karışımı şeklinde oluştuğu vurgusu öne çıkmaktadır. Bu uygulamaların biçimlendirilmesinde ve değiştirilmesinde ise bilginin ve istihbaratın rolü nispeten daha az ilgi görmüştür. Söz konusu eksiklik, bugünün küresel bilgi çağı içerisindeki artan ve gelişen bilgi ve iletişim teknolojileri açısından dikkat çekici olmuştur. Kontrol, özerklik ve otorite bağlamında üç boyutlu kavramsallaştırılarak devlete atfedilen egemenlik, Uluslararası İlişkilerin alışılagelen baskın materyalist okumasına göre belirli bir saha içerisindeki somut alanda yürütülmekte ve askeri gücün ya da ekonomik zenginliğin fiziksel temellerine dayandırılmaktadır. Bununla birlikte, 21. yüzyıl Küresel Bilgi Çağı, bu anlayışın revize edilerek değişebilir bir kurum olan egemenliğin bilgi boyutunun öne çıkmasını ve Uluslararası İlişkiler disiplini içerisinde ağırlık kazanmasını sağlamıştır.[125] Öncelikli olarak keşif ve iletişim amaçlı geliştirilen yapay uydu teknolojisi, bilgi ve iletişim teknolojileri

---

Reflections on Adaptations and Transformations", *The Annals of the American Academy of Political and Social Science*, Cilt 616, Sayı 1, 2008, ss. 152-153.

[124] Eytan Gilboa, "Diplomacy in the Media Age: Three Models of Uses and Effects", *Diplomacy and Statecraft*, Cilt 12, Sayı 2, 2001, ss. 2-3.

[125] Karen T. Litfin, "The Status of the Statistical State: Satellites and the Diffusion of Epistemic Sovereignty", *Global Society*, Cilt 13, Sayı 1, 1999, s. 95.

devrimlerine küresel boyut kazandırarak bilimsel ve teknolojik bilginin devletler arası ilişkilerdeki rolünü zirveye taşımıştır.

1940'lı yıllara kadar dış uzay neredeyse erişilmez kabul edilmiştir. II. Dünya Savaşı sürecinde geliştirilen ve kullanılan modern roket teknolojileri –Alman balistik füzeleri (*A-4/V-2*)[126] ve kıtalararası füzeler– ile uçuş yolları atmosferin ötesine geçmeyi başarmıştır. İtme etkisinin dış uzayda da çalışıyor oluşunun keşfi ve 1950'lerin ortalarına doğru geliştirilen çoklu roketlerin yeterli hız ve itki üretmesiyle dış uzay artık olası erişilebilir bir hedef haline gelmiştir. Aslına bakılırsa iki savaş arası dönemde dış uzaya erişme projesi mühendisler tarafından yoğun şekilde tartışılmış ve bilim ve teknolojide ortaya çıkmaya başlayan bu yeni çağın ilk ve en önemli hedefini ise Dünya yörüngesine yapay bir uydunun yerleştirilmesi oluşturmuştur.[127] Bu bağlamda çeşitli ülkelerden bilim insanları, uluslararası işbirliğini jeofiziğin tüm alanlarında daha üst seviyelere çıkarmak amacıyla toplanan verilerin koordinasyonunu ve elde edilen değerli bilgiler doğrultusunda kendi hükümetlerini bilimsel araştırmalara ekstra para harcamaya ikna etmeyi amaçlamışlardır.[128] Bunun sonucu olarak 1957-1958 arası dönem, çok sayıda devletin de onayıyla "Uluslararası Jeofizik Yılı" (*International Geophysical Year, IGY*)[129] olarak kabul edilmiş ve Soğuk Savaş'ın süper güçleri olan ABD ve SSCB

---

[126] Nazilerin Almanya'da iktidara gelmesinin ardından Nazi liderleri arasında fütüristik silahlara meraklı olanların tavsiyeleri doğrultusunda genişletilen füze programı kapsamında ilk olarak *A-1* (*Aggregat 1/Assembly 1*) isimli füze geliştirilmiş ancak pratikte başarısız olmuştur. Aynı modelin tespit edilen sistem açıkları düzeltilmiş ve yeniden tasarlanmış hali olan *A-2* füzesi, 2,4 km yükseliğe çıkabilme başarısı göstermiştir. Ardından daha yüksek itme gücüne sahip şekilde geliştirilen *A-3* füzelerinde yönlendirme ve kontrol sorunlarıyla karşılaşılmıştır. Yetersiz bulunan ve başarısız kabul edilen bu deneme süreçlerinin sonrasında, 1936 yılında, Alman ordusu tarafından ilk defa bir silah olarak tasarlanması kabul edilen *A-4* füze programı onaylanmıştır. *A-4* füzeleri, daha sonra propaganda adı olan *V-2* (*Vergeltungswaffe-2*) ile tanınmıştır. Alman *V-2* füzeleri, savaşta kullanılan dünyanın ilk balistik füzesi olarak kabul edilmektedir ve uydu sistemi teknolojilerine kadar birçok önemli yeniliğe öncülük eden teknolojik bir devrim şeklinde tanımlanmaktadır. Detaylı bilgi için bkz.: Steven J. Zaloga, *V-2 Ballistic Missiles 1942-52*, Osprey Publishing, Oxford 2003, ss. 3-14.

[127] Daniel Brandau, "Demarcation in the Void: Early Satellites and the Making of Outer Space", *Historical Social Research/Historische Sozialforschung*, Special Issue: Law and Conventions from a Historical Perspective, Cilt 40, Sayı 1 (151), 2015, ss. 239-240.

[128] Arthur P. Cracknell & Costas A. Varotsos, "Editorial and Cover: Fifty Years After The First Artifical Satellite: From Sputnik 1 to ENVISAT", *International Journal of Remote Sensing*, Cilt 28, Sayı 10, 2007, s. 2071.

[129] Uluslararası Jeofizik Yılı'nın düzenlenmesi, özellikle aurora, iyonosfer, meteoroloji, jeomagnetizm, radyo dalgaları ve üst atmosferdeki diğer problemlerle ilgilenen bir grup bilim insanı tarafından tasarlanmıştır. Daha önce 1882-83 ve 1932-33 yılları "Uluslararası Kutup Yılı" (*International Polar Years*) olarak bu karakterdeki çalışmalara ithafen adanmıştır. 1957-58 yılları aralığının seçilmesinin nedeni ise Güneş enerjisi aktivitesinin 11 yıllık döngüsünün maksimum

tarafından Uluslararası Jeofizik Yılı'nın resmi hedefi olarak Dünya yörüngesine yapay bir uydunun başarıyla oturtulması projesi açıklanmıştır.[130] Söz konusu proje kapsamında süper güçler arasında başlayan uzay rekabeti, 4 Ekim 1957 tarihinde 55 cm çapında, yaklaşık 3 metre uzunluğunda ve 83 kg ağırlığında dört antenli küre şeklindeki "*Sputnik I*" isimli dünyanın ilk yapay uydusunun SSCB tarafından Dünya yörüngesine başarıyla oturtulması ve sinyal alışverişinin başlamasının ardından farklı bir boyuta evrilmiş ve küresel ilişkilerde "Uzay Çağı" resmen başlamıştır. "*Sputnik I*" her 96 dakikada bir Dünya etrafındaki dönüşünü tamamlayarak, Dünya yüzeyinin ve atmosferinin dış uzay görüntüsünü radyo sinyalleriyle Dünya yüzeyindeki radyo teleskoplarına iletmiştir. Ardından 3 Kasım 1957 tarihinde yine SSCB tarafından "*Sputnik II*" isimli ikinci bir yapay uydu, içerisinde "*Laika*" isimli köpekle birlikte başarılı şekilde fırlatılarak yörüngeye oturtulmuştur. ABD ise uzay rekabetinde SSCB'nin bir adım gerisinde kalarak 31 Ocak 1958 tarihinde ilk Amerikan yapay uydusu olan "*Explorer I*", ardından da 17 Mart 1958'de "*Vanguard I*" isimli yapay uyduları başarıyla Dünya yörüngesine oturtmuştur.[131] İlk yapay uydunun Sovyetler tarafından yörüngeye başarıyla oturtulması, SSCB açısından büyük bir propaganda zaferi olarak görülürken, Amerikalılar açısından ise ciddi anlamda küresel prestij kaybı doğurmuştur.[132] Bu kaybı bastırabilmek adına ABD Kongresi tarafından "Ulusal Havacılık ve Uzay Dairesi'nin (*National Aeronautics and Space Administration, NASA*)" 500 milyon $ bütçeyle kurulması hızlı bir şekilde

---

değerine en yakın olacağı ve bu süre zarfında da Dünya üzerindeki Güneş etkisinin en yüksek seviyelerde olacağının öngörülmesidir. Dünya üzerinde çeşitli yerlerde konumlandırılmış geniş bir istasyon ağından bilim insanlarının eş zamanlı gözlemler yapabilmesi planlanmıştır. 55 ülkenin çok sayıda bilim insanıyla desteklediği bu projede yaklaşık 100 milyon Sterlin tutarında fon oluşturulmuş ve bilimsel anlamda son derece önemli keşifler –Van Allen radyasyon kuşağı vb.– yapılmıştır. Bugüne kadarki en büyük ve en başarılı uluslararası bilimsel işbirliği olarak nitelendirilen bu proje, küresel boyutta kaygı uyandıran sorunların çözümüne yönelik geniş ölçekli bir bilim formu metodolojisi geliştirmiştir. Detaylı bilgi için bkz.: Hugh Odishaw, "The International Geophysical Year and World Politics", *Journal of International Affairs*, Cilt 13, Sayı 1, 1959, ss. 54-55.; Alan T. Waterman, "The International Geophysical Year", *American Scientist*, Cilt 44, Sayı 2, Nisan 1956, ss. 130-131.; Keith E. Bullen, "The International Geophysical Year", *The Australian Quarterly*, Cilt 29, Sayı 1, Mart 1957, s. 16.; Robert H. Eather, *Majestic Lights: The Aurora in Science, History, and the Arts*, American Geophysical Union, Washington D.C. 1980, ss. 171-185.

[130] Daniel Brandau, *a.g.m.*, s. 240.

[131] Arthur P. Cracknell & Costas A. Varotsos, *a.g.m.*, s. 2071.

[132] Ann Ewing, "Man's First Satellites", *The Science News Letter*, Cilt 72, Sayı 1, Temmuz 1957, s. 10.

onaylanmıştır.[133] 1961 yılında Sovyet kozmonot Yury Gagarin'in uzaya çıkan ilk insan olmasıyla SSCB'nin uzay teknolojileri konusunda bir propaganda zaferi daha kazanmasının ardından da ABD Başkanı John F. Kennedy öncülüğünde "Apollo Projesi" (*Project Apollo*) adı verilen ve Ay'a insan götürülmesi hedeflenen projenin çalışmaları hız kazanmıştır. Bu proje, taşıdığı bilimsel değerinin yanı sıra, ABD açısından uydu ve uzay teknolojilerinde yaşanan gelişmelerin hem iç hem de dış politika aracı haline getirme çabasının en iyi sembollerinden biri olmuştur. Amerikan hükümeti, uzay çalışmalarında elde edilen başarıları, uluslararası ilişkilerde Amerikan siyasi kurumlarının üstünlüğü ve gücü şeklinde sunmakla kalmayıp, aynı zamanda uzay programı oluşturma sürecinde edinilen bilgilerin halkla paylaşılma görevini de üstlenmeye çalışarak küresel ilişkilerde yumuşak ve akıllı gücün belirleyiciliğini geliştirmiştir.[134]

Bilhassa süper güçlerin uzay araştırmaları boyunca geliştirilen uydu sistemi teknolojilerinin alçak Dünya yörüngesindeki sayılarının giderek artmasıyla birlikte küresel iletişim teknolojileri tekrardan dönüşüme uğramıştır. Dünya'nın "küresel bir köye" dönüşme sürecindeki en önemli faktörlerden biri olarak telefon teknolojileri ile birlikte uydu sistemleri; küresel iletişim, eğitim ve propaganda açısından olanak çeşitliliğini artırmıştır.[135] II. Dünya Savaşı sonrasında okyanus ötesi telefon kablosu kullanımının ve yaygınlığının artmasıyla dünya iletişim tesislerinde yaşanan hızlı büyüme, alçak Dünya yörüngesine yerleştirilmeye başlanan yapay uydu sistemlerindeki radyo sinyali tekrarlayıcı istasyonlarının sağladığı daha büyük ölçekte ucuz ve sınırsız iletişim olanaklarıyla boyut değiştirmiştir. İletişim mühendisleri tarafından dünya iletişimini genişletmenin aracı olarak kullanılması önerilen yapay uydu sistemleri, iletişim kurduğu yer istasyonlarına doğru bir görüş hattı olan dış uzayda tekrarlayıcı bir istasyon görevi üstlenmiştir. Böylelikle radyo sinyallerine dayalı iletişim artık iyonosferden yansımaya bağlı olmayacağından, radyo spektrumunun bu bölümünün daha geniş ölçekli kullanımı mümkün

---

[133] Neil P. Hurley, "Satellite Communications: A Case Study of Technology's Impact on Politics", *The Review of Politics*, Cilt 30, Sayı 2, Nisan 1968, s. 170.
[134] Hugh R. Slotten, "Satellite Communications, Globalization, and the Cold War", *Technology and Culture*, Cilt 43, Sayı 2, Nisan 2002, ss. 315-316.
[135] Marshall McLuhan & Bruce R. Powers, *Global Köy: 21. Yüzyılda Yeryüzü Yaşamında ve Medyada Meydana Gelecek Dönüşümler*, Çeviren: Bahar Öcal Düzgören, 1. Basım, Scala Yayıncılık, İstanbul 2001, ss. 186-190.

kılınmıştır. Dolayısıyla söz konusu gelişmenin mühendislik boyutundaki öneminden çok daha fazlası ön plana çıkmaktadır: Küresel boyutta devasa iletişim kapasitesi.[136]

ABD Başkanı Kennedy, 1961 yılında Apollo Projesi'ni başlatırken yapmış olduğu açıklamada, ortaya çıkan bu yeni teknolojinin –maliyet yükseltecek kısmi bölümleri ve hizmetleri de dâhil olmak üzere– teknik olarak mümkün olan en kısa sürede tüm dünyada etkin iletişim sağlayabilecek küresel kapsama alanına çıkarılması ve dünyanın en uzak köşesine dahi anlık olarak sesle, görüntüyle veya yazıyla ulaşılabilecek hale getirilmesi hususunda süratle ilerleneceği vurgusunda bulunmuştur.[137] Özellikle SSCB'nin uzay teknolojileri ve araştırmaları alanında göstermiş olduğu başarıların ardından bu dönemde SSCB ile hem askeri üstünlük hem de uluslararası prestij rekabetine odaklanan ABD Başkanı Kennedy, kendisinden önceki Eisenhower yönetiminin uydu düzenlemelerine yönelik geleneksel olarak düzenlenmiş telekomünikasyonun bir uzantısı olarak ele alma politikasını değiştirmiştir. Bu bağlamda özel iletişim şirketlerine –özellikle de baskın iletişim ortak taşıyıcısı olan *American Telephone and Telegraph* (AT&T) şirketine– özel olarak Avrupa'ya ya da diğer gelişmiş bölgelere yönelik yüksek kar getirebilecek ayrı sistemler kurmalarına izin vermek yerine tek bir dünya sistemi kurulmasında öncülük etmeyi tercih etmiştir.[138] Bu noktada da Başkan Yardımcısı Lyndon Johnson ve NASA Başkanı olarak atadığı James E. Webb'in tavsiyelerine güvenen ABD Başkanı Kennedy, uydu iletişim teknolojileri programı için onaylanan bütçenin 10 milyon $ daha arttırılmasına karar vermiş ve söz konusu bütçe artışı, yeni yönetimin bu yeni teknolojinin geliştirilmesinde aktif bir hükümet rolü sürdürme konusundaki taahhüdünün yansıması olarak yorumlanmıştır.[139] Diğer taraftan Avrupalı devletler, ABD'nin öncülüğündeki bu küresel uydu iletişim sistemine dâhil olarak ortaya çıkan avantajı INTELSAT[140] üzerindeki kontrollerini

---

[136] Current Science Association, "Space Satellites and World Communications", *Current Science*, Cilt 31, Sayı 5, Mayıs 1962, s. 177.
[137] Dallas W. Smythe & J. R. Pierce, "Communication Satellites", *Science, New Series*, Cilt 135, Sayı 3499, Ocak 1962, s. 254.
[138] Hugh R. Slotten, *a.g.m.*, s. 317.
[139] *A.g.m.*, ss. 332-333.
[140] INTELSAT (*International Telecommunications Satellite Consortium*), ABD öncülüğünde 1964 yılında 11 devlet tarafından geçici anlaşmayla kurulan ve kesin statüsünü biri hükümetlerarası diğeri üye devletlerin ilgili haberleşme kurumları arasında olmak üzere iki anlaşma ile 21.05.1971 tarihinde kazanan bir konsorsiyumdur. INTELSAT, kar amacı gütmeyen hükümetlerarası bir kurum olarak

artırmak ve uzay teknolojilerindeki bölgesel ve ulusal yeteneklerini geliştirmek için kullanmışlardır. Böylelikle Avrupa uzay teknolojileri uygulamaları bağlamında Avrupalı devletler, sahip oldukları diğer ulusal hedefleri ve projeleri ciddi şekilde etkilemeksizin kendi iletişim uydularını oluşturabilme yetkinliğine ulaşabilir hale gelmişlerdir.[141]

Uydu sistemleri teknolojisi, evreni yöneten fizik yasalarını özel amaçlar doğrultusunda manipüle eder hale getiren insanlığın entelektüel gelişiminin en belirgin ifadesi şeklinde tanımlanabilmektedir.[142] ABD ile SSCB arasında başlayan teknolojik rekabetin boyutunun ve kapsamının zaman içerisinde genişlemesiyle dış uzaya kadar ulaşması ve uydu sistemi teknolojilerini doğurması, ülkelerin dış uzaydaki bilimsel ve teknolojik faaliyetlerinin yalnızca uzaydaki varlık kapasitelerinin arttırılmasıyla sınırlı kalamayacağını açıkça ortaya koymuştur. Uzay teknolojilerinin çeşitli sektörlerde ve çeşitli uluslar adına yeteneklerin geliştirilmesine yönelik faydalı bir şekilde uygulanabileceği öngörülmüştür. Uluslararası telekomünikasyon alanında böyle bir fırsatın ortaya çıkması, uzay uydu teknolojilerinden yararlanmayı tanıtmak ve yönetmek için potansiyel olarak küresel kapsamda işbirlikçi örgütsel yapıyı gerekli kılmaktadır. Böylece bir taraftan her geçen gün daha da ilerleyen bu yeni teknolojiden yararlanılırken, bir taraftan da hem ulusal hem de uluslararası politik talepler ve ihtiyaçlar karşılanabilecek, yeni teknoloji ustalığı ile diplomasi ustalığını eşleştiren teknoloji ve politika sentezi gerçekleşebilecektir.[143] Dış uzayın ve uydu sistemi teknolojilerinin, uluslararası

---

faaliyet göstermiş ve 1973 yılına gelindiğinde kapsama alanını 109 ülkeyi alacak şekilde genişletmiştir. Tüm ülkelerin uydu iletişim teknolojilerinden faydalanabilmesi için tek bir küresel ticari telekomünikasyon uydu sistemi kurulmasını ve radyo frekans spektrumunun ve yörüngesel uzayın en verimli ve eşit şekilde devletler tarafından kullanılabilmesini sağlamayı hedeflemiştir. 2001 yılında özelleştirilen INTELSAT, medya sektörüne hizmet veren altyapı sistemlerine ve uydulara yatırım yapmaya başlamıştır. Detaylı bilgi için bkz.: Richard R. Colino, "INTELSAT: Facing the Challenge of Tomorrow", *Journal of International Affairs*, Cilt 39, Sayı 1, 1985, ss. 129-130.; David M. Leive, "Intelsat in a Changing Telecommunications Environment", *Jurimetrics*, Cilt 25, Sayı 1, Güz 1984, s. 87.; Hüseyin Pazarcı, *Uluslararası Hukuk*, Turhan Kitabevi Yayınları, Ankara 2003, ss. 306-307.; INTELSAT, "Intelsat History", *http://www.intelsat.com/about-us/history/*, (Erişim Tarihi: 18 Şubat 2019).

[141] John Gerard Ruggie, "International Responses to Technology: Concepts and Trends", *International Organization*, Cilt 29, Sayı 3, 1975, s. 563.

[142] Lloyd V. Berkner, "Earth Satellites and Foreign Policy", *Foreign Policy*, Cilt 36, Sayı 2, Ocak 1958, s. 221.

[143] Steven A. Levy, "INTELSAT: Technology, Politics and the Transformation of a Regime", *International Organization*, Cilt 29, Sayı 3, 1975, ss. 655-656.

ilişkilerin teknoloji ve politika sentezi içerisindeki konumlandırılışına göre devletler açısından ulusal ve uluslararası güvenlik tehdit unsurlarının saptanması kolaylaşarak, tespit edilen tehditlere karşı alınan güvenlik önlemlerinin –silah kontrol önlemleri ve bunlara uyum, nükleer test yasağı, kimyasal ve biyolojik silah kısıtlamaları, biyoteknoloji ve küresel sağlık önlemleri vs.– takibi sağlanabilmektedir.[144] Özellikle gelişmekte olan ülkelere yönelik takipler, temel standartların yer aldığı uydu sistemleri ve bilgisayarlara dayanan kalıcı, birleşik ve dünya çapında kurumsal teknolojik karmaşık altyapıların kurulmasıyla ve bu standartların emsal baskıları ve teknik destek programları ile kısmi zorunlu hale getirilmesiyle mümkün olmaktadır. Gelişmiş ülkeler açısından ise ulusal ve uluslararası anlamda ortak güvenlik istikrarının tesisi adına temel standart saptamaları, karşılıklı gözlem ve istihbarat paylaşımı, işbirliği ve keşif çalışmalarının derinleştirilmesi adına uydu sistemlerinin varlığı, niteliği ve önemi şüphesiz en başta gelmektedir.[145] Dolayısıyla uzay teknolojileri, uluslararası ilişkilerde devletler arası güç dengelerine istihbarat, keşif ve gözlem boyutunda yeni yaklaşımlar kazandırmakla birlikte endüstriyel bağlamda da ülkeler arası ekonomik ilişkilere ve bağlılıklara yepyeni alanlar yaratmaktadır. Bilgi ve iletişim devriminin geldiği en üst nokta olan uydu sistemi teknolojileri, devletlerin klasik güç algısını bilim ve teknoloji araştırma ve geliştirme çalışmaları bağlamında güncelleyerek 21. yüzyıla uygun hale getirmekte ve uluslararası sistemin aktörlerini dönüşmekte olan mevcut sistemin altyapısına entegrasyonunu sağlayarak sistem içerisinde daha kalıcı ve belirleyici unsurlar haline getirmektedir.

3. Sanayi Devrimleri: Endüstri 1.0'dan Endüstri 4.0'a

İnsan topluluklarında değişimin itici gücü her zaman bilgi olmuştur. Binlerce yıl öncesindeki avcı-toplayıcı toplumdan tarım toplumuna geçiş, tohumların ekim, bakım ve hasat için nasıl kullanılacağı bilgisi tarafından yönlendirilmiştir. Tarım toplumlarının odak noktasını ise verimli topraklar oluşturmuştur; ancak elde edilen verimli toprakların nasıl kullanılacağına yönelik bilgi, insanların yaşam biçimlerini küçük göçebe toplumlardan daha organize, istikrarlı ve daha büyük yerleşim

[144] John Krige & Kai-Henrik Barth, *a.g.m.*, s. 4.
[145] Hans-Henrik Rönnow, "The Information Revolution II: Satellites and Peace", *The World Today*, Cilt 45, Sayı 6, Ocak 1989, ss. 97-98.

yerlerine kadar değiştirmiştir. 18. yüzyılda ise fosil yakıtları kontrollü fiziksel güce dönüştürebilmek için makinelerin –özellikle içten yanmalı motorlar ve buharlı motorlar– nasıl kullanılabileceği bilgisine erişilmesiyle tarım toplumundan sanayi toplumuna geçiş başlamıştır.[146] Sanayi Devrimleri[147], tıpkı Bilgi ve İletişim Devrimlerinde[148] olduğu gibi, politik devrimlerin tersine bir çırpıda olmamış, kademeli olarak yavaş yavaş gelişmiştir. Ayrıca sanayi ve teknolojide meydana gelen değişikliklerin eşit düzeylerde olmaması, Uluslararası İlişkilerde büyük güçler arasındaki dengelerde kaymalar yaratmıştır. Öyle ki 19. yüzyıldaki kara ve deniz savaşlarının sonuçlarını, mali etkenler ve kredi durumlarından daha fazla etkiler hale gelmiştir.[149] Bilgi ve İletişim Devrimleri ile Sanayi Devrimleri, tarımın ve kentlerin icadından bu yana dünya tarihinde gerçekleşmiş en önemli olayların başlıcaları olarak kabul görmektedir. Söz konusu devrimler, spesifik bir başlangıca ve sonuca sahip olan bir olay niteliğinden ziyade devrimci değişimlerin bir kural haline dönüştüğü dinamik ve halen devam etmekte olan süreçleri ifade etmektedir.[150]

Bilgi ve İletişim Devrimleri ile Sanayi Devrimleri, her ne kadar kendine has fenomenleri ve sonuçları olan ayrı gelişmeler olarak ele alınsa da "Makine Çağı"nın icatlarıyla ivme kazanarak uluslararası ekonomik bağlamda "Büyük İşletmeler" ile

---

[146] Graciela Chichilnisky, "The Knowledge Revolution", *Journal of International Trade & Economic Development*, Cilt 7, Sayı 1, 1998, s. 40.

[147] Sanayi Devrimi/Endüstri Devrimi (*Industrial Revolution*) terimi, ilk olarak 18. yüzyıl sonları ve 19. yüzyılın ilk çeyreğindeki endüstriyel değişimleri tanımlamak amacıyla kullanılmıştır. 1840'larda İngiltere'de yoğun şekilde kullanılan bu kavram, 19. yüzyıl başında ulusların derin bir ekonomik ve sosyal dönüşüm yaşadıklarını öne süren Fransız yorumcular arasında da yoğun ilgi görmüştür. Literatürde ise bu terimin kullanımına ilk olarak John Stuart Mill ve Karl Marx'ın çalışmalarında rastlanıldığı belirtilse de terimin kurucu babasının Arnold J. Toynbee olduğu görüşü ağırlık kazanmaktadır. Detaylı bilgi için bkz.: Arnold Toynbee, *Lectures on the Industrial Revolution of the 18th Century in England: Popular Adresses, Notes and Other Fragments*, 4. Basım, Longmans, Green and Co., Londra 1894.; Arnold Joseph Toynbee, *A Study of History*, 15. Basım, Oxford University Press, New York 1961, ss. 3-6.; Anna Bezanson, "The Early Use of the Term Industrial Revolution", *The Quarterly Journal of Economics*, Cilt 36, Sayı 2, Şubat 1922, ss. 343-344.; Pat Hudson, *The Industrial Revolution*, Hodder Arnold, New York 1992, s. 11.

[148] Bilgi ve İletişim Devrimi gelişmelerinin karşılıklı tamamlayıcı etkisi de dikkate alındığında Sanayi Devriminin kademeli ilerleyiş, geçiş ve dönüşümler silsilesinde oluşan dinamik bir süreç olduğu tespit edilmiştir. Dolayısıyla bu çalışmada "Sanayi Devrimi" yerine "Sanayi Devrimleri" teriminin kullanılmasının daha yerinde olacağı düşünülmüş ve "Sanayi Devrimleri"nin aşamaları olarak ise literatürde yaygınlık kazanmış olan "Endüstri 1.0", "Endüstri 2.0", "Endüstri 3.0" ve "Endüstri 4.0" terimleri tercih edilmiştir.

[149] Paul Kennedy, *Büyük Güçlerin Yükseliş ve Çöküşleri: 16. Yüzyıldan Günümüze Ekonomik Değişim ve Askeri Çatışmalar*, Çeviren: Birtane Karanakçı, 10. Basım, Türkiye İş Bankası Kültür Yayınları, İstanbul 2005, s. 186.

[150] Eric John Ernest Hobsbawm, *Devrim Çağı: Avrupa 1789-1848*, Çeviren: Bahadır Sina Şener, 3. Basım, Dost Kitabevi, Ankara 2003, s. 38.

doğrudan ilişkilendirilebilir hale gelmeleri sebebiyle karşılıklı tamamlayıcı nitelik taşımaktadırlar. Fabrika sistemi ve sanayi sermayesi ile emeğin yükselişi hakkındaki genellemeler, telgraf, telefon ve uydu teknolojilerinin de dahliyle sınırları daha bulanık ve karmaşık bir yapıya evrilmiştir.[151] Sanayi Devrimleri, güç ve ölçek parametrelerini dönüştürerek fiziksel bağlamda doğal kaynaklara erişimi vurgulayan bir doğrultuda uluslararası ilişkileri, ekonomiyi ve aktörler arası savaş anlayışını belirlemiştir. Bilgi ve İletişim Devrimleri ise fiziksel kaynaklar açısından ters etkiye sahip olmakla birlikte özü itibariyle ilişkileri değiştirme ve zaman-mekân sınırlarını bulanıklaştırarak yeniden çizme ya da silme kapasitesini öne çıkarmaktadır.[152] Bu karmaşık ve tamamlayıcı etkileşimin daha iyi anlaşılabilmesi adına Sanayi Devrimlerinin değişim aşamalarına göre teknik ve Uluslararası İlişkiler perspektifinde derinleştirilmesi isabetli olacaktır.

3.1. Endüstri 1.0

18. yüzyıl öncesindeki dünyanın en gelişmiş ekonomilerinin yapısı, klasik el ve tezgâh üretimi ile tarıma dayalı büyük bir iş gücünün birleşimini içermektedir. El işçiliğine dayalı üretim anlayışı, köylülerden oluşan çeşitli büyüklüklerdeki grupların hasat dönemi ya da yol yapımı gibi yoğun iş gücü gereken işlerde belirli işlemlerin birleşmesini sağlamıştır. Kimi toplumlarda ise köylülerin yanı sıra köle grupları da üretim safhasında yoğunlukla kullanılmıştır. Örneğin; teknolojik değişim yaşanmadan önce ABD'de şeker ve tütün gibi temel tarımsal ürünlerin ticari üretimi için çoğunlukla köleler kullanılmıştır. Çin, Japonya, Hindistan, Orta Doğu, Kuzey Afrika ve Batı Avrupa'da çeşitli topluluklar lüks kumaş, metalurji, demir ve demir ürünleri gibi sofistike zanaat becerisi gerektiren alanlarda önemli beceriler geliştirmişlerdir.[153] Napolyon sonrası dönemde ortaya çıkan uluslararası sistemin bir dizi alışılmadık özelliğinden en dikkat çekicisi, modern çağın da kalıcı özelliklerinden biri olan entegre bir global ekonominin gelişmesi olmuştur. Dünya üzerindeki çok sayıdaki bölgeyi Batı Avrupa ve özellikle Büyük Britanya üzerinde

[151] Robert G. Albion, "The Communication Revolution", *The American Historical Review*, Cilt 37, Sayı 4, Temmuz 1932, s. 718.
[152] Jessica T. Mathews, "The Information Revolution", *Foreign Policy*, Sayı 119, Yaz 2000, s. 63.
[153] Peter N. Stearns, *The Industrial Revolution in World History*, 4. Basım, Westview Press, Philadelphia 2013, s. 21.

odaklayan bu ekonomi, kıtalarötesi ticaret ve maliye ağını yaratmıştır. İngiliz ekonomik hegemonyasının kurulduğu bu yıllarda ulaşım ve iletişim alanında geniş ölçekli yenilikler ortaya çıkmış, sanayi teknolojisinin aktarımı hızlanmış, imalat veriminde atılımlar gerçekleştirilmiş ve tarıma elverişli yeni toprakların ve yeni hammadde kaynaklarının yaratılması teşvik edilmiştir.[154]

Sanayi Devrimlerinin ilk büyük dalgası Büyük Britanya'da gerçekleşmiştir. Daha başarılı olduğu düşünülen diğer Sanayi Devrimi dalgalarının karakteristiği olan devlet yardımının bu ilk dalgada olmayışı ve kendiliğinden meydana gelmesi konuya yönelik özel bir ilgi uyandırmaktadır. Endüstrileşmenin İngilizler tarafından tecrübe edilmesinin tam olarak ne zaman gerçekleştiği tartışmalı olsa da ilk ekonomik tarihçilerden Arnold Toynbee'ye[155] göre bu süreç spesifik bir devrim olarak addedilmiş ve Endüstri 1.0'ın doğuşu "buhar makinesinin"[156] icadıyla sembolleştirilmiştir. 1740-1750 yılları arasında taş kömürü kullanılarak eritmenin yapıldığı demir endüstrisi ise, 1788 yılından itibaren buhar motorunun yüksek fırınlara uygulanmasıyla büyük bir değişim yaşamıştır. Toynbee'nin ifadesiyle; bilgi tabanlı gelişmelerle çözülmeye başlayan klasik endüstriyel yaşamın çerçevesi, buhar makinesinin el emeğini makineleştiren bu doğrudan ve yoğun etkisiyle parçalarına ayrılmıştır.[157]

---

[154] Paul Kennedy, *a.g.e.*, s. 185.

[155] Arnold Toynbee ile Arnold Joseph Toynbee genellikle karıştırılmaktadır. Arnold Toynbee (1852-1883) ilk ekonomik tarihçilerden kabul edilmektedir. Arnold Joseph Toynbee (1889-1975) ise Arnold Toynbee'nin yeğeni olup Siyasi Tarih alanında son derece önemli bir isim olarak görülmektedir.

[156] Uygulanabilir ilk kömür destekli buhar pompası, 1698 yılında Thomas Savery (1650-1715) tarafından yapılmıştır. "Madenci dostu" olarak bilinen bu aygıt, buhar basıncını kullanarak suyun pratikte 9-10 metre yukarıya çıkarılabilmesini sağlamıştır. Yüksek ve büyük yüzeylere monte edilebilen ilk buhar motoru pompası ise Thomas Newcomen (1663-1729) tarafından tasarlanmış ve 1712 yılında ilk kez bir kömür madenine kurulmuştur. Büyük bir pompalama kapasitesine sahip bu alet, buhar basıncını kullanarak suyun 50 metreden fazla yükseğe çıkmasını sağlamış ve madencilik endüstrisi açısından son derece önemli hale gelmiştir. Newcomen motoruna ayrı bir kondansatör ekleyerek endüstriyel anlamda istenilen yüksek verimliliğe getiren isim ise James Watt (1736-1819) olmuştur. 1769 yılında James Watt tarafından patenti alınan buhar makinesi, 1785 yılında bir pamuk fabrikasında kullanılmaya başlanmış ve böylelikle fabrika sistemine ilk adım atılmıştır. Detaylı bilgi için bkz.: Brian Spear, "James Watt: The Steam Engine and The Commercialization of Patents", *World Patent Information*, Cilt 30, Sayı 1, Mart 2008, ss. 54-55.; Orson Desaix Munn, S.U. Wales & A.E. Beach, "Centenary of the Steam Engine: James Watt", *Scientific American*, Cilt 20, Sayı 19, Mayıs 1869, ss. 297-298.; "The First Steam Engine: James Watt", *Scientific American*, Cilt 6, Sayı 6, Ekim 1850, s. 45.

[157] Arnold Toynbee, *Lectures on the Industrial Revolution …,* s. 226.

Tablo-3: İngiliz Sanayileşmesi Sırasında Ekonomik Büyüme Yönleri

	1780	1820	1870	1913
GSYİH	15,2	29,6	95,6	214,5
GSYİH / Kişi	1787	2099	3263	5032
GSYİH Büyüme Oranı	1	1,9	2,4	1,4
Toplam Faktör Verimlilik Büyüme Oranı	0,05	0,4	0,75	0,45
Doğuşta Beklenen Yaşam Süresi	34,7	39,2	41,3	53,4
Yetişkin Okur Yazarlığı	50	54	76	96
Yatırım / GSYİH	6	8,3	8,7	8,7
Tarımsal İstihdam Payı	45	35	22,7	11,8
ABD / Birleşik Krallık Üretim Verimliliği	-	1,49	2,04	2,13

Kaynak: Nicholas Crafts, "Forging Ahead and Falling Behind: The Rise and Relative Decline of the First Industrial Nation", *The Journal of Economic Perspectives*, Cilt 12, Sayı 2, Bahar 1998, s. 195.

Sanayi Devrimlerinin Büyük Britanya'daki ilk dalgasının genel görüntüsünü sakin ve istikrarlı ekonomik büyüme hali oluşturmuştur. Tablo 3'de de görüldüğü üzere; Büyük Britanya'nın gerçek gayri safi yurtiçi hâsıla (GSYİH) büyüme eğilimi, 1780 sonrasında olağanüstü bir hızdan ziyade oldukça sakin ve istikrarlı bir şekilde ivme göstermiştir. Her ne kadar üretim yöntemlerinin dönüştürüldüğü sektörlerde – pamuklu tekstil ürünleri gibi– çıktı artışı önemli seviyelere çıkmış olsa da, bunlar oldukça yavaş büyüme gösteren geleneksel ekonomik faaliyetleri içeren toplam ekonominin nispeten küçük bir alt kümesine karşılık gelmiştir.[158] Buna göre Endüstri 1.0; yavaş büyüme, hızlı nüfus artışı ve büyük yapısal değişimin kendine özgü bir karışımı olarak nitelendirilebilmektedir. Büyüme ve değişimdeki bu yavaşlığın tekrarlayan teması, ilk sanayi ülkesindeki sanayileşmenin zayıflığını ve kırılganlığını ön plana çıkarmaktadır. 1840'lara kadar İngiltere'nin istihdam yapısının, endüstriyel faaliyetlerinin çoğunun küçük ölçekli kaldığı, buhar gücünün kullanımından efektif

[158] Nicholas Crafts, "Forging Ahead and Falling Behind: The Rise and Relative Decline of the First Industrial Nation", *The Journal of Economic Perspectives*, Cilt 12, Sayı 2, Bahar 1998, s. 194.

anlamda az etkilendiği ve yüksek verimlilik ya da karşılaştırmalı üstünlük ile karakterize edilemediği görülmüştür. 1760-1830 arası dönem, yenilikçiliğin yaygınlığından ziyade yapısal değişimin büyük ölçüde tarım kabiliyetinden kaynaklandığı bir süreç olarak ifade edilmektedir.[159]

Endüstri 1.0'ın bu yavaş büyüme seviyesinden dolayı endüstriyel bir devrim etiketini hak edip etmediğine yönelik tartışmaların aksine Crafts'a göre bu sürecin "devrimselliği" iki anlamda oldukça önemlidir: İlk olarak yaşanan bu teknolojik değişim, benzeri görülmemiş şekilde ekonominin yükselen popülasyonun herhangi bir büyümeyle eşleştiği ya da geride bıraktığı Malthusian[160] perspektiften kaçmasını sağlayarak kişi başına düşen GSYİH büyümesini önlemiştir. 1700'den önceki birkaç yüzyıl boyunca yıllık %0,5'ten fazla olan nüfus artışı, gerçek ücret oranlarının her zaman düşmesine neden olmuştur. Buna karşın, Endüstri 1.0 sürecinde Birleşik Krallık, nüfus artışını yılda %1,5 oranına kadar kaldırabilir hale gelmiştir. İkinci olarak ise, İngiliz ekonomisinin istihdamda belirgin ve hızlı bir yapısal değişim geçirmesi, diğer gelişmiş ülkelere göre nispeten daha fazla şehirleşmiş ve sanayileşmiş iş gücüne yol açmıştır.[161]

Netice olarak bu dönemde ekonominin temel karakteri, toprak ve nüfus dengesinin hâkimiyetinden teknolojik değişim ve sermaye birikimi tarafından yönetilenlere kaymıştır. Endüstri teknolojisindeki devrim niteliğindeki değişiklikler yaygın olmamakla birlikte verimliliğe yönelik iyileştirmeler, 19. yüzyılın ikinci çeyreğinden önce GSYİH'nin büyümesine ılımlı bir şekilde katkıda bulunmuş ve muhtemelen yılda yaklaşık %0,33 oranında milli gelir artışına neden olmuştur. Şüphesiz yaşanan bu endüstriyel değişim; sosyal yapıyı, demografik davranışı ve tasarruf alışkanlıklarını değiştirmeye yardımcı olmuş ve bu değişimlere paralel

---

[159] Julian Hoppit, "Counting The Industrial Revolution", *Economic History Review*, Cilt 43, Sayı 2, Mayıs 1990, s. 175.

[160] Malthus Nüfus Teorisi: Salgın, doğal afet vs. gibi kısıtlayıcı etkenlerin olmadığı uygun şartlara sahip herhangi bir popülasyon, her yirmi beş yılda bir katlanarak yani geometrik dizi (1, 2, 4, 8, 16, 32, ….) şeklinde artarken, besin/gıda miktarının üretim artışının ise aritmetik dizi (1, 2, 3, 4, 5, ….) şeklinde olduğu ileri sürülmektedir. Buna göre zaman içerisinde kişi başına düşen besin/gıda miktarı azalmakta ve oluşan bu fark nüfus içerisinde yaşanan eksilmelerle (ölümlerle) doğa tarafından dengelenmektedir. Detaylı bilgi için bkz.: Thomas Robert Malthus, *An Essay On The Principle of Population; or, A View of Its Past and Present Effects On Human Happiness; With An Inquiry Into Our Prospects Respecting The Future Removal or Mitigation of The Evils Which It Occasions*, Cilt 1, 5. Basım, John Murray, Albemarle-Street, Londra 1817, *https://archive.org/details/essayonprinciple01maltuoft*, (Erişim Tarihi: 14 Mart 2019), ss. 1-16.

[161] Nicholas Crafts, "Forging Ahead…", s. 195.

olarak büyümenin teşvik edilmesini sağlamıştır. Bununla birlikte İngiliz büyümesinin üretimdeki yeniliklerin bir sonucu olarak olağanüstü bir sıçrama gerçekleştirdiği görüşünün bu dönem adına sürdürülmesi çok uygun düşmemektedir.[162] Buna karşın, Sanayi Devrimleri öncesindeki ekonomik büyüme yapısıyla kıyas yapıldığında, büyük ölçüde ticaret, daha verimli piyasalar ve kaynakların iyileştirilmiş tahsisiyle büyümenin yönlendirildiği görülürken, modern çağdaki büyümenin yapısının Aydınlanma döneminden edinilmiş bilimsel ve teknolojik bilginin genişletilerek "faydalı bilgiye" dönüştürülmesine dayandığı görülmektedir.[163] Bunun üzerine ise daha iyi bir ekonomi politikası desteklenerek, mevcut sistem içerisindeki teşvik yapılarının iyileştirilmesiyle beraber faydalı bilgi üretimi hem daha elverişli hale getirilmiş hem de erişim maliyetlerinde önemli düşüşler yaşanmıştır.[164] Üretkenlik artışının sürdürülebilir şekilde hızlandırılması, yeni teknolojilerin geliştirilmesi ve ardından yapılan iyileştirmelere yeni enerji türevlerinin eklenmesiyle farklı bir boyuta geçmiştir.

3.2. Endüstri 2.0

Uluslararası ekonominin gelişimi, Sanayi Devrimlerinin serbestlik kazandırdığı verimli güçler, kara ve deniz teknolojisinin geçirdiği modernizasyon aşaması, bölgesel ve kısa süreli savaşlar gibi çeşitli etkenler, kimi Büyük Güçlere diğerlerine kıyasla daha fazla fayda sağlamıştır. Özellikle 1815 sonrası dönemdeki İngiltere, ekonomik ve jeopolitik eğilimlerinden dolayı diğer güçlere kıyasla en fazla faydayı elde etmiştir; ancak 1860'lı yıllardan itibaren ortaya çıkan bu İkinci Sanayi Devrimi dalgasıyla uluslararası arenadaki ekonomik ve siyasi güç dengesi yeniden değişim safhasına girmiştir.[165] 1870-1914 arası dönem, o dönemde icat edilen çok sayıda teknolojinin yaratmış olduğu sosyoekonomik yapı değişimi nedeniyle

---

[162] Nicholas Crafts & Charles Knickerbocker Harley, "Output Growth and the British Industrial Revolution: A Restatement of the Crafts-Harley View", *The Economic History Review*, Cilt 45, Sayı 4, Kasım 1992, ss. 704-705.
[163] Joel Mokyr, *A Culture of Growth: The Origins of the Modern Economy*, Princeton University Press, New Jersey 2017, s. 4.
[164] Nicholas Crafts, "Explaining the First Industrial Revolution: Two Views", *European Review of Economic History*, Cilt 15, Sayı 1, Nisan 2011, ss.163-164.
[165] Paul Kennedy, *a.g.e.*, s. 187.

genellikle "İkinci Sanayi Devrimi" ya da "Endüstri 2.0" olarak adlandırılmaktadır. Bu ikinci dalga sayesinde özellikle petrol türevlerine ve elektriğe dayalı yeni üretim teknolojilerinin hızla gelişiminin yaşandığı bir yüzyıl başlamıştır. Teknolojik değişim hızında yaşanan artış, saatlik üretim miktarına göre ölçülen üretim verimliliğinde daha hızlı büyüme ile karakterize edilen yeni bir ekonomiye geçişin yolunu açmıştır.[166] Kimi yorumlara göre ise sanayileşmedeki ikinci dalga, II. Dünya Savaşı sonrasına kadar sürmüş, Dünya Savaşları ve Büyük Bunalım da dâhil olmak üzere birçok önemli olayı içermiştir. Şüphesiz endüstriyel yapılar bunlardan etkilenmiş ve yapısal olarak yeniden tanımlanmışlardır. Öyle ki daha geniş perspektifte, uluslararası aşamada belirleyici bir kayma ve ileri sanayi ekonomilerine dâhil olanların yeniden tanımlanması 20. yüzyılda şekillenmiştir. 19. yüzyılın ortalarından itibaren Batı ekonomik gücü, yeni sanayi ülkelerinin dünya sanayi tarihinin şekillendirilmesine dâhil olmasıyla birlikte derinden sarsılmıştır.[167] Bu süreçte söz konusu ikinci dalgayı tanımlayan üç önemli gelişme şu şekilde belirtilmektedir: Batı dışında da sanayileşmenin başlaması, Batıdaki sanayi ekonomisinin yeniden tanımlanması ve uluslararası etkinin genel yoğunlaşmasıyla dünyanın endüstriyel olmayan bölgelerinin de sanayileşmeye katılımının artması. Almanya ve ABD de dâhil olmak üzere bazı Batı toplumları, bu dönemde temel dönüşümlerini aktif olarak tamamlamış, daha kentsel hale gelmiş ve kendi üretim güçlerini fabrika sistemine bağlı hale getirerek kurulu sanayi gücü olan İngiltere'ye yeni rekabet zorlukları yaratmışlardır.[168] Rusya'nın ve Japonya'nın 1880'lerde sanayileşmeye başlaması ise uluslararası diplomasiyi etkilemekle kalmamış, uluslararası ekonomik güç dengesi üzerinde derin etkiler yaratmıştır. Bu bağlamda Sanayi Devrimlerinin ikinci dalgasının odak noktasını, söz konusu iki kilit ulusun dönüşümü oluşturmuştur. 1950'lere dek bu iki devletin devrimsel dönüşüm aşamaları tamamlanmış; ancak Batının mevcut sanayi gücü henüz yakalanamamıştır. Daha öncesinde ABD ve Almanya'nın geçirmiş olduğu süreçler de dikkate alındığında, Sanayi Devrimlerinin

[166] Andrew Atkeson & Patrick J. Kehoe, "Modeling the Transition to a New Economy: Lessons from Two Technological Revolutions", *The American Economic Review*, Cilt 97, Sayı 1, Mart 2007, s. 64.
[167] Peter N. Stearns, *a.g.e.,* s. 120.
[168] *A.g.e.,* s. 109.

kilit özelliğinin sonradan sanayileşen toplumların yerleşik sanayi güçlerinden daha hızlı şekilde büyüme gösterebilmesi olduğu net olarak görülmektedir.[169]

İlk Sanayi Devrimi ve ondan önceki çoğu teknolojik gelişme, bilimsel temel açısından oldukça yetersiz olan dönemlerdir. Öyle ki bu durum, ilk endüstricilerin bilimle ve bilimin fayda sağlayabilecek pratikleriyle hiç ilgilenmedikleri anlamını doğurmamaktadır; sadece uygun koşulların oluşmasıyla birlikte Sanayi Devrimlerinin teknik yeniliklerinin ortaya çıkışı gereklilik olarak kendiliğinden belirecektir.[170] 1850'lere kadar mühendislik, tıp teknolojisi ve tarım, mevcut doğal süreçlerin içerisinde işe yaradığı bilinen uygulamalı bilgi organları şeklinde konumlandırılmıştır. İlgili süreçlerin neden ve nasıl çalıştıklarına dair temel bilgi alanı yetersiz kalmış, bu süreçlerin derinlemesine anlaşılabilmesi, açıklarının giderilmesi, kalitenin artırılması ve üretim süreçlerinin kullanıcı dostu haline getirilmesi oldukça zor aksiyonlar olarak kabul edilmiştir. 1859-1873 yılları arasındaki dönem, tarihin en yoğun ve verimli inovasyonlarının gerçekleştirildiği süreçlerden biri olarak dikkat çekmiş ve 1870 sonrasındaki teknolojik yeniliklerde, önceki dönemdekilere kıyasla "faydalı/yararlı bilgi" (*useful knowledge*)[171] esasına dayalı sistemik ve disipline olmuş bilimsel temelli yeni teknolojiler ön plana çıkmıştır. İkinci Sanayi Devrimi, bu bilgi formları arasındaki –bilim ve teknoloji–

---

[169] *A.g.e.*, ss. 111-112.

[170] Eric John Ernest Hobsbawm, *a.g.e.*, s. 40.

[171] "Faydalı/Yararlı bilgi (*useful knowledge*)" nosyonu, Joel Mokyr tarafından öne çıkarılmaktadır. Buna göre yeni bilimsel görüşler, yeni tekniklerin icadı ve bunların üretim süreçlerine başarılı şekilde uygulanmaları, insanlık nüfusunun oldukça küçük bir bölümünün eylemlerinin sonucu gerçekleşmiştir. İnsanlar ile fiziksel çevreleri arasındaki etkileşimin; doğa olayları, kuralları ve düzenleri üzerinden anlamlandırılması, elde edilen anlayışın doğrudan ve efektif olarak üretime yansıtılması, insan kitlelerinin maddi refahının sürekli iyileştirilebileceği inancını doğurmaktadır. Bilgi, uzun zamandır ciddi kamu yararı özelliklerine sahip alışılmadık bir meta şeklinde anlaşılmaktadır. Başkalarının onu kullanmasını engellemek oldukça zor olmakla birlikte bilgi paylaşımının bilgi sahibine maliyeti ihmal edilebilir boyutlarda olabilmektedir. Ekonomistler bilginin kronik olarak yetersiz üretilme eğiliminde olduğundan şüphelenmişler, buna gerekçe olarak ise kaynakları, zamanı ve çabayı harcayanların herhangi bir getiriyi elde etme konusunda yaşadıkları zorlukları ileri sürmüşlerdir. Buna karşın, entelektüel tarih ile bilim ve teknoloji tarihinden elde edilen materyallerin üretim tekniklerinde yarattığı gelişmeler ve yenilikler sayesinde ekonomik büyümenin ve ilerlemenin ana motoru "faydalı/yararlı bilgi" olmuştur. Bilim ve teknolojinin Sanayi Devrimlerindeki tam rolü hala tartışılmakla beraber ekonomik büyüme hızlandıkça, bilim ve teknolojiden gelen girdilerin giderek arttığı ve özellikle 1830'lu yılların sonrasında bir anlamda baskın motivasyon gücü haline dönüştüğü şüphesizdir. Detaylı bilgi için bkz.: Joel Mokyr, *A Culture of Growth: The Origins of the Modern Economy*, Princeton University Press, New Jersey 2017, ss. 142-164.

karşılıklı geri bildirimlerin hızlandırılmasını sağlamıştır.[172] İkinci sanayileşme dalgasının etkisel kökeni, karşılık gelen eylemleriyle birlikte gelişen üç ayrı fikir zinciriyle ifade edilmektedir: İlk olarak muhasebe anlayışının dönüşümü dikkat çekici olmuştur. Salt geçmiş işlemlerin kaydı olmaktan çıkan muhasebe, iş insanlarının faaliyetlerinde tercih ettikleri politikalara yardımcı olmak için tasarlanmış uygulamalı bir bilime dönüşmüş ve fabrika maliyetlerini efektif olarak hesaplanabilir hale getirmiştir. İkinci olarak ise köprü, gemi, kazan ve diğer büyük ölçekli teknik işlerin yapımında güvenliğin sağlanması ve uygun ekonomik yöntemin kullanılması için saf bilim sonuçlarını uygulayan mühendisler, temel kuralları ya da deneme-yanılma yöntemlerini kesinliğe dayalı hesaplamalara ve ölçümlere dönüştürmüşlerdir. Son olarak da üreticiler ve gittikçe genişleyen pazarlar sayesinde ticari rekabet hız kazanmıştır. Bu rekabete bağlı olarak fiyatların düşmesi neticesinde seri üretim[173], maliyet düşürme yöntemleri içerisinde başarılı bir araç halini almıştır. Bazı endüstrilerde –dikiş ipliği, kâğıt, bisküvi vb. yapımında olduğu gibi– seri üretim, sürekli üretime katılarak "sürekli seri üretime" dönüşmüştür.[174]

Diğer taraftan bu dönemde ulaşım ve enerji kaynakları bağlamında önemli gelişmeler yaşanmıştır. Ulaşıma bakıldığında, 1850 yılına kadar demiryollarının genişlemesi endüstriyel ihtiyaçlardan kaynaklanmış ve hızla yayılmıştır. 1850 yılında İngiltere'de 10.715 km, Almanya'da 6.080 km ve Fransa'da 3.174 km demiryolu olduğu tespit edilmiştir. Sonrasında yolcu taşımacılığı karlı bir iş haline dönüşmüş ve demiryolu seyahati popüler hale gelmiştir. Özellikle 1830'lu ve 1840'lı yıllarda demiryolu ağlarının genişlemesinin ekonomik etkisi çok büyük olmuştur. Ucuz nakliye ve düşük fiyatlar talebin artmasına ve yerel tekellerin kırılmasına yol açmıştır.[175] 1850 sonrasında ise demiryolları daha hızlı, daha güvenli ve daha konforlu hale getirilmiştir. Bu süreç içerisinde sürekliliği olmayan tek değişiklik, demiryollarında yeni güç kaynaklarının kullanımı olmuştur. Dizel motor ve

---

[172] Joel Mokyr, *The Lever of Riches: Technological Creativity and Economic Progress*, 1. Basım, Oxford University Press, New York 1990, s. 245.

[173] Yalnızca özel aletlerin veya makine ayarlamalarının kullanıldığı ve bir defada aynı üründen çok sayıda yapılması anlamına gelmektedir.

[174] H. Stanley Jevons, "The Second Industrial Revolution", *The Economic Journal*, Cilt 41, Sayı 161, Mart 1931, ss. 1-2.

[175] Teun Koetsier, *The Ascent of GIM, the Global Intelligent Mechine: A History of Production and Information Machines*, Springer, Cham 2019, ss. 211-212.

sonrasında da elektrikli lokomotif kullanımı başlamıştır. Elektriğin endüstriyel hayata girmesi, ikinci sanayi dalgasının en önemli yeniliklerindendir. 1870'lerden itibaren elektriğin kullanımı hızlı bir şekilde gelişmiştir. 1879'da Berlin Fuarında minyatür bir elektrikli demiryolu sergilenmiş, 1883'te Viyana Sanayi Fuarında elektrikli battaniyeler ve elektrikli ocaklar tanıtılmış, 1884 yılına gelindiğinde ise Frankfurt ve Glaskow'da elektrikli tramvaylar çalışır hale gelmiştir. 1890 yılında elektriğin kullanımına dair tespit edilen esas teknik sorunlar çözülmüş ve elektrik enerjisi doğrudan kullanılabilir hale gelmiştir. Ardından elektrik kullanımına dayanan, güvenilirliği ve dayanıklılığı artırıp, maliyeti düşüren bir dizi mikro icat süreci başlamıştır. 1900 yılında akkor ampulun maliyeti yirmi yıl öncesine kıyasla beşte bir azaltılırken, verimliliği ise iki katına çıkarılmıştır; ancak fabrika sistemi içerisinde elektrik enerjisinin bir sanayi gücü formu olarak sağladığı avantajların farkına varılması aynı şekilde yavaş yavaş gerçekleşmiştir.[176]

Netice olarak Sanayi Devrimlerin ikinci dalgası, teşvik unsurunun etki alanını genişleterek önceki yüzyıllarda Avrupa'da biriken bilgilerin, bilimsel boyutlara ulaşarak teknolojik ilerlemelerin yaşanmasına ve bu ilerlemelerin uygulanabileceği kârlı fırsatlar yaratan piyasaların oluşmasına vesile olmuştur.[177] 1914 sonrasındaki dönemde yaşanan iki büyük savaş ve küresel ekonomik kriz, teknolojik ilerleme hızında yavaşlamaya neden olmuş, uluslararası konjonktürde aşılması gereken toplumsal ve yapısal çöküntü ortamına haiz olmuştur. II. Dünya Savaşı sonrasında ise toparlanma süreci başlamış ve Sanayi Devrimlerinin üçüncü dalgası ortaya çıkmıştır.

3.3. Endüstri 3.0

Sanayi Devrimlerinin üçüncü dalgası olan "Endüstri 3.0", önceki dalgalara kıyasla dünyanın değişim hızına hız katan gerçek bir küresel fenomen olarak kabul edilmektedir. Bu dalganın literatürdeki karşılığı olarak yoğunlukla kullanılan "Üçüncü Endüstri Devrimi" (*The Third Industrial Revolution,* TIR) kavramı iktisatçı

[176] Joel Mokyr, *a.g.m.*, s. 143.
[177] Daron Acemoğlu & James A. Robinson, *Ulusların Düşüşü: Güç, Zenginlik ve Yoksulluğun Kökenleri*, Çeviren: Faruk Rasim Velioğlu, 45. Basım, Doğan Kitap, İstanbul 2019, s. 101.

Jeremy Rifkin tarafından yaratılmış ve geliştirilmiştir.[178] İlk Sanayi Devrimi dalgası makineleşmeyi, merkezi fabrikaları ve endüstriyel kapitalistleri ortaya çıkarmış, amiral gemisi olarak tabir edilebilecek birincil aracı olan buharla çalışan motor geliştirilmiş ve bunun toplumsal yansıması ise emek ile sermaye arasında bölünme şeklinde gerçekleşmiştir. İkinci dalgayla otomasyon, bilimsel yönetim ve yönetim danışmanları ortaya çıkmış, konveyör bantı birincil araç haline gelmiş ve bunun sosyal yansımasında ise beyaz yakalı ile mavi yakalı işler arasında ayrım vuku bulmuştur. Söz konusu bu üçüncü dalga ile de makineler, İnternet'e bağlı uygun fiyatlı dijital üretim araçları haline gelmiştir. Böylelikle uygun fiyatlı araçlar büyük sermaye yatırımı gerektirmeksizin emek-sermaye bölünmesine köprü olurken, dijital araçlar da tasarım ve üretimi birbirine bağlayarak beyaz yakalı işler ile mavi yakalı işler arasında köprü olmuştur.[179]

1914-1945 arasındaki küresel ihtilaf hali, sanayi ekonomilerindeki araştırma ve geliştirme (Ar-Ge)[180] yapısını değiştirerek global anlamda bilimsel yönlendiriciliğin Batı Avrupa kanadındaki unsurlarının da ABD'ye kaymasını neden olmuştur. Özellikle 1945 sonrası yaşanan teknolojik gelişmeler, 1970'lerden itibaren şeklini almaya başlayacak bu üçüncü dalganın altyapısını oluşturmuştur. Örneğin; 1947 yılında AT&T Bell Laboratuvarlarında çalışan araştırmacıların ilk transistörü[181] geliştirmesiyle birlikte ileri teknoloji dijital bilgisayarların üretiminin yolu açılmıştır. Pratik anlamda bilinen tüm modern elektroniğin ve seri üretimin kolaylaşmasının

---

[178] Detaylı bilgi için bkz.: Jeremy Rifkin, *The Third Industrial Revolution: How Lateral Power is Transforming Energy, The Economy, and The World*, Palgrave Macmillian, New York 2013.

[179] Peter Troxler, "Making the Third Industrial Revolution: The Struggle for Polycentric Structures and a New Peer-Production Commons in the FabLab Community", *FabLab of Machines, Makers and Inventions*, Editörler: Julia Walter-Herrmann & Corinne Büching, Transcript Publishers, Bielefeld 2013, s. 182.

[180] Ekonomik Kalkınma ve İşbirliği Örgütü (OECD)'nün tanımına göre "Araştırma ve Geliştirme (Ar-Ge) (*Research and Development, R&D*)", bilgi birikimini –insan, kültür ve toplum bilgisi dâhil olmak üzere– artırmayı ve bu bilgi birikiminin yeni uygulamalar geliştirmek için kullanılmasını sağlamak amacıyla sistematik şekilde yürütülen yaratıcı çalışmaları içermektedir. Ar-Ge; temel araştırma, uygulamalı araştırma ve deneysel gelişim olmak üzere üç ana aktiviteyi kapsamaktadır. Detaylı bilgi için bkz.: OECD, *OECD Factbook 2013: Economic, Environmental and Social Statistics*, OECD Publishing, Paris 2012, s. 150.

[181] Transistörün geliştirilmesi, teknolojide birçok yeni ilerlemeyi potansiyel olarak mümkün kılmıştır. Baş ilgi alanlarına sahip yarı iletkenler –germanyum ve silikon– yalıtkanlar açısından en iyi şekilde anlaşılabilmektedir. Bundan dolayı belirtilen yarı iletkenlerin birleştirilmesiyle oluşturulmuştur ve teknolojik ilerlemenin atlama noktası olarak kabul edilmektedirler. Transistörler, devre içerisinde anahtarlama veya zayıf sinyalleri güçlendirme işlevi gören temel devre elemanlarıdır. Detaylı bilgi için bkz.: William Shockley, "Transistor Physics", *American Scientist*, Cilt 42, Sayı 1, Ocak 1954, ss. 41-42.

anahtar unsurunu oluşturan transistör, küresel teknolojik değişim üzerinde katalizör etkisinde bulunmuştur.[182] 1950'lerden itibaren Bilgi ve İletişim Teknolojileri (BİT) ve biyomedikal biliminde yaşanan yeniliklerle birlikte yeni endüstriler hızla büyümeye başlamıştır. Küresel ticaret ve yatırım akışları yeniden canlanırken, uluslararası teknoloji akışları da genişlemiş ve 1980-1990 arası Japonya, Güney Kore ve Tayvan gibi ekonomiler endüstriyel yenilik kaynakları olarak ortaya çıkmaya başlamıştır. Bu tarz ekonomik bölgelerde devletler, kendi ulusal inovasyon sistemlerinin içerisinde özellikle sanayide Ar-Ge çalışmalarının doğrudan desteklenmesi ve bilgi yoğunluklu sanayi ürünlerinin tedarik süreçlerinde kolaylaştırılarak hızlandırılması bağlamında birincil aktör pozisyonunda yer almışlardır.[183] Öyle ki, yeni teknolojilerin sanayi ekonomilerinde benimsenmesi oldukça yavaş gerçekleşmektedir. Yeni fikirlerin somut bağlamda ilk vücut bulmaları hata yoğunluklu olmaları nedeniyle genellikle pahalı kabul edilmektedir. Yatırımlara özgü teknolojik ilerlemelerin gelir ve üretkenlik üzerindeki etkisinin birbiriyle ilişkili iki faktör tarafından düzenlenmesi muhtemeldir: Ekonomik yapıların ve etkenlerin yeni teknolojiyi öğrenmesi ne kadar pahalı olursa, teknolojinin yayılması da o kadar yavaş olmaktadır; ancak yeni teknoloji, bir ekonomi içerisinde ne kadar hızlı benimsenir ve yayılırsa, onun öğrenilmesi de o kadar kolaylaşmaktadır. Dolayısıyla yeni teknolojik bilgilerin benimsenme maliyeti ile benimsenme kapsamı arasında bir geri bildirim döngüsü bulunmaktadır. Yeni teknoloji, geçmiş teknolojilerin geliştirilmesinden ziyade radikal bir ayrımı temsil ediyorsa, toplumların onunla ilgili bilgisi başlangıçta oldukça sınırlı kalabilmektedir. Fakat bu yeni teknolojinin kullanımı yaygınlaştıkça, toplumların onunla olan deneyimleri artar ve dolayısıyla teknolojinin kümülatif oranda verimliliği de yükselmektedir.[184] Christopher Freeman'ın ifadesiyle "tekno-ekonomik paradigma" (*techno-economic paradigm*), teknik olarak uygulanabilir yeniliklerin kombinasyonları arasından bir ekonomik seçim süreci anlamına gelmektedir ve gerçekten de yeni bir paradigmanın belirginleşmesi ve sistem üzerinde yayılması oldukça uzun süreleri bulmaktadır. Bu

[182] *Flashes Magazine*, "The Third Industrial Revolution", Sayı 34, Ekim 2017, s. 54.
[183] David C. Mowery, "*Plus ca change*: Industrial R&D in the 'Third Industrial Revolution'", *Industrial and Corporate Change*, Cilt 18, Sayı 1, Şubat 2009, s. 7.
[184] Jeremy Greenwood, "The Third Industrial Revolution: Technology, Productivity, and Income Inequality", *Economic Review*, Cilt 35, Sayı 2, Bahar 1999, s. 8.

yayılma, kurumsal yeniliklerin son derece önemli olduğu teknolojik, ekonomik ve politik güçler arasında karmaşık bir etkileşimi içermektedir.[185] Buhar gücünün ve elektrik gücünün yayılması, bu derin dönüşümün en net örnekleridir. Aynı şekilde elektronik bilgisayar sistemleri ile ilgili yenilikler de bu şekilde değerlendirilmelidir.

Diğer taraftan Sanayi Devrimlerinin bu üçüncü dalgasının aynı zamanda "Bilgi Çağının Başlangıcı" şeklinde addeden görüşler bulunmaktadır. Buna göre bilgi işlem ve iletişim, aynı zamanda kuvvet çarpanlarıdır ve üretim adına otomasyonun yaptığı hizmetleri yapmaktadır. İnsanın kas gücünden ziyade beyin gücünü artırmakta, mevcut endüstrilerdeki verimlilik kazancını sürdürerek yenilerini oluşturabilmekte ve mevcut işlerin daha hızlı yapılabilmesini sağlayarak yeni işler için olanak yaratabilmektedirler. Tıpkı bir dizi teknolojik gelişmenin, geçen uzun sürelerin neticesinde bir araya gelmesiyle gerçek etkilerinin hissedilebildiği ilk iki Sanayi Devrimi dalgasında olduğu gibi, dijital bilgi işleminin icadı da kendi başına yeterli olmamış, bilgisayar sistemlerinin ağlarla ve sonuçta tüm ağların ağı olan İnternet ile birleştirildiğinde dönüştürücü kültürel ve ekonomik etkileri hissedilebilir olmuştur.[186] Kısacası 1950'lerden itibaren hızlanan BİT yenilikleri, 1969 yılında beş şirketin –*Bedford Associates; General Motors Hydra-matic Division, Ypsilanti, MI Plant; International Instruments Inc.* (3I); *Digital Equipment Corporation* (DEC); *Struthers-Dunn Systems Division in Bettendorf,* IA.– öncülüğünde ilk programlanabilir mantık devrelerinin (*programmable logic controllers*, PLCs) geliştirilmesiyle küresel sistemi total olarak etkileyebilecek devrimsel seviyeye ulaşmıştır. Bu devreler sayesinde girilen bilgiler, yazılan programa göre işlenerek iş elemanlarına aktarılabilir hale gelmiştir. 1970'lerde önce mikro bilgisayarların, ardından da kişisel bilgiyarların geliştirilmesi ve bu devrelerin endüstrilerde uygulanabilir hale gelmesiyle birlikte de üretim sistemlerinin otomasyonu sağlanmıştır.[187] 1990'lardan itibaren de İnternet ve *World Wide Web*'in (WEB) geliştirilmesiyle küresel bağlılık güçlenerek derinleşmiştir. Anderson'a göre Endüstri 3.0, en iyi olarak dijital üretim ile kişisel üretimin birleşimi şeklinde görülmektedir.

---

[185] Christopher Freeman, "New Technology and Catching Up", *Technology and Development in the Third Industrial Revolution*, Editörler: Charles Cooper & Raphael Kaplinsky, Frank Cass, Londra 2005, s. 87.
[186] Chris Anderson, *Makers: The New Industrial Revolution*, Crown Business, New York 2012, s. 40.
[187] Ken Ball, "How Programmable Emerged From", *Control Engineering*, Eylül 2008, ss. 66-67.

Eşya üretiminin dijitalleşmesi, mevcut üretimin daha verimli kılınmasından daha fazlası anlamına gelmektedir. Ayrıca mevcut üreticilere ek olarak sıradan insanları girişimci haline getirerek üretici popülâsyonunun genişlemesi sağlanmaktadır.[188]

Diğer taraftan Rifkin'e göre ise üreticiler ile dijital üretim, Endüstri 3.0'ın nedenlerinden ziyade etkilerinden biri olarak kabul edilmektedir. Endüstri 3.0, önceki Sanayi Devrimlerinde olduğu gibi iletişim altyapısı ve enerji üretimindeki değişikliklerle –19. yüzyıldaki matbaanın icadı ve buhar gücü teknolojisinin geliştirilmesi, 20. yüzyıldaki elektrikli iletişim araçları (radyo, TV) ve çoğunlukla fosil yakıtlardan üretilen elektrik enerjisi– tetiklenmiştir. 21. yüzyıl ise Rifkin tarafından fosil yakıtlara dayanan endüstriyel çağın sonu olarak tanımlanmaktadır.[189] Fosil yakıtların kıt kaynak olma özelliğinden kaynaklı ekonomik krizlerin yanı sıra 19. ve 20. yüzyıllardaki Sanayi Devrimlerinde atmosfere yayılan yüksek miktardaki karbondioksit (CO2) miktarları küresel iklim değişikliği gibi yeni kriz türlerinin artacağını göstermektedir. Bundan dolayı Tablo 4'te de sunulduğu üzere karbon bazlı enerji kaynaklarından yenilenebilir enerji kaynaklarına geçiş, 21. yüzyılın temel karakteristiği olacaktır.

Tablo-4: Sanayi Devrimleri ve Sürücüleri (*Drivers*): İletişim ve Enerji Kaynakları

I.DEVRİM	II.DEVRİM	III.DEVRİM
19. Yüzyıl	**20. Yüzyıl**	**21. Yüzyıl**
Matbaa	**Radyo & TV**	**İnternet**
Kömür & Buhar	**Petrol & Elektrik**	**Yenilenebilir Enerjiler**

Kaynak: Peter Troxler, "Making the Third Industrial Revolution: The Struggle for Polycentric Structures and a New Peer-Production Commons in the FabLab Community", *FabLab of Machines, Makers and Inventions*, Editörler: Julia Walter-Herrmann & Corinne Büching, Transcript Publishers, Bielefeld 2013, s. 183.

[188] Chris Anderson, *a.g.e.*, s. 41.

[189] Justin Gerdes, "Jeremy Rifkin: Energizing the Third Industrial Revolution", *Siemens Living Energy: The Magazine for International Energy Leadership*, Sayı 8, Temmuz 2013, s. 10.

Öte taraftan Rifkin, 1990'ların ortalarından itibaren yenilenebilir enerjiler ile BİT arasında gelişen sinerji sayesinde dünyayı değiştirebilecek yepyeni güçlü bir ekonomik altyapının 21. yüzyılda netlik kazandığını belirtmektedir. Öyle ki bu yüzyıl, milyonlarca insanın kendi yeşil enerjisini kendi evlerinden, ofislerinden ya da fabrikalarından üretebileceği ve bir "enerji interneti" (*energy Internet*) üzerinden birbirleriyle paylaşabileceği çağ olacaktır. Enerjinin bu şekilde demokratikleşmesi ise insan ve devlet ilişkilerinde son derece önemli bir yeniden düzenleme yaratarak, küresel ekonomik ilişkilerden toplumların şekillendirilmesine kadar çok yönlü etkiler yaratabilecektir.[190]

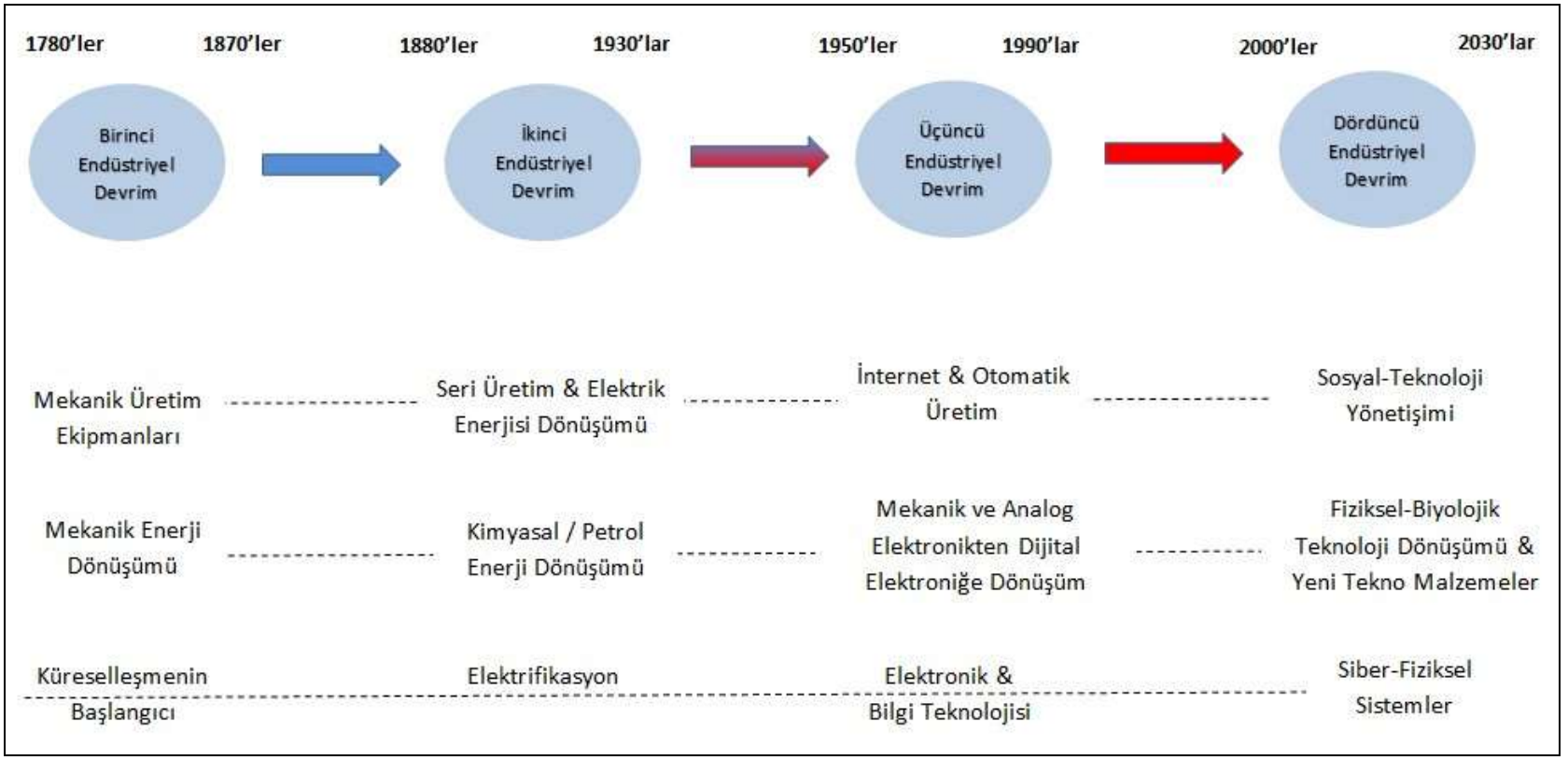
3.4. Endüstri 4.0

Yaklaşık olarak 1760-1840 yılları arasında ortaya çıkan ilk Sanayi Devrimi dalgası, demiryollarının inşası ve buhar makinesinin icadıyla tetiklenerek mekanik üretime geçişin önünü açmış, 19. yüzyılın sonlarıyla beraber 20. yüzyılın başlarında başlayan İkinci Sanayi Devrimi dalgası ise elektriğin ve montaj hattının geliştirilmesiyle birlikte seri üretimi mümkün kılmıştır. Özellikle 1960'lardan itibaren ortaya çıkan Üçüncü Sanayi Devrimi dalgası, "bilgisayar devrimi" ya da "dijital devrim" gibi çeşitli adlandırmalara tabi olmuş ve 1950'lerin ortalarından 1970'lerin başlarına kadar mikro-elektronik ve yarı iletkenlerdeki gelişmelerle ortaya çıkmıştır. Bu gelişmeler sayesinde ilk çok büyük ölçekli entegrasyon (*very large-scale integration,* VLSI) süreçlerinin binlerce transistorü tek bir çipte birleştirerek entegre devreler (*integrated circuits,* IC) yarattığı görülmüştür. Ortaya çıkan bu entegre devreler, mekanik ve analog teknolojiden dijital elektroniklere geçişi hızlandırmış ve esasen bilginin sayısallaştırılmasını ve yaygın bilgisayar kullanım kültürünü değiştirmiştir. Öte yandan telekomünikasyon alanındaki gelişmeler, 1990'lı yılların başında İnternet'in başlamasına ve sonraki on yılda küresel veri merkezleri ile arama motorlarının, çevrimiçi pazarların, sosyal medya ve mobil cihazların ortaya çıkmasına zemin hazırlamış, dünyanın ve endüstrilerin her köşesine yayılmasına vesile olmuştur.[191]

---

[190] Jeremy Rifkin, *The Third Industrial Revolution: How Lateral Power is Transforming Energy, The Economy, and The World*, Palgrave Macmillian, New York 2013, s. 2.
[191] Mark Skilton & Felix Hovsepian, a.g.e., s. 8.

Tablo-5: Sanayi Devrimlerinin Etkileri



Kaynak: Mark Skilton & Felix Hovsepian, *The 4th Industrial Revolution: Responding to the Impact of Artificial Intelligence on Business*, Palgrave Macmillan, Cham 2018, s. 6.

"Endüstri 4.0" terimi, Dünya Ekonomik Forumu'nun (*World Economic Forum,* WEF) kurucusu ve başkanı olan Alman Klaus Schwab tarafından ortaya atılmıştır. Schwab'a göre Endüstri 4.0, bu yüzyılın başında dijital devrime dayanarak başlamıştır. Çok daha yaygın ve mobil bir İnternet ağı, daha ucuz hale gelen daha küçük ve daha güçlü yapay sensörler, yapay zekâ ve makine öğrenimi ile karakterize edilmektedir. Çekirdeklerinde bilgisayar donanımı, yazılımı ve ağları olan dijital teknolojiler şüphesiz yepyeni gelişmeler değildir ancak Üçüncü Sanayi Devrimi dalgasına paralel olarak, daha karmaşık ve bütünleşik hale gelmiş ve bunun neticesinde de toplumları ve küresel ekonomiyi dönüştürücü boyutlara ulaşmıştır.[192]

"Endüstri 4.0" süreci, ilk olarak Avrupa'da başlatılmış ve Alman hükümet programlarıyla birlikte Siemens, Bosch gibi önde gelen Alman şirketleri tarafından desteklenmiştir.[193] ABD'de bu yaklaşım genellikle "Akıllı Üretim" (*Smart Manufacturing*) şeklinde adlandırılırken, Çin'de "Çin Yapımı 2025" (*Made in China 2025*) ve Japonya'da ise "İnovasyon 25" (*Innovation 25*) konseptleri üzerinden tartışılmaktadır.[194] Dördüncü Sanayi Devrimi dalgası, sadece akıllı ve entegre makineler ve sistemler ile ilgili değildir. Kapsamı çok daha geniş olan bu dalganın, gen diziliminden nanoteknolojiye, yenilenebilir enerjiden kuantum hesaplamaya kadar birçok alanda eş zamanlı atılımlar yarattığı görülmektedir. Schwab'a göre ortaya çıkan teknolojiler ve geniş tabanlı inovasyon, dünyanın bazı bölgelerinde hala yeni yeni çıkmaya devam eden öncekilere kıyasla çok daha hızlı ve geniş kapsamlı yayılmaktadır. Öyle ki; İkinci Sanayi Devrimi, dünyanın yaklaşık %17'sinde (yaklaşık 1.3 milyar insan) elektriğe erişim olmadığı için henüz tam olarak yaşanmamıştır. Bu durum benzer şekilde Üçüncü Sanayi Devrimi için de geçerlidir ve gelişmekte olan ülkelerde yaşayan ve İnternet erişimi olmayan dünya nüfusunun yarısından fazlası (yaklaşık 4 milyar insan) henüz bu üçüncü dalgayı yaşamamaktadır. Yayılma hızının da geçmişe kıyasla çok fazla ilerlediğine dair verilen şu örnek ise oldukça dikkat çekicidir: İlk Sanayi Devrimi dalgasının ürünlerinden biri olan motor milinin (iğ/dingil) Avrupa dışına yayılması neredeyse

---

[192] Klaus Schwab, *The Fourth Industrial Revolution*, World Economic Forum, Cenevre 2016, ss. 11-12.

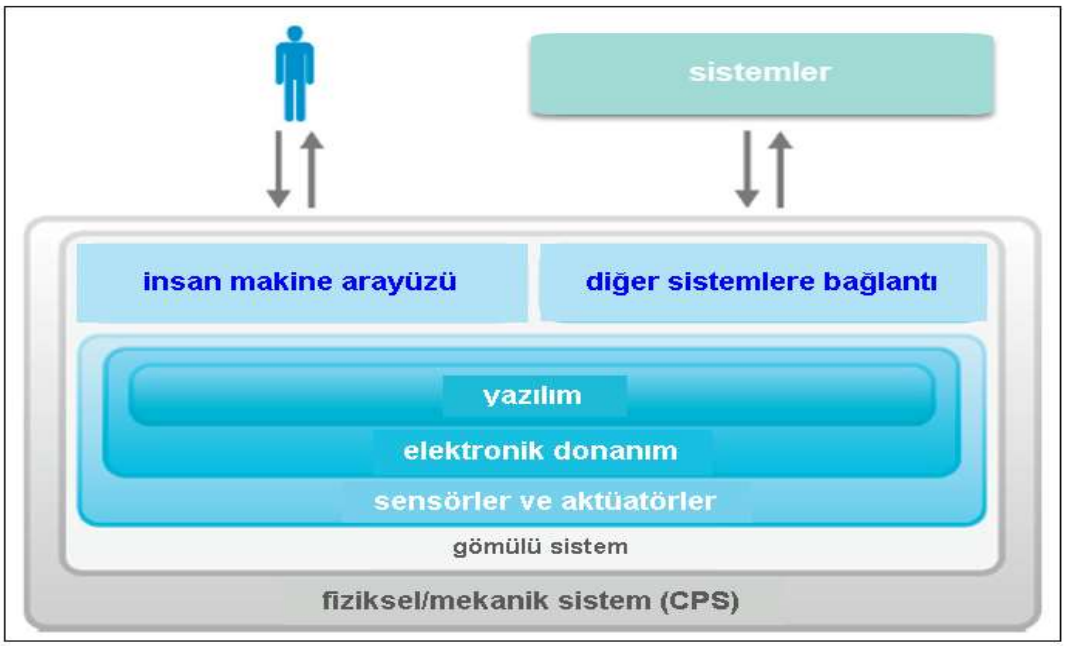
[193] Jennie S. Hwang, "The Fourth Industrial Revolution (Industry 4.0): Intelligent Manufacturing", *SMT (Surface Mount Technology) Magazine*, Temmuz 2016, s. 12.

[194] Alin Stăncioiu, "The Fourth Industrial Revolution 'Industry 4.0'", *Fiabilitate Şi Durabilitate,* Sayı 1, 2017, *s*. 74.

120 yıl sürmüşken, buna karşılık internet, on yıldan daha kısa bir sürede dünyanın genelinde erişilebilir hale gelmiştir.[195] Yani bir taraftan tüm Sanayi Devrimi dalgaları dünyanın her yerinde eş zamanlı tecrübe edilemezken, diğer taraftan her sürecin öne çıkan unsurunun yayılma hızı bir öncekilere kıyasla çok daha yüksek seviyelere ulaşmaktadır.

Endüstri 4.0 üzerine daha teknik yaklaşıldığında, bu sürecin mekanizasyon ve otomasyondaki artışlar, dijitalleşme, ağ oluşturma ve minyatürleşme gibi geniş bir kavram yelpazesini içerdiği görülmektedir.[196] Dahası Endüstri 4.0, fiziksel temel sistemlerin ve yazılım sistemlerinin diğer branşlar, ekonomik sektörler ve endüstri türleriyle entegrasyonunda dinamik değer yaratma ağlarının entegrasyonuna dayanmaktadır. Bundan dolayı araştırma ve inovasyon, referans mimarisi, standardizasyon ve ağ bağlantılı sistemlerin güvenliği, Endüstri 4.0 altyapısının uygulanabilmesi için temel unsurlardır.

Tablo-6: Siber-Fiziksel Sistemlerde İnsan ve Makine Etkileşim Modellemesi



Kaynak: László Monostori, "Cyber-Physical Production Systems: Roots, Expectations, and R&D Challenges", *Procedia CIRP*, Cilt 17, 2014, s. 11.

[195] Klaus Schwab, *a.g.e.*, ss. 12-13.
[196] Heiner Lasi, Peter Fettke, Thomas Fed & Michael Hoffman, "Industry 4.0", *Business & Information Systems Engineering*, Cilt 6, Sayı 4, 2014, s. 239.

Siber-fiziksel sistemler –sensörler, makineler, işyerleri, iletişim ağları vb.– olarak adlandırılan bu sistemler ile sistemler arası koordinasyon, İnternet tabanlı protokol ve standartlarla sağlanmaktadır.[197] Tablo 6'da görüldüğü üzere siber-fiziksel üretim sistemleri (*Cyber-Physical Production Systems,* CPPS); insanlar, makineler ve ürünler arasında iletişimi mümkün kılmakta ve destekleyebilmektedir. Siber-fiziksel üretim sistemlerinin unsurları veri toplayabilmekte ve bunları işleyebilmekte, belirli görevleri kendi kendine kontrol edebilmekte ve arayüzlerle insanlarla etkileşime geçebilmektedir.[198] Herhangi bir siber-fiziksel sistem; entegre hesaplama, ağ ve fiziksel süreçleri olan herhangi bir şey olabilmektedir. Bir insan üzerinden modellendirildiğinde, herhangi bir insan operatörü siber-fiziksel bir sistem olarak fiziksel ve siber bileşenlere sahiptir ve akıllı bir fabrikadır. Bu örneğe göre operatörün hesaplama yetisi olan bir beyni vardır ve insan makine arayüzü (*human machine interface*) aracılığıyla diğer insanlarla ve sistemle iletişim kurar ve çevrelerini etkilemek için mekanik arayüzlerle yani elleriyle etkileşime girerler. Tıpkı bu örnekte olduğu gibi siber-fiziksel sistemler de bilgisayarların ve yazılımların sanal dijital dünyasının fiziksel analog dünyası ile süreç yönetimi ve geri bildirim kontrolü gibi etkileşimlerle birleşmesini sağlayarak nesnelerin, verilerin ve hizmetlerin İnterneti[199] olmasına yol açmaktadır. Diğer taraftan makinelerin, bileşenlerle ve bazen de yapım sürecindeki ürünlerle iletişim kurarak birçok iş

---

[197] Ceren Salkin, Mahir Öner, Alp Üstündağ & Emre Çevikcan, "A Conceptual Framework for Industry 4.0", *Industry 4.0: Managing The Digital Transformation*, Editörler: Alp Üstündağ & Emre Çevikcan, Springer, Cham 2018, ss. 4-5.

[198] László Monostori, *a.g.m.*, s. 11.

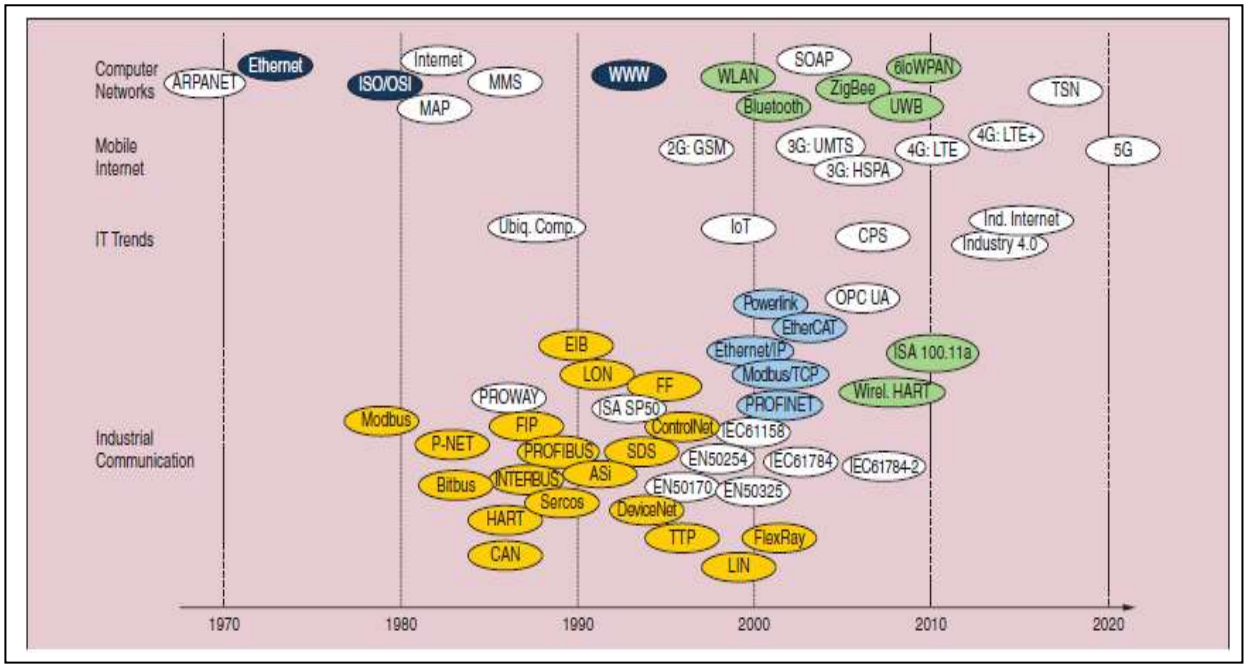
[199] "Nesnelerin İnterneti (*Internet of Things,* IoT)", kimi kaynaklarda "Endüstriyel İnternet (*Industrial Internet*)", "Her Şeyin İnterneti (*Internet of Everything*)" şeklinde görülebilmekle birlikte çoğunlukla "Nesnelerin İnterneti (*Internet of Things,* IoT)" ya da "Nesnelerin Endüstriyel İnterneti (*Industrial Internet of Things,* IIoT)" kullanımı tercih edilmektedir. IoT / IIoT, ağ bağlantısı kapsamındaki fiziksel cihazların birbiriyle iletişim kurabildiği ve uygulama sürecinin yürütülmesinde uzaktan kontrolün mümkün olabildiği bir sistem olarak tanımlanmaktadır. Enerji üretiminden tarıma, sağlıktan ulaştırmaya, lojistikten havacılığa kadar çok farklı sektörlerde uygulanabilen IoT / IIoT üzerine pek çok iş dünyası lideri, hükümet, akademisyen ve teknoloji satıcısı tarafından büyüme ve verimliliğin çok daha fazla artacağı yönünde büyük potansiyel barındırdığına dair öngörülerde bulunulmaktadır. Detaylı bilgi için bkz.: Alasdair Gilchrist, *Industry 4.0: The Industrial Internet of Things*, Apress Media, New York 2016, ss. 1-3.; Mehmet Soysal & Nurten Sinem Pamuk, "Yeni Sanayi Devrimi Endüstri 4.0 Üzerine Bir İnceleme", *Verimlilik Dergisi*, Sayı 1, 2018, s. 48.; Mehmet Özkan, Arzu Al & Serkan Yavuz, "Uluslararası Politik Ekonomi Açısından Dördüncü Sanayi-Endüstri Devrimi'nin Etkileri ve Türkiye", *Siyasal Bilimler Dergisi*, Cilt 1, Sayı 1, s. 12.

sürecini eş zamanlı gerçekleştirebildiği bir akıllı üretim hattı da endüstriyel açıdan verilebilecek bir başka örnektir.[200]

Yukarıda sunulan örneklerden görüleceği üzere Endüstri 4.0, diğer Sanayi Devrimi dalgalarına kıyasla çok yönlü, kapsamlı ve oldukça eklektik bir süreç olarak dikkat çekmektedir. Sürecin bu karmaşık yapısı, şüphesiz devletler arası ilişkilerde ve uluslararası güvenliğin doğası üzerinde derin etkiler yaratacaktır. Schwab'a göre küresel anlamda esas kritik tehlike, hiper seviyede bağlantılı hale gelen ve hızla yükselen bir eşitsizlik dünyasının çeşitli parçalanmalara, ayrışmalara ve toplumsal huzursuzluklara yol açabileceği ve bunun da şiddetli aşırılıkçılar için uygun şartlar yaratabileceği hususudur. Sanayi Devrimlerinin bu dördüncü dalgası, hem coğrafi dengeleri hem de devletten devlet dışı aktörlere doğru meydana gelen güç kaymalarını etkilerken, aynı zamanda da güvenlik algısını ve güvenlik tehditlerinin karakterini değiştirmektedir. Zaten daha da karmaşık bir hale gelen jeopolitik manzaranın içinde olası silahlı devlet dışı aktörlerin yükselişiyle karşı karşıya kalındığında, beraberindeki daha zorlu meydan okumalarda, kilit uluslararası güvenlik hususları etrafında işbirliği için ortak bir platform oluşturulması olasılığı giderek kritik hale gelmektedir.[201]

[200] Alasdair Gilchrist, *a.g.e.*, s. 36.
[201] Klaus Schwab, *a.g.e.*, ss. 76-77.

Tablo-7: Endüstriyel İletişim ve İlgili Teknoloji Alanlarının Gelişimindeki Kilometre Taşları



Kaynak: Martin Wollschlaeger, Thilo Sauter & Jürgen Jasperneite, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0", *IEEE Industrial Electronics Magazine*, Cilt 11, Sayı 1, Mart 2017, s. 19.

Bilgisayar ağları, mobil internet, Bilgi Teknolojileri trendleri ve endüstriyel iletişim teknolojilerindeki gelişmelerin kronolojik olarak gösterildiği Tablo 7, devletlerin ve devlet dışı aktörlerin ulusal ve uluslararası güvenliklerine yönelik olası tehditlerin türleri, türevleri, izleyeceği yöntem ve kanallar ile yaratabileceği zayiatların tahayyül edilebilmesi adına etkili bir çerçeve çizmektedir. 1970'lerde ARPANET ile başlayan süreç, 1980 sonrası İnterneti doğurmuş ve 1990 sonrasında İnternet *World Wide Web* (www) ile küresel kapsamda yayılmış ve yeni milenyumla birlikte Nesnelerin İnterneti (IoT) boyutunu alarak gündelik yaşamın bir parçası olaraka yaygın olarak kullanılmaya başlanmıştır. Bu süreçteki olağanüstü gelişmelerle birlikte yaşanan dönüşümler, sadece endüstrileri, imalat ve üretim yapılarıyla iş modellerini değil, devletler arası ilişki kültürünü, kamu yönetimlerini, sağlık hizmetlerini, çalışma koşullarını ve özlük haklarını derinden etkilemiştir. Böylelikle kaliteli altyapı hizmetlerinin sağlanması, geniş bant ağlarının geliştirilmesi, proaktif yaklaşımlar için

küçük işletmelerin teşvik edilmesi, Endüstri 4.0'ın benimsenmesi ya da güvenlik standartlarının sağlanması gibi önemli hususlarda devlet yönetimlerinden beklentilerin daha da fazla artmasına neden olmaktadır.[202]

Netice olarak son yıllarda giderek artan Nesnelerin İnterneti (IoT) ve Siber-Fiziksel Sistemler (CPS) konusundaki araştırma ve geliştirmelerle birlikte Endüstri 4.0'ın sağlayabileceği büyük fayda eğilimini fark ederek yararlanabilme gayesiyle devletler ve endüstri liderleri uluslararası çapta büyük yatırımlara yönelmişlerdir.[203] Devletlerin planları perspektifinden bakıldığında şu örnekler son derece dikkat çekicidir: ABD'nin 2011'de kabul ettiği "*Advanced Manufacturing Partnership* (AMP)"[204] başlıklı geleceğin üretim liderliğine yönelik öneri ve eylem raporu; Almanya'nın 2012 yılındaki IoT ve teknolojik aktiviteleri destekeleyen "*High-Tech Strategy 2020*"[205] eylem planı; Fransız hükümetinin 2013 yılındaki "*La Nouvelle France Industrielle*"[206] isimli Fransız endüstrisindeki politika önceliklerine yönelik stratejik değerlendirmesi; Birleşik Krallık'ın 2013 yılında sunduğu "*Future of Manufacturing*"[207] başlıklı 2050 yılına kadarki imalat sektöründeki gelişmelere yönelik öngörü çalışması; Avrupa Komisyonu'nun 2014 yılında "*Factories of the Future* (FoR)"[208] başlıklı yeni Kamu-Özel Sektör Ortaklığı sözleşmesi; Güney Kore'nin 2014 yılında "*Innovation in Manufacturing 3.0*"[209] ile Kore yerli

---

[202] Marta Götz & Barbara Jankowska, "Clusters and Industry 4.0: Do They Fit Together?", *European Planning Studies*, Cilt 25, Sayı 9, 2017, s. 1641.

[203] Yongxin Liao, Fernando Deschamps, Eduardo de Fritas Rocha Loures & Luiz Felipe Pierin Ramos, "Past, Present and Future of Industry 4.0: A Systemic Literature Review and Research Agenda Proposal", *International Journal of Production Research*, Cilt 55, Sayı 12, 2017, s. 3609.

[204] Office of Science and Technology Policy, Executive Office of the President, "Report To The President On Ensuring American Leadership In Advanced Manufacturing", Haziran 2011, *https://www.manufacturing.gov/sites/default/files/2018-01/pcast-advanced-manufacturing-june2011.pdf*, (Erişim Tarihi: 5 Temmuz 2019).

[205] Germany Trade & Invest (GTAI), "The High-Tech Strategy", *https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Why-germany/industrie-4-0-why-germany-policy,t=the-hightech-strategy,did=1798576.html*, (Erişim Tarihi: 5 Temmuz 2019).

[206] Ministry for the Economy and Finance, "New Industrial France: Building France's Industrial Future", *https://www.economie.gouv.fr/files/files/PDF/web-dp-indus-ang.pdf*, (Erişim Tarihi: 5 Temmuz 2019).

[207] Government Office for Science and Department for Business, Innovation & Skills, "Future of Manufacturing", *https://www.gov.uk/government/collections/future-of-manufacturing*, (Erişim Tarihi: 5 Temmuz 2019).

[208] European Factories of the Future Research Association (EFFRA), "Factories of the Future", *https://www.effra.eu/factories-future*, (Erişim Tarihi: 5 Temmuz 2019).

[209] Jung Suk-yee, "Innovation in Manufacturing 3.0 Stretegy Needs Better Focus with Clearer Direction", *BussinessKorea*, 19 Kasım 2015,

üretiminde ve inovasyonundaki yeni yol haritası; Çin hükümetinin 2015 yılında yayınladığı "*Made in China 2025*"[210] stratejisi ve "*Internet Plus*"[211] planı; Japon hükümetinin dünyada oluşmaya başlayan "Süper Akıllı Toplum"un liderliğini hedefleyerek 2016 yılında kabul ettiği "*5th Science and Technology Basic Plan*"[212]; Singapur hükümetinin 2016 yılında yaklaşık 16 milyar $ taahhüt ettiği "*RIE2020 Plan*"[213] isimli araştırma, yenilik ve girişim planı. Endüstri planları perspektifinden bakıldığında ise şu örnekler ön plana çıkmaktadır: 2014 yılında AT&T, Cisco, General Electric, IBM ve Intel tarafından endüstriyel internet teknolojilerine olanak sağlamak ve önceliklerini koordine etmek için "Endüstriyel İnternet Konsorsiyumu" (*Industrial Internet Consortium*, IIC) kurulmuştur. Ayrıca Siemens, Hitachi, Boschi Panasonic, Honeywell, Mitsubishi Electric, ABB, Schneider Electric ve Emerson Electric gibi diğer büyük firmalar da IoT ve CPS ile ilgili projelere büyük yatırımlar yapmışlar ve önemli işbirlikleri gerçekleştirmişlerdir.[214]

Sonuç olarak Endüstri 4.0'a geçiş, tüm Sanayi Devrimlerine eşlik eden niteliklerle doğrulanan yeni bir Sanayi Devrimi olarak kabul edilmektedir. Lojistik ve imal edilen ürünlerdeki derin değişiklikler ile sonuçlanan birikmiş endüstriyel inovasyonların ve endüstrideki sistemik dönüşümlerin toplu olarak uygulanmasının neticesi olarak da teknoloji tipinin değişimini içermektedir.

---

http://www.businesskorea.co.kr/news/articleView.html?idxno=13060, (Erişim Tarihi: 5 Temmuz 2019).

[210] The State Council of The People's Republic of China, "Made in China 2025", *http://english.gov.cn/2016special/madeinchina2025/*, (Erişim Tarihi: 5 Temmuz 2019).

[211] The State Council of The People's Republic of China, "Internet Plus", *http://english.gov.cn/2016special/internetplus/*, (Erişim Tarihi: 5 Temmuz 2019).

[212] Ministry of Education, Culture, Sports, Science and Technology-Japan, "Science and Technology Basic Plan", *http://www.mext.go.jp/en/policy/science_technology/lawandplan/title01/detail01/1375311.htm*, (Erişim Tarihi: 6 Temmuz 2019).

[213] National Research Foundation Prime Minister's Office Singapore, "RIE2020 Plan", *https://www.nrf.gov.sg/rie2020*, (Erişim Tarihi: 6 Temmuz 2019).

[214] Yongxin Liao vd., *a.g.m.*, s. 3610.

Tablo-8: Sanayi Devrimlerinin Temel Parametrelerinin Kıyaslanması

PARAMETRELER	Endüstri 1.0	Endüstri 2.0	Endüstri 3.0	Endüstri 4.0
Zaman Aralığı	**18. Yüzyıl - 19. Yüzyılın Başları**	**19. Yüzyılın Sonları - 20. Yüzyılın Başları**	**20. Yüzyılın İkinci Yarısı**	**21. Yüzyıl**
Birikmiş Endüstriyel Yenilikler	**Dökme demir, Buhar motorları ve Tekstil endüstrisi üretimi**	**Yüksek kalite çelik üretimi, Demiryolları, Elektrik ve Kimyasalların dağıtımı**	**Yenilenebilir enerji kaynakları, Dijital teknolojiler, İş süreçlerinin ağ organizasyonu**	**Nesnelerin İnterneti, Robotik süreç otomasyonları**
Teknolojik Biçim Türü	**Endüstriyel üretim**	**Konveyör üretim**	**Dijital teknolojiler tabanlı küresel üretim**	**Tam otomatik üretim**
Gerekli Yeni Altyapı	**Endüstriyel ekipman**	**Konveyör ekipmanları, Demiryolları**	**Dijital ekipman, Küresel altyapı**	**Yüksek hızlı İnternet, Robotik ekipmanlar**
Endüstrideki Sistemik Dönüşümlerin Mahiyeti	**Endüstriyel üretimin oluşumu**	**Konveyör üretimin oluşumu**	**Dijital teknolojiler tabanlı küresel üretimin oluşumu**	**Tam otomatik üretimin oluşumu**
Lojistikte Etkin Değişiklikler	**Buharlı taşımacılık**	**Demiryolu taşımacılığı**	**Elektrik enerjisi, hibrit ve diğer ulaşım araçları üreten binalar**	**Manipülatörler, Robototronik**
Ürünlerde Etkin Değişiklikler	**Dökme demir ürünler**	**Çelik ürünler**	**Bilgisayar ürünleri**	**Yeni inşaat malzemeleri**

Kaynak: Elena G. Popkova, Yulia V. Ragulina & Aleksei V. Bogoviz, "Fundamental Differences of Transition to Industry 4.0 From Previous Industrial Revolutions", *Industry 4.0: Industrial Revolution of the 21st Century*, Editörler: Elena G. Popkova, Yulia V. Ragulina & Aleksei V. Bogoviz, Springer International Publishing AG, Cham 2019, s. 24.

Nihayetinde Endüstri 4.0'ın diğer Sanayi Devrimlerine kıyasla daha önce çok sayıda görülmemiş özelliğe sahip olduğunu, yukarıda sunulan kıyaslamalı Tablo-8 üzerinden şu şekilde özetleyerek bu bölümün bitirilmesi isabetli olacaktır: Endüstriyel üretimin oluşumu, buhar gücünün ulaşım dâhil çok yönlü kullanılmaya başlanması ve dökme demir üretimine geçiş Endüstri 1.0'ın öne çıkan özellikleri olmuştur. Konveyör üretiminin oluşumu, demiryolu ulaşımının yayılması ve çelik üretimine geçiş Endüstri 2.0 temel özellikleri olmuştur. Dijital teknolojilere dayalı küresel üretimin oluşumu, elektrik enerjisi ve çeşitli yakıt türleriyle çalışan ulaşım aracı üreten fabrikaların kurulması ve bilgisayar üretiminin başlangıcı Endüstri 3.0'ın esasını oluşturmuştur. Son olarak da; tam otomatik üretimin oluşturulması, insanın üretim sürecinden elemine edilmesi, endüstriyel şirketlerin tüm iş süreçlerinde devrimsel değişikliklerin yaşanması, küreselleşmenin eş zamanlı kullanılması ve olumsuz sosyal sonuçların en aza indirilebilmesi ihtimalinin ortaya çıkması, endüstriyel patentlerin özünün değiştirilmesi ve endüstriyel üretimdeki uzmanlaşmalarda hızlı değişim imkanlarının oluşması Endüstri 4.0'ın karakterini oluşturmaktadır.[215]

4. Kuramsal Yaklaşım

II. Dünya Savaşı'nın sonra ermesiyle birlikte bağımsız bir disiplin olarak hem "Uluslararası İlişkiler" çalışmaları hem de "Gelecek Çalışmaları" (*Future Studies*) olarak adlandırılan bilimsel perspektife dayanan araştırma ve geliştirme alanı içerisindeki araştırmalar hız kazanmıştır. 1960'lara kadar akademilerde ve karar verme mekanizmalarında hâkim olan "savaş hali" ve "savaş ihtimali" konseptleri nedeniyle Realist teori dominantlığı görülmüştür. 1960-1970 arasında farklı Uluslararası İlişkiler yaklaşımları –Neo-Realizm, karar verme yaklaşımları, sistem yaklaşımları, davranışsal yaklaşımlar, ekolojik yaklaşımlar vs.– artış göstermiştir. 1970'ler Realizme meydan okuyan normatif ve kavramsal karşı argümanlarla şekillendirilmiş, 1980'ler ve 1990'lar boyunca ise Uluslararası İlişkiler teorileri, küreselleşme ve post-modernleşmenin sorunlarına yönelik kısmi cevap arayışındaki Liberal, Neo-Liberal, İnşacı, Feminist ve Çevreci yaklaşımların alternatif

[215] Elena G. Popkova vd., *a.g.m.*, s. 27.

argümanlarıyla zenginleştirilmiş, Normatif ve Eleştirel yaklaşımlar ise Uluslararası İlişkilerin kavramsal yönleriyle daha ilgili olmuştur.[216] Martin Hollis ve Steve Smith'in Uluslararası ilişkiler disiplininde her daim "iki tür hikâye" –uluslararası süreçlerin nedensel analiziyle uluslararası politikanın açıklanabilmesi ve uluslararası aktörlerin eylemlerinin anlamlarını ve nedenlerini araştırmak suretiyle uluslararası politikaların anlaşılabilmesi– olduğu yönündeki tespiti[217], sosyal dünyaya yönelik nedensel ve nedensel olmayan yaklaşımların temel ikiliğinin 1990'lardan itibaren Uluslararası İlişkiler disiplinine nüfuzunu artırmıştır.[218] Aynı zamanda 1990'lardan itibaren kullanımı yoğunlaşmaya başlayan "bilgi teknolojileri", "bilgi ekonomisi", bilgi toplumu", "Dijital Çağ" söylemleri, Paul Virilio'nun "*chrono-politics*"[219] olarak vurguladığı, rekabet sahalarının artık coğrafyadan ziyade elektronik içerisine girdiği ve bilgi ile iletişim hızlarının anlık seviyelere yükseldiği yepyeni bir uluslararası yapıyı[220] ve bu yapının nedensel-ereksel yaklaşımlar üzerinden açıklanabilme ve anlaşılabilme tartışmalarını beraberinde getirmiştir. Özellikle sosyal dünyanın teleolojik (ereksel) yaklaşımları, teknolojik ilerlemeye dair deterministik bakışlar, tarihsel süreç içerisindeki insan faktörünün belirleyiciliğinin seviyesi ve sosyal gelişmenin tarih dışı boyutuna yönelik karmaşık tartışmalar ve analizler, bilim ve teknolojinin bugünün sosyal dünyasında yeniden tespitini gerekli kılmıştır.[221] Yukarıda sunulan söylem örneklerinin ve analiz çeşitliliğinin artması, Uluslararası İlişkiler disiplininin bilim ve teknoloji sözlüğünü ve yaklaşımını zenginleştirerek diğer Sosyal Bilimlere kıyasla daha aykırı bir konuma taşımıştır. Bununla birlikte, onlarca yıldır yapılan yenilikçi araştırmalar sayesinde geniş bir bilgi birikimine sahip olunmuştur. İşte bu koşullar altında diğer disiplinlerden ampirik kavrayış ve teorik kavramlar dahil edilmesi son derece önemlidir. Ek olarak ise mevcut disiplin sınırlarının daha esnek hale getirilerek disiplinlerarası etkileşimlerin geliştirilmesi,

---

[216] Mert Bilgin, "The State of Future in International Relations", *Futures*, Cilt 82, Eylül 2016, s. 55.
[217] Martin Hollis & Steve Smith, *Explaining and Understanding International Relations*, Oxford University Press, 1. Basım, New York 1990, ss. 1-7.
[218] Milja Kurki, "Causes of a Divided Discipline: Rethinking the Concept of Cause in International Relations Theory", *Review of International Studies*, Cilt 32, Sayı 2, Nisan 2006, s. 189.
[219] Paul Virilio & Slyvere Lotringer, *Pure War: Twenty-Five Years Later*, Çeviren: Mark Polizzotti, Semiotext(e), Los Angeles 2007, s. 21.
[220] Paul Virilio, *Speed and Politics*, Çeviren: Marc Polizzotti, Semiotext(e), Los Angeles 2007, s. 7.
[221] Daniel R. McCarthy, "Technology and 'the International' or: How I LEarned to Stop Worrying and Love Determinism", *Millennium: Journal of International Studies*, Cilt 41, Sayı 3, ss. 470-471.

hem alt alanlara hem de Uluslararası İlişkiler disiplininin geneline önemli katkılar sağlamaktadır.[222] Geliştirilen ve ilerletilen bu disiplinlerarası etkileşimler ile Uluslararası İlişkiler disiplinini yalnızca ifade edildikleri sosyal ve kurumsal biçimlerle değil, bilimsel bilgi iddialarının içerikleriyle de ilgili kılmış ve disiplinin bilim ve teknoloji anlayışının hem analitik hem de teorik bağlamda derinleştirilmesi ve farklılaştırılması sağlanmıştır.[223] Bu bağlamda Uluslararası İlişkiler disiplininin tarihsel kökenini oluşturan Büyük Tartışmaların (*The Great Debates*) aralarında gelişen çeşitli yaklaşımlar ve teoriler sayesinde Uluslararası İlişkiler anlayışında kayda değer ilerlemeler yaşanmış ve farklı teorilerin zengin ekosistemi disipline edilmiştir.[224] Böylelikle Uluslararası İlişkiler alanındaki uygulayıcılar ile küresel bilim ve teknoloji politikasının akademik mensupları ve araştırmacılar, karşılıklı öğrenerek ve zengin bir tartışma geleneğine dayalı komşu disiplinler inşa ederek faydalanır hale gelmişlerdir.[225] Bu noktada böylesi eklektik ve karmaşık bir yapıda, bilimsel ve teknolojik ilerlemelerin Uluslararası İlişkiler üzerinde yarattığı etkilerin analizi ve gelecek öngörüleri adına geliştirilen ve literatürde oldukça yeni olan "Karmaşık Uluslararası İlişkiler Teorisinin" (*Complex International Relations Theory,* CIR*)* Büyük Tartışmalar üzerinden ortaya çıkışının ele alınarak detaylandırılması yerinde olacaktır.

4.1. Karmaşık Uluslararası İlişkiler Teorisinin Ortaya Çıkışı: Beşinci Büyük Tartışma

Uluslararası İlişkiler Teorisinin akademik bağlamı "Büyük Tartışmalar" (*The Great Debates*) olarak adlandırılan bir dizi ardışık tartışmaların tarihi olarak çerçevelenmektedir. Uluslararası İlişkilerin "Beşinci Büyük Tartışması" (*The Fifth Great Debate*), Prof. Dr. Emilian Kavalski tarafından 2000 sonrası Uluslararası

[222] Barry Buzan & Richard Little, "Why International Relations has Failed as an Intellectual Project and What to do About it", *Millennium: Journal of International Studies*, Cilt 30, Sayı 1, 2001, ss. 19-22.
[223] Andrew Barry, "The Translation Zone: Between Actor-Network Theory and International Relations", *Millennium: Journal International Studies*, Cilt 41, Sayı 3, 2013, s. 420.
[224] David A. Lake, "Theory is Dead, Long Live Theory: The End of the Great Debates and the Rise of Eclecticism in International Relations", *European Journal of International Relations*, Cilt 19, Sayı 3, s. 568.
[225] Maximilian Mayer, Mariana Carpes & Ruth Knoblich, "The Global Politics of Science and Technology: An Introduction", *The Global Politics of Science and Technology – Vol. 1: Concepts From International Relations and Other Disciplines*, Editörler: Maximilian Mayer, Mariana Carpes & Ruth Knoblich, Springer-Verlag, Berlin Heidelberg 2014, s. 18.

İlişkiler Teorisini anlamlandırabilmek adına geliştirilmiştir.[226] Literatürde oldukça yeni olmasına rağmen son derece ilgi çekmiş olan bu tartışma, "Karmaşıklık Teorisinin" "Karmaşık Uluslararası İlişkiler Teorisine" evrilmesi üzerinden sunulmuştur. Bu sürecin iyi anlaşılabilmesi adına Birinci Büyük Tartışmadan Beşinci Büyük Tartışmaya kadarki tüm Tartışmaların kısaca hatırlatılması isabetli olacaktır:

"Birinci Büyük Tartışma" (*The First Great Debate*) 1930'ların sonlarıyla 1940'ların başlarına denk gelmektedir. İdealistler (ya da Ütopikler) ile Realistler arasında gerçekleşmiştir. Bu dönemde reel dünyaya dair bir dizi olay –Japonya'nın Mançurya'yı istilası, İtalya'nın Etiyopya'yı işgali, Milletler Cemiyeti'nin başarısızlığı vs.– yaşanmıştır.[227] I. Dünya Savaşı sonrasından 1929 yılında başlayan Büyük Buhran'a kadarki dönem "İdealizm" üzerinden kritik edilmeye başlanmış ve Büyük Buhran neticesinde çözülmeye başlayan uluslararası ekonomik sistemin Büyük Savaşı kaybeden ülkelerde milliyetçilik duygusunu yoğunlaştırmasıyla uluslararası statükoyu değiştirme çabaları giderek artmış ve nihayetinde de oluşturulmaya çalışılan barış temalı uluslararası düzenin sarsılmasına neden olmuştur.[228] İki savaş arası dönemin "İdealistleri", tipik olarak dikkatlerini uluslararası siyasetin sert gerçeklerini analiz etmekten ziyade reformlara odaklayan bir grup pasifist, ahlakçı ve hukukçu olarak tasvir edilmiştir.[229] Edward Hallet Carr'ın 1939 yılında yayınlanan "Yirmi Yıllık Bunalım 1919-1939" (*The Twenty Years' Crisis 1919-1939*) isimli eseriyle İdealist (Ütopik)-Realist ayrımı netleştirilmiş, İdealistlerin var olan gerçekleri veya mevcut araçları eleştirel bir şekilde analiz etmek için çok az girişimde bulunduğu yönünde eleştirilerek Uluslararası İlişkiler disiplininin kurucu tartışması Realistler lehine yorumlanmıştır.[230]

---

[226] Emilian Kavalski, "The Fifth Debate and the Emergence of Complex International Relations Theory: Notes on the Application of Complexity Theory to the Study of International Life", *Cambridge Review of International Affairs*, Cilt 20, Sayı 3, 2007, ss. 435-454.

[227] Fahir H. Armaoğlu, *Siyasi Tarih (1789-1960)*, Sevinç Matbaası, Ankara 1964, ss. 548-626.

[228] Atila Eralp, "Uluslararası İlişkiler Disiplininin Oluşumu: İdealizm-Realizm Tartışması", *Devlet, Sistem ve Kimlik: Uluslararası İlişkilerde Temel Yaklaşımlar*, Editör: Atila Eralp, 9. Basım, İletişim Yayınları, İstanbul 2007, ss. 68-69.

[229] Brian C. Schmidt, "Introduction", *International Relations and The First Great Debate*, Editör: Brian C. Schmidt, Routledge, New York 2012, s. 4.

[230] Edward Hallet Carr, *The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations*, Macmillan & Co Ltd, Londra 1946, ss. 8-13.

"İkinci Büyük Tartışma" (*The Second Great Debate*), 1950'li ve 1960'lı yıllarda metodolojiyle ilgili olarak ortaya çıkmıştır. Tartışmanın tarafları olan Gelenekselciler ile Davranışsalcılar birbirinden açıkça çok farklı iki yaklaşımdır. Geleneksel yaklaşım, insan dünyasının karmaşıklığını kabul eden, Uluslararası İlişkileri insan dünyasının bir parçası olarak gören ve içine girerek insancıl bir şekilde anlamaya çalışan bütünsel bir yaklaşımdır. Bundan dolayı Uluslararası İlişkiler, insancıl bir konudur ve kesinlikle bilimsel ya da dar bir teknik kapsama indirgenemez.[231] Davranışsalcılar ise insanlara ait sosyal dünyayı ve Uluslararası İlişkileri bilimsel kanunlara göre ampirik modeller ve teoriler üzerinden formüle etmeye çalışmaktadır. Fiziksel olan ile insani olan arasında doğrulama ve iletişim ihtiyacına ilişkin bir ayrım olmamakla birlikte toplumsal norm ve değerler ile bilimsel bilgi arasında bir odaklanma ayrımı söz konusudur.[232] Gelenekselci teorisyenler için "kavrayış" önemliyken, Davranışsalcılar açısından "açıklama" esastır.[233] Bu İkinci Büyük Tartışmanın galibi olmamakla birlikte her bir yaklaşım, diğerine bilgilendirici ve zenginleştirici etkilerde bulunmuş ve her yaklaşımdaki endemik fazlalıkların kontrol edilebilmesine vesile olmuştur.[234] Öte yandan Davranışsalcılığın Uluslararası İlişkiler üzerinde kalıcı bir etkisi olmuş ve Davranışsalcı metotlardan yoğun şekilde etkilenen Realizm ve Liberalizmin yeni formülasyonlarına yol açmıştır. Bu yeni formülasyonlar –Neo-Realizm ve Neo-Liberalizm– ise yeni tarihsel ve metodolojik koşullar altında ilk ana tartışmanın tekrarlanmasına yol açmıştır.[235]

Diğer taraftan "Üçüncü Büyük Tartışma" (*The Third Great Debate*) ile "Dördüncü Büyük Tartışma" (*The Fourth Great Debate*) oldukça tartışmalıdır. Üçüncü Büyük Tartışmanın odak noktası epistemoloji olmakla beraber bu tartışmayı popüler kılan Yosef Lapid'e göre tarih ile bilimin karşılaştırmalarında zorlukla

---

[231] Robert Jackson & Georg Sørensen, *Introduction to International Relations: Theories and Approaches*, 5. Basım, Oxford University Press, Oxford 2013, ss. 44-45.
[232] Morton A. Kaplan, "The New Great Debate: Traditionalism vs. Science in International Relations", *World Politics*, Cilt 19, Sayı 1, Ekim 1966, s. 4.
[233] Martin Hollis & Steve Smith, *a.g.e.*, s. 1.
[234] Richard B. Finnegan, "International Relations: The Disputed Search for Method", *The Review of Politics*, Cilt 34, Sayı 1, Ocak 1972, s. 64.
[235] Robert Jackson & Georg Sørensen, *a.g.e.*, ss. 45-46.

sarsılan pozitivist epistemolojik uzlaşı haline bu tartışmayla son verilmiştir.[236] İkinci Büyük Tartışmada dar bir şekilde tanımlanmış metodoloji argümanlarıyla meşgul olunmasına rağmen Üçüncü Büyük Tartışmanın tipik olarak Uluslararası İlişkiler alanındaki bilginin doğası ve ilerlemesi hakkındaki öncü fikirleri kolaylaştırması beklenmiştir. Hatta bu tartışmayla birlikte Uluslararası İlişkiler Teorisinin yeniden yapılandırma sürecinin başladığı iddia edilmiştir.[237] 1980'lerde ana akım Uluslararası İlişkiler Teorilerine yönelik eleştirel yansımaların ortaya çıkmasıyla Pozitivistler ile Post-Pozitivistler arasındaki meta-teorik sorunlar Üçüncü Büyük Tartışmanın özünü oluşturmuştur. Genel olarak sosyal bilimlerdeki ampirik-pozitivist ortodoksiden uzaklaşma eğilimiyle birlikte ortaya çıkan Pozitivizm-Post-Pozitivizm tartışması, Uluslararası İlişkiler camiasında bilimsel çabaların epistomolojik ve ontolojik temellerinin eleştirel olarak yeniden incelenmesine neden olmuştur.[238] 1990'lardan itibaren İnşacılığın klasik anlayıştan koparak "orta yol" söylemine dönüşmesi "Dördüncü Büyük Tartışmanın" altyapısını oluşturmuştur. Buna göre Uluslararası İlişkiler içerisinde artan "inşacı dönüş" söylemi[239], Üçüncü Büyük Tartışma aracılığıyla orta yol temelli bir uzlaşı inşa çabasına dönüşmüştür.[240] Öncesinde Robert O. Keohane tarafından yapılan Rasyonalizm-Reflektivizm ayrımı[241], sonrasında Pozitivizm-Post-Pozitivizm ayrımına evrilmiştir. Daha çok sosyal ve maddesel yeteneklere odaklanan ontolojik yaklaşımı kapsayan bu tartışma, nedensel ve inşacı kavrayış ve açıklamayı karşı karşıya getirmektedir. Bu tartışma sayesinde hem daha çok felsefi mesele ana akıma dâhil edilmiş, hem "egemenlik" tarzı

---

[236] Yosef Lapid, "The Third Debate: On the Prospects of International Relations Theory in a Post-Positivist Era", *International Studies Quarterly*, Cilt 33, Sayı 3, Eylül 1989, s. 238.
[237] Mark Hoffman, "Conversations on Critical International Relations Theory", *Millennium: Journal of International Studies*, Cilt 17, Sayı 1, 1988, s. 91.
[238] Tanja E. Aalberts & Rens van Munster, "From Wendt to Kuhn: Reviving the 'Third Debate' in International Relations", *International Politics*, Cilt 45, Sayı 6, Ağustos 2008, s. 723.
[239] Jeffrey T. Checkel, "Review: The Constructivist Turn in International Relations Theory", *World Politics*, Cilt 50, Sayı 2, Ocak 1998, ss. 324-328.
[240] Alexander Wendt, *Social Theory of International Politics*, 1. Basım, (Virtual Publishing, 2003), Cambridge University Press, New York 1999, ss. 39-40.
[241] Robert O. Keohane, "International Institutions: Two Approaches", *International Studies Quarterly*, Cilt 32, Sayı 4, Aralık 1988, ss. 386-393.

konularda taraflar arasında yakınsama yaratılmış, hem de taraflar içerisinde marjinalleşmeler oluşmuştur.[242]

[242] Ole Wæver, "Figures of International Thought: Introducing Persons Instead of Paradigms", *The Future of International Relations: Masters in the Making?*, Editörler: Iver B. Neumann & Ole Wæver, Routledge, Londra 2005, ss. 23-24.

Tablo-9: Uluslararası İlişkilerde Büyük Tartışmalar

Çerçeve	Birinci Büyük Tartışma	İkinci Büyük Tartışma	Üçüncü Büyük Tartışma	Dördüncü Büyük Tartışma	Beşinci Büyük Tartışma
Zaman	1920'ler-1930'lar	1950'ler-1960'lar	1980'ler	1990'lar	2001 - *
Paradigma	İdealizm vs Realizm	Bilimsel Davranışçılık vs Gelenekçilik	Post-Pozitivizm vs Pozitivizm	İnşacılık vs Rasyonalizm vs Reflektivist	Doğrusallık vs Doğrusal olmama
Odak Noktası	Kurumlar vs Çıkarlar	Bilim vs Tarih	Epistemoloji: Pozitivizm vs Post-Pozitivizm / Eleştirel Teori	Ontoloji: Sosyal Yetenekler vs Maddi Yetenekler	Epistemoloji ve Ontoloji: Açıklamaya ve/veya Kavrayışa Yönelik Refleksif Biyolojik Dönüşün Reddi vs Kabulü
Yenilik	Devlet Sistemi vs Devletler Toplumu	Davranışsal Açıklama	Açıklama vs Kavrayış	Nedensel Açıklama ve/veya Kavrayış vs Kurucu Açıklama ve/veya Kavrayış	Birbiriyle Bağlantılı Olma (İlişkisellik) vs İnsani ve İnsani Olmayan Sistemlerin Ayrımı

* 2001 yılı, 9/11 Terör Olaylarıyla birlikte bilim adamlarının, karar vericilerin ve çeşitli toplumların karmaşıklığın gerçeğiyle yüzleştikleri bir olay ve zaman dilimi olmasıyla sebebiyle sembolik olarak başlangıç tarihi olarak kabul edilmiştir.

Kaynak: Emilian Kavalski, "The Fifth Debate and the Emergence of Complex International Relations Theory: Notes on the Application of Complexity Theory to the Study of International Life", *Cambridge Review of International Affairs*, Cilt 20, Sayı 3, 2007, s. 445.

"Beşinci Büyük Tartışma" (*The Fifth Great Debate*) ise literatürde şu an için tanımlanması en zor olandır çünkü kaynak altyapısı henüz oluşma safhasındadır. Söz konusu Tartışmanın ana hatları, "Karmaşıklık Teorisinin" (*Complexity Theory*, CT) Doğa Bilimlerindeki popüler kullanımının ötesinde Uluslararası İlişkiler Teorisine uygulanmasıyla yaratılan "Karmaşık Uluslararası İlişkiler Teorisi" (*Complex International Relations Theory,* CIR) ile çizilmektedir. Uluslararası İlişkiler, sadece aktörlerin birbirleriyle ilişkilendirildiği ya da etkileşim yollarının bulunduğu bir alan olmamakla birlikte aktörlerin hem sistemlerin içinde ve dışında yer alabildiği hem de sistemlerin kendisiyle doğrudan etkileşimlerde bulunabildiği bir saha şeklinde düşünülmelidir. Bu sebeple bazı teorilerin "sistemik" veya "devlet merkezli" olarak sınıflandırılması, doğrusal olmaktan uzak bu disiplini kolaylaştırmaktadır. Buna göre bir fenomenin birçok farklı yol kullanılarak anlaşılabilmesi mümkün olabilmektedir. Buna karşın sorunun özü, kendisine özgü bilinen tüm gerçekleriyle ilişkilendirilmeden açıklanamamaktadır.[243] Uluslararası İlişkiler disiplininin çoklu teorik akışları arasında yer alan büyük tartışmaların hepsi, algılanan gerçekliğin daha geniş farkındalığı için her bir teorinin farklı algılarını birleştirmek yerine bilimsel ya da epistemolojik argümanlar sunmakla yetinmiştir. Daha da önemlisi, dünya siyaseti hakkındaki düşünce tarihinin belirli bir okumasını haklılaştırmak ve belirli yaklaşımların rolleri üzerine güncel tartışmalar için uygunluk ve söz konusu uygunluğun doğasıyla ilgili tartışma terimlerinin oluşturulması adına çok fazla görüş barındırmaktadırlar.[244]

Diğer Büyük Tartışmalara kıyasla Beşinci Büyük Tartışma'da öne çıkan üç temel husus bulunmaktadır: 1) Uluslararası İlişkilerde doğrusallık sorunu (*linearity vs. nonlinearity*); 2) Uluslararası İlişkilerde biyolojik dönüşüm (*biological turn*); 3) İnsani ve insani olmayan sistemlerin uluslararası ilişkilerdeki yeri. Kavalski'nin tespitine göre; bir taraftan günümüz hâkim Uluslararası İlişkiler yaklaşımları, doğrusal nedensellik kalıplarınca bilgilendirilirken, diğer taraftan ise Doğa Bilimleri ile Sosyal Bilimler arasındaki disiplinlerarası tozlaşmadaki artış son derece dikkat

---

[243] Daniel Gómez Amaya, *The Theory of Complexity Adapted To International Relations: The Behaviour Of The Visegrad-Ukraine Complex Adaptive System Since November 2013*, (Universidad del Rosario, School of International Relations, Basılmamış Doktora Tezi), Bogotá 2016, s. 38.

[244] Steve Smith, "The Discipline of International Relations: Still An American Social Science?", *British Journal of Politics and International Relations*, Cilt 2, Sayı 3, Ekim 2000, ss. 376-377.

çekici boyutlara ulaşmıştır.[245] Jonathon Louth'a göre doğrusal yöntemler, otomobil bakımına benzetilebilmektedir. Buna göre tamirci, aracın tüm parçalarını birbirinden bağımsız olarak düşünebilir, söküp takarak ya da değiştirerek aracın en iyi durumda çalışır olmasını sağlayabilmektedir. Bu durum, "kapalı" (*closed systems*) olarak adlandırılabilecek sistemlerin en temel özelliğidir. Öyle ki, siyasi ve sosyal sistemleri içeren "karmaşık sistemler" (*complex systems*) kapalı sistemler değildir ve bu şekilde incelenmesi gerekmektedir.[246] "Doğrusallık" (*linearity*) kavramının çoğunlukla matematik dünyasındaki matematiksel araçlarda kullanıldığı görülmektedir. John Henry Holland tarafından yapılan kabaca tanımlamaya göre doğrusallık, parçalarının değerleri toplanarak bütün için bir değer elde edilmesi anlamına gelmektedir.[247] Bu yaklaşım, her daim kurallara ilham veren aksiyomlar arayan Sosyal Bilimler için sınırsız ek mantık şekli sunmaktadır. Böylelikle doğrusal anlamda sebep ve sonuç ilişkisi, doğa yasalarından yola çıkarak ana akım Uluslararası İlişkiler teori inşasının öngörülebilirlik ve nispeten karmaşık olmayan parçalarının düzenli evrensel niteliklerine dayanan bir talep genişliği yaratmasına olanak tanımış ve uluslararası sisteme dair hesaplamalarda açıkça ortaya çıkmıştır.[248] Fakat disiplinin fiziksel bilimlere öykünmesi yeterince başarılı olamamış ve uluslararası rekabetin sonuçlarını tahmin edebilme kabiliyeti çok sınırlı kalmıştır. Alvin M. Saperstein'a göre bunun nedeni ulusların arasındaki etkileşimlerin tanımlanabilmesi için sezgisel olarak çok fazla değişkenin gerekli görünmesinde yatmaktadır. Ayrıca uluslar, bireysel olarak karmaşık insanların çokluğundan oluşmaktadır ve bu durum, kolektif davranışları temsil eden uluslararası değişkenlerin göreceli olarak basit fonksiyonel ilişkileri yerine getirebileceğine olan inancı zorlaştırmaktadır.[249] Dolayısıyla özellikle 1950'lerde geliştirilen insan rasyonelliği ve temel fiziksel düzene olan inancı temel alan paradigmanın, tüm fiziksel olayların aşamalı olarak değişeceğini ve

---

[245] Emilian Kavalski, *a.g.m.*, ss. 435-436.
[246] Jonathon Louth, *Imagining A Complex World: Science, Order and International Relations*, (Adelaide Üniversitesi, Tarih ve Politika Okulu, Basılmamış Doktora Tezi), Avusturalya, Kasım 2009, s. 6.
[247] John Henry Holland, *Hidden Order: How Adaptation Builds Complexity*, Baci (Helix) Books, New York 1995, s. 15.
[248] Jonathon Louth, *a.g.e.*, ss. 5-6.
[249] Alvin M. Saperstein, "The Prediction of Unpredictability: Applications of the New Paradigm of Chaos in Dynamical Systems to the Old Problem of the Stability of a System of Hostile Nations", Editörler: L. Douglas Kiel & Euel Elliott, *Chaos Theory In The Social Sciences: Foundations and Applications*, The University of Michigan Press, Michigan 1997, s. 139.

öngörülebilir yörüngeleri izleyeceğini öne süren indirgemeci yöntemleri kullanarak yüksek düzeyde düzen ve öngörülebilirlik sunan doğrusal modellerinin aksine 20. yüzyılda yaşanan görelilik teorisi ve kuantum mekaniğinin gelişimiyle birlikte çeşitli fenomenlerin düzenli, düzensiz, dinamik, olasılıklı, adaptif, çoklu, doğrusal ya da doğrusal olmayan şekilde var olabileceğini göstermiştir.[250]

Öte taraftan, akademik disiplinlerin içinde bulundukları toplumlardaki temel siyasi ve entelektüel eğilimleri sayısız ve karmaşık metotlarla yansıttığı gerçeği göz önünde bulundurulduğunda, Uluslararası İlişkiler teorisyenlerinin zamanın kültürel olarak önde gelen bilimlerinden fikirler çekmesi ve entelektüel meşruiyet sağlaması olağandır. II. Dünya Savaşı'nı takip eden süreçte nükleer silahların geliştirilerek caydırıcılık unsuru halini almasında "fizik" biliminin belirleyiciliği ortadayken, Duncan Bell'e göre ise 21. yüzyılda "biyolojik bilimler" öne çıkarak örnek teşkil edecek ve Uluslararası İlişkiler de bu yönelimden nasibini alacaktır.[251] Uluslararası İlişkiler araştırmalarına yönelik yapılan bu "biyolojik dönüşüm" uyarısı, Uluslararası İlişkiler paradigmasındaki sosyobiyolojik toplu karmaşıklık biçimiyle, insan dışı sistemlerin de dâhil ve belirleyici olduğu total karmaşıklık biçimi arasında uyum ve uyumsuzluk hallerinin yaratıcı dönüşümlerine yönelik önemli fırsatlar sunabilir.[252] Böylelikle değişimlerin, çelişkilerin ve doğrusal olmayan dinamiklerin odak noktasını oluşturduğu yaklaşımlarla "düzen" (*order*) halinden ziyade "çeşitlilik" (*variety*) halinin normal ve esas olduğu öne çıkarılmaktadır.[253]

4.2. Karmaşıklık Teorisi: Karmaşıklığın Tanımlanması

Sosyal Bilimler içerisinde tercih edilen "karmaşıklık" (*complexity*) kavramı, pek çok sosyal olgunun çağdaş algısı açısından bir üst kavram niteliğine haiz

---

[250] Robert R. Geyer, "Beyond The Third Way: The Science of Complexity and The Politics of Choice", *British Jorunal of Politics and International Relations*, Cilt 5, Sayı 2, Mayıs 2003, ss. 239-240.

[251] Duncan Bell, "Beware of False Prophets: Biology, Human Nature and the Future of International Relations Theory", *International Affairs (Royal Institute of International Affairs 1944-)*, Cilt 82, Sayı 3, Mayıs 2006, ss. 493-494.

[252] Steve M. Manson, "Simplifying Complexity: A Review of Complexity Theory", *Geoforum*, Cilt 32, Sayı 3, Ağustos 2001, ss. 411-412.

[253] Robert R. Geyer, "Globalization, Europeanization, Complexity, and the Future of Scandinavian Exceptionalism", *Governance: An International Journal of Policy, Administration, and Institutions*, Cilt 16, Sayı 4, Ekim 2003, s. 572.

olmuştur. Toplumsal olayların doğada karmaşık olduğu konusundaki temel anlayış üzerine dayanan bu kavram, doğrusal olmama, âdemi-merkeziyetçilik ve öz-örgütlenme gibi farklı özellikler barındırmaktadır.[254] Bunların yanı sıra karmaşıklık, mevcut bilimsel yaklaşımların sınırlarını ortaya koyan doğrusal olmayan, uyarlanabilir ve kendi kendini düzenleyen fenomenler ya da problemlerle bağlantılı şekilde ortaya çıkan kavramlar, yöntemler ve sezgiler dizisi olarak da düşünülebilmektedir. Dolayısıyla dünyanın yapısına dair öngörülebilirlik ve kontrolün sınırlılığına yönelik mütevazı bir yaklaşım olarak ifade edilebilmektedir.[255] Çok çeşitli sistemleri ve fenomenleri kapsayan genel bir terim olarak karmaşıklığın kullanımı 1970'lerden itibaren hızla artmış ve dünya genelinde karmaşıklığın çok çeşitli yönleri üzerine araştırmalar yapan merkezler ve enstitüler kurulmaya başlamıştır.[256] 1990'lardan itibaren ise Sosyal Bilimlerin tüm ana alanlarında – Felsefe, Sosyoloji, Siyaset Bilimi, İşletme, Ekonomi, Uluslararası İlişkiler– temellerini oluşturmuştur.[257] 21. yüzyılın başlangıcıyla birlikte karmaşıklık fiziği geliştirilerek çağdaş Sosyal Bilimlere uygulanır hale gelmiştir. Fiziksel ve sosyal dünyaların analizleri arasındaki örtüşmeleri ve etkileşimleri inceleyen Karmaşıklık Çalışmaları, John Urry tarafından "21. Yüzyıl Sosyal Fiziği" olarak addedilmiştir.[258] Özellikle ağların matematiğini analiz etmek isteyen fizikçiler ve matematikçiler, sosyal ağların sosyolojisine yönelmişler ve giderek karmaşıklaşan küresel süreçlerin sosyolojik analizlerine doğrusal olmayan adaptif sistemlerin fiziğinin ve

---

[254] Armando Geller, "The Use of Complexity-Based Models in International Relations: A Technical Overview and Discussion of Prospects and Challenges", *Cambridge Review of International Affairs*, Cilt 24, Sayı 1, Mart 2011, s. 63.

[255] Antoine Bousquet & Robert R. Geyer, "Introduction: Complexity and The International Arena", *Cambridge Review of International Affairs*, Cilt 24, Sayı 1, Mart 2011, s. 1.

[256] Dünyadaki çeşitli üniversitelerin katılım sağlayarak ücretli ya da ücretsiz olarak sundukları kitlesel açık çevrimiçi kurslar kapsamında da çeşitli alanlardaki karmaşıklık üzerine araştırmalar ve dersler paylaşılmaktadır. Detaylı bilgi için bkz.: MOOC (Massive Open Online Courses), *http://mooc.org/*, (Erişim Tarihi: 17 Kasım 2019); edX, *https://www.edx.org/*, (Erişim Tarihi: 17 Kasım 2019); Coursera, *https://www.coursera.org/*, (Erişim Tarihi: 17 Kasım 2019); UDACITY, *https://www.udacity.com/*, (Erişim Tarihi: 17 Kasım 2019); Udemy, *https://www.udemy.com/*, (Erişim Tarihi: 17 Kasım 2019); Harvard Online Courses, *https://online-learning.harvard.edu/*, (Erişim Tarihi: 17 Kasım 2019); MIT Open Courseware, *https://ocw.mit.edu/index.htm*, (Erişim Tarihi: 17 Kasım 2019); Stanford Online, *https://online.stanford.edu/*, (Erişim Tarihi: 17 Kasım 2019); Canvas Network, *https://www.canvas.net/*, (Erişim Tarihi: 17 Kasım 2019); Khan Academy, *http://www.khanacademy.org.tr/*, (Erişim Tarihi: 17 Kasım 2019).

[257] Christopher Ansell & Robert R. Geyer, "'Pragmatic Complexity' A New Foundation for Moving Beyond 'Evidence-Based Policy Making'?", *Policy Studies*, Cilt 38, Sayı 2, ss. 154-154.

[258] John Urry, "The Complexities of the Global", *Theory, Culture & Society*, Cilt 22, Sayı 5, 2005, s. 235.

matematiğinin girmesini sağlamışlardır. Böylelikle doğrusal olmayan dinamikler, sadece düzenin kendiliğinden ortaya çıkmasını değil, aynı zamanda karmaşıklığın da tanımlanabilmesine yardımcı olmaktadır.[259] Karmaşıklık üzerine yapılan çalışmaların odak noktası geleneksel bağlamda "yapılar" olmasına rağmen bilhassa 21. yüzyıl itibariyle odak noktası yapılar kadar "yapıların ortaya çıkış süreçlerine" de kaymıştır. Çeşitli alanlardan on farklı bilim insanını[260] Immanuel Wallerstein başkanlığında bir araya getiren Gulbenkian Komisyonu, söz konusu bu karmaşık dönüşe (*complexity turn*) reaksiyon göstermiş ve 1996 yılında "*Open The Social Sciences: Report Of The Gulbenkian Commision On The Restructuring Of The Social Sciences*"[261] isimli raporu yayınlamıştır. Bu rapora göre; Doğa Bilimleri ve Matematik alanlarında çalışan bilim insanları, giderek daha karmaşık hale gelen olaylarla karşılaşmakta ve ortaya çıkan sorunlara yönelik eski teorilerin çözüm önerileri her geçen gün daha da yetersiz kalmaktadır. Özellikle 1945'lerden itibaren Sosyal Bilimlerde egemen hale gelen nomotetik epistemoloji[262] modeli, 1960'lardan itibaren Doğa Bilimleri ile Sosyal Bilimler arasındaki ayrımın gerçekliği ve geçerliliği hususundaki sorgulamaların artmasıyla sarsılmıştır. Doğa Bilimlerinde yaşanan yeni gelişmelerle birlikte doğrusal olmayan dinamiklerin doğrusal dinamiklere kıyasla üstünlüğü, karmaşıklığın basitliğe kıyasla gerçekliği, ölçenin ölçülenden ayrımının zorluğu ve hatta karmaşık koşullar altında kalitatif yorumların, doğruluğu daha sınırlı kabul edilen kantitatif ölçümlere nazaran daha üstün olabildiği ve zaman kavramına yönelik vurgunun artması gibi önemli hususlar neticesinde Doğa Bilimleri ile Sosyal Bilimler arasındaki güçlü ayrım sarsılmış ve Doğa Bilimlerinin Sosyal Bilimlere

---

[259] Fritjof Capra, *The Hidden Connections: Integrating The Biological, Cognitive, and Social Dimensions of Life Into A Science of Sustainability*, 1. Basım, Doubleday, New York 2002, s. 14.

[260] Komisyon üyeleri: Immanuel Wallerstein, Calestous Juma, Evelyn Fox Keller, Jürgen Kocka, Dominique Lecourt, Valentin Y. Mudimbe, Kinhide Mushakoji, Ilya Prigogine, Peter J. Taylor. Detaylı bilgi için bkz.: The Calouste Gulbenkian Foundation, *https://gulbenkian.pt/en/*, (Erişim Tarihi: 18 Kasım 2019); Binghamton University, The State University of New York, "Publications: Gulbenkian Commission on the Restructuring of the Social Sciences", *https://www.binghamton.edu/fbc/publications/gulbenkian.html#members*, (Erişim Tarihi: 18 Kasım 2019).

[261] Immanuel Wallerstein (Editör), *Open The Social Sciences: Report Of The Gulbenkian Commission On The Restructuring Of The Social Sciences*, Mestizo Spaces / Espaces Metisses, Stanford University Press, California Mart 1996.

[262] Nomotetik epistemoloji: Nomotetik, kelime olarak tekrarlayan olgular ve süreçler üzerinden evrensel yasa oluşturulması anlamına gelmektedir. Nomotetik epistemoloji ile evrensel olanın bilgisi ve felsefesi kastedilmektedir. Detaylı bilgi için bkz.: William Little, H. W. Fowler & J. Coulson, *a.g.e.*, s. 1334.

benzeşmesi söz konusu olmuştur. Doğa Bilimleri ile Sosyal Bilimler arasındaki çelişkilerin azalması ise insanlığı makineye benzeten eski anlayışların yerine doğayı etkin ve yaratıcı gören yeni anlayışların almasına vesile olmuştur.[263]

Karmaşıklık Teorisi (*Complexity Theory*, CT), çoğunlukla Doğa Bilimleri, Matematik ve Teknoloji alanlarında etkili olmuştur. Sosyal Bilimlerdeki etkisi, nispeten daha yeni ve daha az gelişmiştir. Tamamlanmış bir Karmaşıklık Teorisinin yapısı terimlerle çelişkili görünebilmektedir yani belirli karmaşık düzenlerin talep ettiği formlara bölünebilmektedir.[264] Öte yandan bu teori, Sosyal Bilimlere yönelik temel pragmatik yaklaşımın yeniden düşünülmesini sağlayan bir perspektif sunmaktadır. 20. yüzyılın ikinci yarısında Doğa Bilimlerinde ortaya çıkan Karmaşıklık Teorisi, 1980'lerden günümüze dek Sosyal Bilimlere giderek daha fazla yayılmıştır. Bu teori, esas itibariyle karmaşıklık problemine çözüm sunmamaktadır. Aksine, insan toplumları için karmaşıklık halinin neden normal ve sağlıklı olduğunun anlaşılabilmesi üzerine çalışmaktadır.[265] Karmaşıklık Teorisinin ortaya çıkışına dair en eski örneklerden bir tanesi matematikçi ve meteorolog –aynı zamanda Kaos Teorisinin kurucularından biri olarak da kabul edilen– Edward Norton Lorenz'e dairdir: Lorenz, 1960'ların başında basit bir hava sisteminin bilgisayar modelini inşa etmiştir. Önceki çalışmalarının devamı esnasında sayı dizilerinde yaptığı ufak bir değişikliğin neticeye olan etkisinin çok az –sapma oranının 1'in altında– olacağını hesaplamasına rağmen grafiklerde ortaya çıkan sonucun çok farklı olduğunu tespit etmiştir. Başlangıçta bilgisayar hatasından kaynakladığı düşünülen ve tutarsız kabul edilen bu sonucun aslında oluşturulan hava durumu sisteminin sanılandan daha karmaşık olduğu, başlangıç koşullarına ve değişkenlere aşırı duyarlı olduğu gerçeğinin kabul edilmesiyle doğrusal olmayan modellemelerin ortaya çıkmasına vesile olmuştur. Sosyal Bilimler açısından bakıldığında ise başlangıç koşulları ve değişken kavramları, bilgisayar modellemelerinin daha sınırlı uygulamalarına karşı Sosyal Bilimler gibi süreç disiplinlerini barındıran bir alan içerisindeki analizler

---

[263] Gulbenkian Komisyonu, *Sosyal Bilimleri Açın: Sosyal Bilimlerin Yeniden Yapılanması Üzerine Rapor*, Çeviren: Şirin Tekeli, 4. Basım, Metis Yayınları, İstanbul 2003, ss. 60-61.

[264] John Smith & Chris Jenks, *Qualitative Complexity: Ecology, Cognitive Processes and The Re-Emergence of Structures in Post-Humanist Social Theory*, 1. Basım, Routledge, New York 2006, ss. 3-4.

[265] Robert R. Geyer, "Globalization, Europeanization, Complexity, …", s. 560.

adına oldukça endişe verici olmuştur.[266] Bu bağlamda Karmaşıklık Teorisi, çok sayıda aktör arasındaki etkileşimin, aktörlere özgü davranışlardan beklenmeyen olgulara yol açabileceğini düşünmektedir. Bir öz-örgütlenme biçiminde bütün, parçalarının toplamından daha fazlası olan, çevresinden ayırt edilebilir fakat buna karşı gelinemeyen sonuçlar yaratabilmektedir.[267] Öte taraftan disiplinlerin diğer disiplinlerden metodolojik olarak faydalanma, kullanılan tekniklerden ödünç alma ya da kendi amaçları dışında görülen konular hakkında spekülasyonda bulunabilme eğilimleri her daim vardır. Hatta potansiyel yanlış yönlendirmeler pahasına da olsa gerçekleşen çapraz akademik etkileşimler sayesinde geçmişin hantal ve indirgemeci bilim anlayışına karşı "karmaşıklık" başlığı altında yeni bir dinamizm katılması söz konusu olmuştur.[268] İşte bu dinamizm hali, görünüşte karmaşık sistemleri basitleştirmenin bir aracı olarak da ele alınabilmektedir. Söz konusu teorinin uygulaması, tanımlanabilir tek bir Karmaşıklık Teorisi olmadığı için oldukça zor olabilmektedir. Bunun yerine, karmaşık sistemlerle bağıntılı olan teoriler, genel anlamda "karmaşıklık" başlığı altında toplanabilmektedir. Bu nedenle karmaşıklık üzerine yapılan araştırmaların kesin niteliğinin, karmaşıklık fikirlerinin disiplin sınırları içerisinde ne ölçüde işlem gördüğüne bağlı olarak keşfedilebilmesi oldukça zor olabilmektedir.[269]

Karmaşıklık, nedenlerdeki büyük değişikliklerin etkilerde büyük değişiklikler yarattığı genel kabul görmüş nosyonu reddetmektedir. Deterministik bir kurallar dizisinin ardından öngörülemeyen ancak farklı modellemelerde sonuçlar elde edilebilmektedir. Bunlar, büyük etkiler yaratan durumlarda küçük nedenler olabileceği gibi tam tersi de söz konusu olabilir. Dolayısıyla denklemlerine yönelik çözüm önerileri, başlangıç koşullarına karşı son derece hassastır ve değişkenler arasındaki ilişkiler, ani değişimlerle birlikte doğrusal olmayabilir. Bu sebeple aynı nedenler belirli durumlarda niteliksel olarak farklı etki türleri üretebilirler.[270]

---

[266] John Smith & Chris Jenks, *a.g.e.*, s. 4.
[267] Mark Chinen, "Complexity Theory and The Horizontal and Vertical Dimensions of State Responsibility", *The European Journal of International Law*, Cilt 25, Sayı 3, 2014, s. 704.
[268] John Horgan, "From Complexity to Perplexity", *Scientific American*, Cilt 272, Sayı 6, Temmuz 1995, s. 104.
[269] Steven M. Manson, *a.g.m.,* s. 405.
[270] John Law & John Urry, "Enacting The Social", *Economy and Society*, Cilt 33, Sayı 3, 2004, ss. 400-401.

Öte taraftan karmaşıklık teorisi, genel sistemler teorisi (*general systems theory*)[271] düşüncesinin bir değişkeni olarak da görülmektedir. Genel sistemler teorisinin argümanı; etkileşimli nesneler, aktörler ya da amiller topluluğunun bir "sistem" olarak düşünülmesine ve tüm sistemlerin –Güneş sistemi, Ceza adalet sistemi, Uluslararası sistem vb. fark etmeksizin– içindeki paydaşların ortak özelliklere sahip olduğu inancına dayanmaktadır. Söz konusu nesneler, aktörler ya da amillerin davranışlarını gözlemlemek, çerçevelendirmek ve modellemek ise esas amacı teşkil etmektedir. Karmaşıklık Teorisi, Doğa Bilimlerindeki çeşitli sistemlerin yapılarının kendiliğinden oluştuğu gözlemine dayanarak "merkezi kontrolöre" gerek duyulmaksızın var olan çeşitlilik düzenini açıklamaya çalışmaktadır.[272] Dahası sistemlerin diğer sistemlerle bağlantı ağında olduğu ve dâhili olarak karmaşık yapıda olduğu kabul edilmektedir. Dolayısıyla sistemler, bir ağ üzerinde birbirine bağlanan oluşumlar ya da topluluklar olarak anlaşılmaktadır. Özellikle canlı sistemler, özellikleri küçük parçalarına indirgenemeyen bütünlerdir ve temel özellikleri, parçaların doğrudan sahip olamadığı bütünün özellikleridir. Eğer bir sistem, kendisini oluşturan yalıtılmış parçalara ayrılarak analiz edilmeye çalışılırsa, temel ve sistemik özelliklere zarar verilmiş olur.[273]

Fizikte ya da biyolojideki karmaşık sistemlere bakıldığında, temel bileşenlerin ve temel yasaların genellikle oldukça basit olduğu görülmektedir. Karmaşıklığın ortaya çıkışı, aynı anda etkileşime giren bu basit bileşenlerin birçoğunun bilgisine sahip olunduğunda doğmaktadır; yani karmaşıklık aslında sistemin bileşenlerinin etkileşime girebilmesi için sayısız olası yolu barındıran organizasyondadır.[274] Karmaşıklık teriminin belirsiz karakteristiği, açıkça tanımlanmış ve formulüze edilmiş bir bilimsel teoriyi ifade etmek yerine doğrusal olmayan dinamik sistemlere yönelik geniş bir araştırma alanını kapsadığı gerçeğini

---

[271] 1960'lı yıllarda, özellikle bilgisayar bilimlerinde popüler olan genel sistemler teorisi, temel olarak çeşitli unsurlardan oluşan büyük ağların incelenmesi ve anlaşılabilmesi adına çoğunlukla insan oluşumlarını idealize etmiştir.Detaylı bilgi için bkz.: Stephen Wolfram, *A New Kind Of Science*,1. Basım, Wolfram Media, Illinois 2002.

[272] Steven Wheatley, "The Emergence of New States in International Law: The Insights from Complexity Theory", *Chinese Journal of International Law*, Cilt 15, Sayı 3, s. 580.

[273] Fritjof Capra, *The Web of Life: A New Scientific Understanding of Living Systems*,1. Basım, Anchor Books, Doubleday, New York 1996, s. 36.

[274] M. Mitchell Waldrop, *Complexity: The Emerging Science At The Edge Of Order And Chaos*, 1. Basım, Touchstone Book, Simon & Schuster, New York 1993, s. 86.

yansıtmaktadır. Bu nedenle karmaşıklık, dinamik sistemlerin oluşumu ve davranışına ilişkin çeşitli araştırmalarla geliştirilen farklı içgörüler ve kavramlar için geniş bir başlık niteliğindedir.[275]

Stephen Wolfram, karmaşıklığın temel bir bağımsız fenomen olarak incelenebileceğini ve genel karmaşıklık olgusuna ve kökenlerine dair temel bir anlayış geliştirilmesinin mümkün olabileceğini belirtmiştir. Somut sonuçlar, karmaşık yapılı ama oldukça basit davranışlara sahip spesifik programlara dayanma eğilimi gösterebilmektedirler.[276] Bilgisayar Bilimlerindeki Hesaplamalı Karmaşıklık Teorisi (*Computational Complexity Theory,* CCT) üzerinden hesaplamalı evrende fiziksel evrenin bulunup bulunamayacağını sorgulayan Wolfram, fizik tarihinin evren kurallarının oldukça karmaşık olması gerektiğine inanmamızı sağladığını ancak hesaplamalı evrende, inanılmaz derecede basit olan kuralların inanılmaz derecede zengin ve karmaşık davranışlar üretebileceğini belirtmektedir.[277]

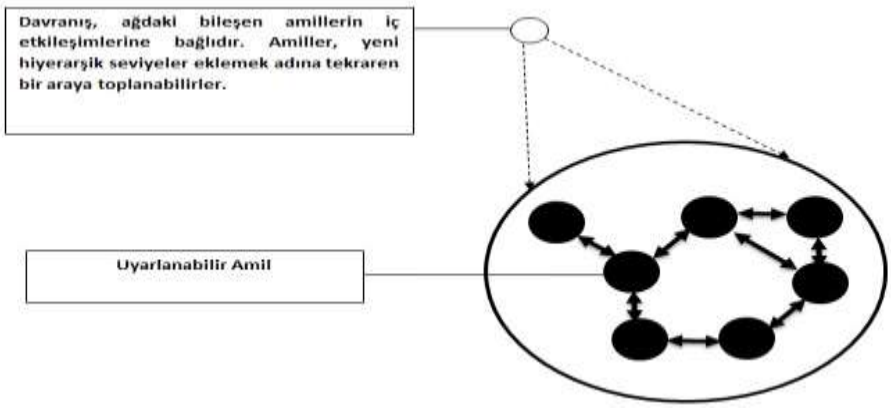
Karmaşıklık Teorisinin karakterine bakıldığında, tek bir Karmaşıklık Teorisinden ziyade karmaşıklıktan ilham alan kavramları kullanan bir dizi yaklaşımın söz konusu olduğu görülmektedir. İki temel kavramın söz konusu yaklaşımlarda sıklıkla öne çıktığı tespit edilmiştir: otopoez (*autopoiesis*) ve karmaşık uyarlamalı sistem (*the complex adaptive system,* CAS).[278] Otopoez (*autopoiesis*) kavramı, kabaca kendi kendini yapılandırma anlamına gelmektedir. Bilişsel biyoloji (*cognitive biology*) biliminden ödünç alınan bu kavram, orjinal haliyle canlı organizmaların bileşenleri ve çevreleriyle olan ilişkileri ürettiğini ve düzenlediğini vurgulamaktadır.[279] Karmaşık sistemlerin aktif olarak yaratıcılık ve öngörülemezlik özellikleri ön plandadır. Bu sebeple özellikle sosyal sistemlerin gelişimine yönelik incelemelerin daha dikkatli ve farklı perspektiflerle yapılması gerekmektedir. Örneğin; Kenneth Waltz, devletlerin belirli şekillerde hareket etmesini şart koşan

---

[275] Antoine Bousquet, "Complexity Theory and the War on Terror: Understanding The Self-Organising Dynamics of Leaderless Jihad", *Journal of International Relations and Development*, Cilt 15, Sayı 3, 2012, s. 349.
[276] Stephen Wolfram, *A New Kind Of Science*,1. Basım, Wolfram Media, Illinois 2002, ss. 14-45.
[277] Stephen Wolfram, "Computating A Theory Of All Knowledge", TED2010, Şubat 2010, *https://www.ted.com/talks/stephen_wolfram_computing_a_theory_of_all_knowledge*, (Erişim Tarihi: 24 Kasım 2019).
[278] Erika Cudworth & Stephen Hobden, "The Foundations of Complexity, The Complexity of Foundations", *Philosophy of the Social Sciences*, Cilt 42, Sayı 2, 2012, s. 168.
[279] John Smith & Chris Jenks, *a.g.e.*, s. 6.

anarşi halinin belirleyici özellikleri nedeniyle uluslararası sistemi değişmez olarak yorumlamaktadır.[280] Karmaşıklık teorisyenleri ise uluslararası sistemin karmaşık bir sistem olduğunu varsaymakta ve belirli bir süre boyunca istikrarlı görünse de, nihayetinde otopoezin sistemin karakterinde değişikliklere yol açabileceğini savunmaktadırlar. Bundan dolayı özellikle Uluslararası İlişkiler çalışmalarında karmaşık sistem anlayışının gelişimi, kendi kendini yapılandıran özelliklerin ve diğer insani ve insan dışı sistemlerle olan ilişkilerin dikkatle incelenmesiyle olabilir.[281] Öte yandan Karmaşık Uyarlamalı Sistemler (*Complex Adaptive Systems,* CAS) büyük ölçekli sosyal etkileşimlerin dinamikleri hakkında değerli bilgiler sağlamaktadırlar. Başlarda sadece ekosistemler ve beyin yapıları gibi fiziksel fenomenleri analiz etmek için kullanılan karmaşık uyarlamalı sistemler, ilerleyen süreçlerde seçim davranışları, borsa algoritması ve savaşın evrimi gibi çeşitli alanlarda da uygulanır olmuştur.[282] Karmaşık uyarlamalı sistemler, deneyimlerden değişebilen ve öğrenebilen özel bir karmaşık sistem durumu oluşturmaktadır. Karmaşıklık teorisyeni John Henry Holland, karmaşık uyarlamalı sistemlerin bilimsel olarak çalışılan çoğu sistemden oldukça farklı olduğunu, merkezi yönlendirmeler olmaksızın koşullu eylemler ve beklentiler ile değişim altında tutarlılık sergileyebildiklerini belirtmektedir.[283]

Tablo-10: Karmaşık Uyarlamalı Sistem Modellemesi



Kaynak: John Henry Holland, *Hidden Order: How Adaptation Builds Complexity*, Baci (Helix) Books, New York 1995, s. 6.

[280] Kenneth N. Waltz, *Theory of International Politics*, 1. Basım, McGraw-Hill, Inc., New York 1979, s. 54.
[281] Erika Cudworth & Stephen Hobden, *a.g.m.*, s. 179.
[282] Seva Gunitsky, "Complexity and Theories of Change in International Politics", *International Theory*, Cilt 5, Sayı 1, Mart 2013, s. 35.
[283] John Henry Holland, *a.g.e.*, ss. 38-39.

Tablo 10'da da görüldüğü üzere Holland'a göre karmaşık uyarlamalı sistemler, paralel olarak ve sürekli şekilde hareket eden çok sayıda, çeşitli formlarda ve özelliklerdeki amillerin, diğer amillerin yaptıklarına verdikleri reaksiyonları da kapsayan dinamik ağ olarak tanımlanmaktadır. Karmaşık uyarlamalı sistemlerin kontrolü oldukça dağınık ve merkezden uzaklaşma eğiliminde olduğu için sistemlerin içerisindeki her türlü tutarlı davranış, amiller arasındaki rekabet ve işbirliklerinden kaynaklanmaktadır. Sistemlerin genel davranışının da çok sayıda amil tarafından alınan tüm bireysel kararların birikimi olduğu vurgulanmaktadır.[284] Dolayısıyla bir dizi stratejik aktörün tekrarlanan etkileşimlerinin yarattığı yeni özellikler, doğrusal olmayan dinamikler ve eş adaptasyon hali, karmaşık bir sistemi öne çıkaran tanımlayıcı özellikler olarak yorumlanabilmektedir.[285] "Uluslararası sistem" olarak adlandırılan sistemin içinde yer alan birçok unsur, aktör ve eylemin yukarıda aktarılan özelliklerin çoğunu barındırmasına rağmen Uluslararası İlişkilerde geleneksel olarak kabul edilen ve genellikle uluslararası fenomenleri doğrusal bir bakış açısıyla analiz eden yaklaşımın, karmaşıklık üzerine yapılan çalışmaların Uluslararası İlişkiler gibi gerçek bir Sosyal Bilime uyan bir araç haline dönüştürülmesiyle farklı bir boyut kazanacağı düşünülmektedir.[286]

4.3. Karmaşık Uluslararası İlişkiler Teorisi

Geleneksel Uluslararası İlişkiler Teorisinin nadir ve beklenmedik olayları öngörme ve anlama konusundaki başarısızlığı son derece dikkate değer olmuştur. Öyle ki, beklenmedik ve nadir olayların anlaşılmasındaki başarısızlık hali, değişimi açıklayan daha büyük başarısızlıkların belirtisi olarak yorumlanmaktadır. Bu bağlamda Matthew J. Hoffmann, değişimin deneysel olarak değil, doğası gereği teorik ve göreceli olarak açıklanabileceğini belirtmektedir. Değişimin açıklanması teoriktir; çünkü değişimin açıklanabilme iddiası, kullanılan teorik perspektifin politik aktörler, davranışlar, tutumlar, ilişkiler vb. "şeyler" üzerinden gözlenen çeşitliliği ortaya çıkarabileceği anlamına gelmektedir. Görecelidir; çünkü perspektifler akla

[284] Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, 2. Basım, Columbia University Press, New York 2009, s. 175.
[285] Seva Gunitsky, *a.g.m.*, s. 39.
[286] Daniel Gómez Amaya, *a.g.e.*, s. 38.

gelebilecek değişkenlikler açısından karşılaştırılmaktadır.[287] Çoğu Uluslararası İlişkiler teorisi, esasa yönelik politikaların bazı yönlerini genelleştirir veya sabit tutar ve böylece alt seviyelerdeki değişimi açıklayabilmektedirler. Önemli aktörleri (genellikle devletler), politik ilişkileri (güvenlik ikilemi vb.) ve genelleme davranışlarındaki belirli kavramları dondururlar. Bu yöntemle çok değerli işler yapılmış olmasına rağmen bu tür genellemeler yapan teorilerin nadir ve ani görülen olaylardan kaynaklanan değişimlere karşı savunmasız kaldığı gerçeğini değiştirmemektedir. Teoriler ani ve nadir gelişen olayları görmezden gelirse, sabit tutulan esasa yönelik politik koşulları değiştirme potansiyeline sahip, olası diğer olayları da görmezden gelebilir.[288] Başlangıç koşullarındaki en ufak değişikliklerin bile çok çeşitli sonuçlara yol açabilmesi ve genellikle rastgele olarak da ifade edilebilen küçük değişikliklere karşı aşırı duyarlılık hali, karmaşıklık teorisinin Uluslararası İlişkilere uyarlamasında da aynı derecede büyük önem arz etmektedir. Karmaşık sistemler, özellikle kritik noktalarda çok önemli görülmeyen olaylardan doğrudan etkilenebilmektedirler.[289]

Uluslararası süreçlerin karmaşıklığına atıfta bulunan "Karmaşık Uluslararası İlişkiler Teorisi"; karmaşık karşılıklı bağlılık (*complex interdependence*)[290], karmaşık öğrenme (*complex learning*)[291], karmaşık güvenlik (*complex security*)[292] gibi alan içerisinde kullanımı tercih edilen çeşitli kavramlarla "karmaşıklığı" Uluslararası İlişkiler söylemlerinin ayrılmaz bir parçası haline getirmiştir.[293] Bununla beraber Karmaşık Uluslararası İlişkiler Teorisi, Uluslararası İlişkilerin incelenmesinde "Beşinci Büyük Tartışma"yı çizmektedir. Ana hatları, Gulbenkian Komisyonu'nun önerisini takiben, karmaşıklık tarafından kuşatılan Doğa Bilimleri ile Sosyal Bilimler arasındaki bölünmeyi azaltarak yakınsama yaratmak

---

[287] Matthew J. Hoffmann, "Constructing a Complex World: The Frontiers of International Relations Theory and Foreign Policy-making", *Asian Journal of Political Science*, Cilt 11, Sayı 2, Aralık 2003, ss. 41-42.
[288] Matthew J. Hoffmann, *a.g.m.*, s. 43.
[289] Matthew J. Hoffmann & John Riley Jr., "The Science of Political Science: Linearity or Complexity in Designing Social Inquiry", *New Political Science*, Cilt 24, Sayı 2, 2002, ss. 311-312.
[290] Joseph S. Nye, Jr. & David A. Welch, *Understanding Global Conflict and Cooperation: An Introduction to Theory and History*, 10. Basım, Pearson, Boston 2017.
[291] Alexander Wendt, *Social Theory of International Politics*, 1. Basım, (Virtual Publishing, 2003), Cambridge University Press, New York 1999.
[292] Ken Booth (Editör), *Critical Security Studies and World Politics*, 1. Basım, Lynne Rienner Publishers, Colorado 2005.
[293] Emilian Kavalski, *a.g.m.*, s. 441.

üzerine kurulmuştur.[294] Geleneksel Uluslararası İlişkiler yaklaşımlarından farklı olarak Karmaşık Uluslararası İlişkiler Teorisi, uluslararası yaşam kalıplarının, fiziksel ve sosyal ilişkilerin panarşik melezleri olduğunu kabul etmektedir. Teknoloji, İnternet, sağlık, çevre vb. melezler, küresel ilişkilerin analizlerinde merkez teşkil etmekte ve birbirine doğrudan ve dolaylı şekillerde bağlı olan fiziksel-sosyal dünyaların ya da insan dışı oluşumların karmaşıklık analizleri geliştirilerek incelenmektedir. "Fiziksel" ve "Sosyal" arasındaki sosyo-tarihsel bölünmenin aşılabilmesi için farklı kabul edilen dünyaların dinamik bağımlılıkları ve etkileşimleri, karmaşıklık üzerinden incelenerek ortaya çıkarılan özellikler daha etkin bir şekilde anlaşılabilmekte ve böylelikle iki kutup arasında var olan derin bölünmenin dağılması sağlanabilmektedir.[295]

Uluslararası İlişkiler Teorisinin alaka düzeyi, teorisyenlerin herhangi bir dönemin yeni ufuklar açan olaylarını öngörme ya da en azından anlayabilme yeteneklerine dayanmaktadır. Özellikle Soğuk Savaş'ın sona ermesinin Uluslararası İlişkiler teorisyenlerinde yarattığı büyük şaşkınlık hali ile 9/11 Terör Saldırıları'na disiplinin vermiş olduğu reaksiyon karmaşası son derece dikkat çekicidir. Bu büyük gelişmeler, Uluslararası İlişkiler disiplininin süreksiz ve doğrusal olmayan değişime dayanan aksiyonların anlaşılması, açıklanması, öngörülmesi ve kavramsal çerçeveler sağlanabilmesi açısından yetersiz kalabildiğini gözler önüne sermiştir. Ortaya çıkan bu önemli boşluk, küresel politikaların öne çıkan iki kritik yönü olan "değişim" ve "karmaşıklık" karşısında disiplinin gerçekten zorlandığının belirtileri şeklinde yorumlanmıştır.[296] Ani ve beklenmeyen dengelerin zarar görmesi, sistemleri yeni cazibe noktalarına çekebilmektedir. Yine 9/11 Terör Saldırıları örnek alınırsa, ortaya çıkan dramatik olaylar esnasında göç hareketleri ya da küresel bilinçlilik gibi daha belirsiz kavramlar gündeme getirilmesine rağmen sadece ekonomik aktiviteler üzerinde anlık olarak yavaşlamalar yaşanmıştır. Yaşanan bu değişim ve süreklilik sürecinde, yalnızca maddi düzeyde ve doğrusal olmayan dinamizmin küresel iletişim, ticaret, medya, finans ve dağıtım sistemleri üzerindeki etkileri ve geri dönüşleri gibi birçok konuya dahli söz konusu olmuştur. Benzer şekilde dünya siyasetine ve küresel

---

[294] *A.g.m.*, s. 449.
[295] John Urry, *Global Complexity*, 1. Basım, Polity Press, Cambridge 2003, ss. 17-18.
[296] Matthew J. Hoffman, "Constructing a Complex... ", ss. 37-38.

ilişkilere bakıldığında; uluslarüstü örgütlerin, çok uluslu şirketlerin ve hükümet dışı kuruluşların çoğalmaya ve değişmeye devam etmesi muhtemel olacaktır. Uluslararası politikalar daha farklı düzen türleri bulmaya devam ettikçe dünya, zaman zaman yaşanan/yaşanacak dramatik değişimlerle hafifletilen daha karmaşık biçimlerde örgütlenmeye devam edecektir.[297] Ana akım Uluslararası İlişkilerdeki doğrusal değişim algılarının -değişkenlerde değişimler meydana gelir ama etki sabittir- aksine Karmaşık Uluslararası İlişkiler Teorisi'nde "şeylerin değişime uğradığı" vurgusu söz konusudur. Ortaya çıkan uluslararası yaşam kalıplarının tahmin edilemezliği, "kendini düzenleyen kritiklik" (*self-organized criticality*) çerçevesinde kavramsallaştırılmaktadır.[298] Bir sistemin kritik bir noktaya yaklaşacak ve sonrasında kendisini o noktada tutabilecek şekilde evrimleşebilmesi kabiliyetine "kendini düzenleyen kritiklik" (*self-organized criticality*) adı verilmektedir.[299] Per Bak tarafından geliştirilen bu nosyona göre; doğadaki karmaşık davranışlar, birçok bileşenin bulunduğu büyük sistemler içerisinde ufak çaplı kabul edilen sorunların yüksek derecede dengesiz kritik durumlara dönüşme eğilimini yansıtmaktadır. Kendileri üzerine adapte olan karmaşık sistemlerdeki değişimlerin çoğu, kademeli yumuşak bir yol izlemekten ziyade yıkıcı olaylarla gerçekleşmekte ve sistemin izleyeceği yeni yol öngörülemez ve kontrol edilemez olmaktadır.[300] Benzer şekilde yerleşik organizma tarafından öne sürülen dünya, sadece bir dünya olarak görülmemeli, ilgili bağlardan yani kısmen izlenimler, kısmen inşa edilmişlik ve kısmen deneyimlenen ilgili olayların bağıntısından oluşmaktadır. Çevre ise olunması istenen soyut dilsel yapı değil; yerelleştirilmiş, heterojen, kökten zamansal ve kendisi de kısmen organizmaya benzeyen bir sistemler topluluğu olarak ele alınmaktadır.[301]

Karmaşık Uluslararası İlişkiler Teorisi'nin değeri, uluslararası yaşamın içerisindeki ara bağlantıların karmaşık sistemler açısından düşünülmesinde yatmaktadır. Buna göre dünya siyaseti, sistemik teoriden ziyade karmaşık ve koşullu

---

[297] Jonathon Louth, *a.g.e.,* s. 326.
[298] Emilian Kavalski, *a.g.m.,* s. 448.
[299] Myriam A. Dunn, "Securing The Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory", Editörler: Johan Eriksson & Giampiero Giacomello, *International Relations and Security in the Digital Age*, 1. Basım, Routledge, New York 2007, s. 99.
[300] Per Bak, *How Nature Works: The Science of Self-Organized Criticality*, 1. Basım, Springer-Verlag, New York 1996, ss. 1-3.
[301] John Smith & Chris Jenks, *a.g.e.,* s. 52.

olarak düşünülmelidir.[302] Karmaşık Uluslararası İlişkiler Teorisinin küresel bağlamdaki en dolaysız katkısı olarak ise insani durum hakkındaki anlayışın derinleştirilmesi gösterilmektedir. Başlarda söz konusu teorinin soyutlamaları, en acil endişelerden uzak görünse de hem insan hem de doğa bilimlerinin karmaşık sistemler içerisindeki ve arasındaki geniş çaplı etkileşimlerinin merkezinde çok çeşitli nedensellik ve uyum çizgileri olan daha bağımlı bir anlayış sunmaktadır. Ayrıca karmaşıklık çalışmalarında toplanan içgörüler sayesinde belirsizlik, öngörülemezlik ve risk anlayışlarına daha net katkılar sağlanmaktadır.[303]

Tablo-11: Karmaşık Uluslararası İlişkiler Fenomeni



Kaynak: Robert R. Geyer, "European Integration, The Problem of Complexity and The Revision of Theory", *JCMS: Journal of Common Market Studies*, Cilt 41, Sayı 1, 2003, s. 29.

Tablo 11'e göre Karmaşık Uluslararası İlişkiler, uluslararası yaşamın düzen halinin yokluğundan ziyade düzen (doğrusal modeller), karmaşıklık (doğrusal olmayan modeller) ve düzensizlik (düz modeller) hallerinin bir arada bulunduğu; yalnızca bir tür "düzen" değil, her tür model çeşitliliğinin var olduğu bir ortam olarak görülmektedir. Uluslararası sistemin temel çerçevesi -özellikle önemli güç eşitsizlikleri- en belirgin doğrusal yönü olarak görünmektedir. Güç eşitsizlikleri yaşamış ve sürekli bu durumu lehine değiştirmek için mücadele etmiş önemli

[302] Emilian Kavalski, *a.g.m.*, s. 443.
[303] Jim Whitman, *The Limits of Global Governance*, 1. Basım, Routledge, New York 2005, s. 55.

aktörlerden olan ulus-devletler, uluslararası sistemin temel çerçevesi olarak görünenlerin birer parçasıdır. ABD üzerinden örneklemek gerekirse; ABD'nin gücü 11 Eylül tarzı olaylara cevap verme seçeneklerini önemli ölçüde etkilemiştir. Bununla birlikte uluslararası karmaşıklığı etkileyen uluslararası kurumların ve rejimlerin (BM, bölgesel oluşumlar, ticari kuruluşlar vs.) prosedürleri çerçevesinde mekanik karmaşıklık olarak derhal algılanmıştır. Ardından ABD'yi "terörle mücadele" konusunda destekleme seçeneği, çeşitli ülkelerden kabul edilebilir bir tepki modeline yol açmıştır; ancak alınan bu kararların arkasındaki kesin nedenlerin ya da sonrasında hangi aktörlerin bu kararı alabileceğini tahmin edebilmek oldukça zor olacaktır.[304]

Küresel karmaşıklık hali, basit bir anarşik bozukluk olarak düşünülmemelidir. Bu genel düzensizlik kalıbı içerisinde belirli bir performans sergileyen ve çeşitli geri bildirim süreçleriyle çoklu zaman aralıklarında çalışan süreçler için çeşitli ağları, akışkanları ve yönetişim mekanizmalarını kapsayan unsurlar bulunmaktadır. İşte bu unsurlar sayesinde "küresel" olarak adlandırılan "şey"in paralel kavramları ve süreçleri geliştirilmektedir. Böylelikle dünya genelinde çeşitli ölçeklerde bulunan düzensiz ancak çok farklı şekillerde benzerlikler taşıyan "küresel fraktal" olarak da adlandırılabilecek aktörler söz konusu olmaktadır.[305] Bu teoriye göre karmaşıklık, kaos anlamına gelmemektedir çünkü sistemik etkiler düzenlilikler üretebilmektedir. Sistem, aktörlerin tekrar eden, tanımlanabilir ve açık olmayan öncelik ve tercihlerinde kendini göstermektedir. Her ne kadar Karmaşık Uluslararası İlişkiler Teorisinin bu savları, test edilebilir bir uluslararası politika teorisi üretebilmek için oldukça geniş olsa da, mevcut teorilerin yaklaşımlarındaki eksiklikleri ve gözden kaçabilecek noktaları işaret edebilmesi adına son derece faydalı görülmektedir.[306]

Karmaşık Uluslararası İlişkiler Teorisinin özellikle ontolojik yaklaşımı, geleneksel Uluslararası İlişkilerin "herhangi bir bağlamda, herhangi bir zamanda keşfedilmeyi bekleyen tek bir gerçekliğin olduğu" varsayımına aykırıdır.[307] Bu nedenle geleneksel yaklaşımların farklı bakış açılarına aykırı biçimde Karmaşık

---

[304] Robert R. Geyer, "European Integration, The Problem of Complexity and The Revision of Theory", *JCMS: Journal of Common Market Studies*, Cilt 41, Sayı 1, 2003, s. 29.
[305] John Urry, *a.g.e.*, s. 102.
[306] Seva Gunitsky, *a.g.m.*, s. 44.
[307] Emilian Kavalski, *a.g.m.*, s. 446.

Uluslararası İlişkiler Teorisi, farklı gerçeklikleri etkilemekte ve tek bir dünya olmadığını iddia etmektedir. Tek bir dünya düşüncesinden, dünyanın farklı ve tartışmalı sosyal ve maddi ilişkilerde çoğaldığı düşüncesine sürükleyen bir değişimden bahsetmektedir.[308] Organizasyonu ve kısıtlamayı yansıtan asimetrik ilişkilere sahip daha fazla sayıda bileşen arasındaki daha fazla karşılıklı bağımlılık ve ara bağlantıya bağlı olarak daha karmaşık topluluklar daha büyük bilgi yüküne sahip olmaktadırlar. Söz konusu durum, hem iletişim hem de bilgi işleme süreçleri için geçerli olmaktadır.[309] Karmaşık Uluslararası İlişkiler Teorisi, otopoez ve karmaşık uyarlamalı sistem kavramları aracılığıyla yapılar ve dönüşüm, istikrar ve değişim ile çeşitli sistemik seviyelerde çalışan çoklu aktörlerin etkileşimlerini bir araya getirme zorluğu ile baş edebilmektedir. Genel Sistemler Teorisindeki "bir sistem, parçalarının toplamından ve aralarındaki etkileşim ve ilişki kalıplarından daha fazlası görünemez" yaklaşımı, ana akım Uluslararası İlişkiler görüşündeki devletlerin anarşik bir ortamdaki etkileşimine uygulanmaktadır.[310] Otopoez kavramı, uluslararası sistemin karakterizasyonunda, sistemin mikro ve makro unsurlarının birbirine bağlanması ve sistemin en düşük seviyelerinde bile yüksek seviyelerde etkiler yapabileceğini gösterme konusunda daha fazla esneklik sağlamaktadır. Karmaşık uyarlamalı sistemler teorisi ise sistemi oluşturan elemanların zaman içinde etkileşimle birlikte evrimleşebildiklerini belirtmektedir. Buna göre basit ve koordine olmayan stratejiler izleyen bireysel aktörlerin, zorunlu olarak öngörülebilir ve istikrarlı olmasa da, karmaşık ve düzenli toplam davranışlar üretebildiği gösterilebilmektedir.[311]

Karmaşık Uluslararası İlişkiler Teorisi, geleneksel uluslararası ilişkilerin hiyerarşik analitik perspektiflerinin aksine "panarşi" (*panarchy*) kavramını önermektedir. Hiyerarşi (*hierarchy*) kelimesine antitez olarak tanımlanan bu kavramın temel odak noktası, değişim ve süreklilik ile öngörülebilir olan ve öngörülebilir olmayan arasındaki etkileşimi rasyonalize etmektir. Teorinin çapraz

---

[308] John Law & John Urry, *a.g.m.*, s. 397.
[309] Nader Elhefnawy, "Societal Complexity and Diminishing Returns in Security", *International Security*, Cilt 29, Sayı 1, Yaz 2004, s. 153.
[310] Antoine Bousquet & Simon Curtis, "Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations", *Cambridge Review of International Affairs*, Cilt 24, Sayı 1, Mart 2011, s. 51.
[311] Robert Jervis, *System Effects: Complexity In Political and Social Life*, 10. Basım, Princeton University Press, New Jersey 1997, s. 7.

ölçekli, disiplinlerarası ve dinamik yapısı, artan insan faaliyetlerinin etkisi sonucu ekolojik, ekonomik ve kurumsal süreçlerin analitik entegrasyonu için çerçeve sunmakta ve zorunlu olarak ölçek ve disiplin sınırlarını aşmaktadır.[312] Karmaşık Uluslararası İlişkiler Teorisi çalışmalarının ekseriyeti, uluslararası yaşamın karmaşıklığını kavrayabilme aracı olarak amil tabanlı modellemeleri ve matematiksel algoritmalar ile veri setlerine dayanan bilgisayar simülasyonlarını desteklemektedir.[313]Amiller sistemlerde bulunurlar ve onlara bağlıdırlar, ancak sistemler amiller tarafından oluşturulur ve değiştirilebilirler. Tüm amiller eşit çalışmamakla birlikte aynı sınırlamalara da sahip olmayabilirler ve göreceli ağırlıkları değişkenlik gösterebilir. Karmaşık Uluslararası İlişkiler Teorisi, savunduğu argümanlar ve öncelikleriyle söz konusu nüansları yakalayabilmek için uygun görülmektedir.[314]

Karmaşık Uluslararası İlişkiler Teorisi, Dördüncü Büyük Tartışmanın belirleyici teorisi olan İnşacılığın (*Constructivism*) "farklı perspektifleri biraraya getiren" mozağini, Siyaset Biliminin ontolojik alanının dışına çıkararak daha geniş yaşam sistemleri bağlamında konumlandırmaktadır. Dördüncü Büyük Tartışmadaki uluslararası yaşama yönelik çalışmaların temel olarak birbirine bağımlı ve örtüşen sosyal düzen kümelerinden oluşması, "insani" ve "insan dışı" sistemler arasındaki yanlış ikilemin sürdürülmesine neden olmuştur.[315] Karmaşık Uluslararası İlişkiler Teorisi, Beşinci Büyük Tartışmayı çizerek yanlış biçimlendirilen ontolojik tartışmaya devam etmek yerine yeniden formüle ederek ek çalışmalar, farklı ve karmaşık alanlardan tamamlayıcı okumalarla bir tür güncelleme sağlamaktadır. Sonuç olarak; karmaşıklığı Uluslararası İlişkilere uygulayan bu genel bakış, uluslararası yaşama dair yapılan çalışmaların karmaşık sistemler açısından düşünülmesini sağlamaktadır. Oldukça yeni olan bu yaklaşım, karmaşıklığın metodolojik araçlar aracılığıyla yapılandırılabileceğini belirtmektedir. Buna göre karmaşıklık hali

---

[312] Crawford S. Holling, Lance H. Gunderson & Donald Ludwig, "In Quest of a Theory of Adaptive Change", Editörler: Lance H. Gunderson & Crawford S. Holling, *Panarchy: Understanding Transformations in Human and Natural Systems*, 3. Basım, Island Press, Washington DC 2002, s. 5.
[313] Emilian Kavalski, *a.g.m.*, s. 447.
[314] Walter C. Clemens Jr., *Complexity Science and World Affairs*, 1. Basım, State University of New York Press, New York 2013, s. 30.
[315] Hayward R. Alker, "On Learning From Wendt", *Review of International Studies*, Cilt 26, Sayı 1, 2000, ss. 142-143.

düzenlenememekte, sadece tecrübe edilebilmektedir. Geleneksel Uluslararası İlişkiler anlayışını karmaşıklık kalıplarıyla karşı karşıya getiren bu teori, nesnelerin bilgisini bağlamlarından ayırmakta ve nesneler arasında ayrım yaparken onları birbirine daha bağlı hale getirmektedir.[316] Bundan dolayı, uluslararası yaşamın karmaşıklığını anlama girişimleri, Uluslararası İlişkilerde "Beşinci" olarak nitelendirilen diğer büyük tartışma sürecini başlatmıştır.

[316] Marie-Joelle Browaeys & Walter Baets, "Cultural Complexity: A New Epistemological Perspective", *The Learning Organization*, Cilt 10, Sayı 6, 2003, s. 335.

İKİNCİ BÖLÜM

SİBER UZAY VE ULUSLARARASI İLİŞKİLER

"Siber Uzay", 21. yüzyılın en temel gerçekliği olarak görülmektedir. Gelişmiş toplumlarda neredeyse herkes bu gerçekliğin farkındayken, gelişmekte olan toplumlarda da söz konusu farkındalığın boyutu her geçen gün hızla artmakta ve 21. yüzyılın bu yeni sahasının yaşamın her boyutuna doğrudan dâhil olduğu gerçeğiyle tekrar tekrar yüzleşilmektedir. Yaygınlığı, ölçeği ve kapsamı dikkate alındığında, milyonlarca bilgisayarı anlık zaman biriminde dünyanın her yerinden birbirine bağlayan İnternet ağı, bu ağın yönetimi ve sağladığı deneyimler de hesaba katıldığında, insanlığın yaratılan bu yeni gerçeklik sahasına geri dönülemez şekilde eklemlendiği görülmekte ve etkilerinin hangi boyutlara ulaşabileceği dahi öngörülemeyen belirsizliklerle dolu bu sürecin detaylı olarak gözlenmesini elzem kılmaktadır. Bu gereklilik; Sosyal, Fen ve Sağlık Bilimleri kapsamındaki tüm alanların herhangi bir boyutunun siber saha ortamlarıyla illa bir şekilde kesiştiği tecrübeleriyle apaçık hale gelmiştir. Uluslararası İlişkiler disiplini açısından bakıldığında ise Uluslararası İlişkilerin herhangi bir boyutundan ziyade tüm boyutlarıyla siber saha ortamları arasında doğrudan, güçlü, dinamik ve karmaşık bir etkileşim hali olduğu görülmektedir. Öyle ki; siber uzay sahasının göstermiş olduğu hızlı değişim ve yaratmış olduğu ciddi gelişmelerin önemi tam olarak idrak edilemeden sürekli olarak yeni değişimleri beraberinde getirmesi, 20. yüzyıl Uluslararası İlişkileri ile 21. yüzyılın gerçeklikleri arasında güçlü bir kopukluk halinin yaşanmasına vesile olmuştur. Buna bağlı olarak Uluslararası İlişkilerin, ulusal güvenliğin, dünya politikasının ve küresel sistemin siber özelliklerini daha geniş ve karmaşık bir şekilde tanımlayarak kurgulayan tamamen yeni bir kelime dağarcığı ortaya çıkmıştır.[317] Söz konusu yeni kelime dağarcığının Uluslararası İlişkiler perspektifinden en iyi şekilde anlaşılabilmesi adına bu bölümde öncelikle Uzay sahası, Dış Uzay ve Siber Uzay boyutlarıyla ele alınacak, ardından Siber Uluslararası

[317] Chintan Vaishnav, Nazli Choucri & David Clark, "Cyber International Relations as an Integrated System", *Environment Systems and Decisions*, Cilt 33, Sayı 4, Kasım 2013, s. 561.

İlişkilere dair temel kavramlar detaylandırılacak, sonrasında Siberpolitik incelenecek ve nihayetinde de uluslararası siber düzenlemeler, anlaşmalar, organizasyonlar ve işbirlikleri incelenecektir.

1. Uzay Sahası

1950'li yıllara kadar uzay sahası üzerine yapılan gözlem ve araştırmalar yeryüzüyle sınırlı kalmış ve "Uzay" (*Space*) kavramının kullanımı, Dünya gezegenini de bünyesinde barındıran geniş alanı belirtme gayesiyle tercih edilmiştir. Öyle ki, 1950 sonrasında –özellikle 1957 yılında SSCB'ye ait olan *Sputnik I* ve *Sputnik II* isimli dünyanın ilk yapay uydularının Dünya yörüngesine başarıyla oturtulmasının ardından– ABD ile SSCB arasında başlayan uzay çalışmalarına yönelik teknolojik rekabet, uzay sahasının kavram olarak kullanımını daha katmanlı bir hale getirmiştir.[318] Özellikle bu dönemden itibaren bilim insanları ve mühendisler tarafından gerçekleştirilen uzay çalışmaları ve misyonları neticesinde Güneş Sistemindeki çeşitli gezegenlere ve hatta Dünya'ya yakın çeşitli asteroitlere ve gök cisimlerine insanlı ve insansız görevler gerçekleştirilmiştir. Çok sayıdaki araştırma ve geliştirme –aynı zamanda Birinci Bölümde bahsedilmiş olan bilim, teknoloji ve Uluslararası İlişkilerin karşılıklı etkileşiminin neticesi olarak da değerlendirilebilir– sayesinde insanlık, Kozmoloji bilimini geliştirmiş ve uzaya dair derin bilgilere sahip olmuştur. Öyle ki bu doğrultuda, uluslararası sistemin ana aktörleri tarafından Uzay sahasına yönelik büyük bir endüstriyel değişim teşvik edilmiştir.[319] Söz konusu hızlı ve karmaşık bilimsel ve teknolojik ilerlemeler bağlamında edinilen bilgiler ve oluşturulan literatür ışığında Uzay sahasının iki ana katmanından ayrı ayrı bahsetmek mümkün olmuştur: Yeryüzünün atmosferik yapısı dışında kalan kısmı niteleyen "Dış Uzay Sahası" (*Outer Space Domain*) ve bilgi teknolojileri altyapılarının bağımsız ağlarını içeren küresel etkinlik alanını niteleyen "Siber Uzay Sahası" (*Cyberspace Domain*).

---

[318] Redmond Kathleen Molz & Phyllis Dain, *Civic Space / Cyberspace: The American Public Library in the Information Age*, The Massachusetts Institue of Technology Press, Cambridge, Massachusetts 1999, s. 129.

[319] Edythe E. Weeks, Esq., *Outer Space Development, International Relations and Space Law: A Method for Elucidating Seeds*, Cambridge Scholars Publishing, Newcastle 2012, s. 1.

1.1. Dış Uzay Sahası

Dış Uzay sahası, en genel ifadeyle, yeryüzünün atmosferik hava sahasının bittiği yerden başlayan alanı ifade etmektedir; ancak yeryüzünün atmosferik hava sahasının bitiş noktası ile Dış Uzay sahasının başlangıç noktasını birbirinden ayıran sınır çizgisinin nasıl baz alınacağına dair tam netlik olmamakla birlikte çok çeşitli öneriler ve görüşler sunulmuştur.[320] Söz konusu öneri çeşitliliği içerisinde en fazla benimsenen görüşe göre; hava sahası ile Dış Uzay sahası arasındaki sınır çizgisini, yapay bir uydunun en az bir kez Dünya yörüngesine yerleştirilebileceği maksimum 100 millik (yaklaşık 161 km) irtifa mesafesinin oluşturduğu belirtilmiştir.[321] Uluslararası İlişkiler açısından bakıldığında ise I. Dünya Savaşı'ndaki savaş stratejilerinin, hava sahasını kontrol etmek için kullanılan iletişim ve ulaşım teknolojilerinin, II. Dünya Savaşı'nda geliştirilen roket teknolojileriyle beraber hava sahasında uzun menzilli güç kullanımına evrilmesi, hava sahasının hem serbest hem de paylaşımlı özelliğinin çelişkileri üzerinden gelişmiştir. Bunun üzerine de hava sahasının güvenliğinin sağlanması girişimleri savaş nedeni haline gelirken, hava sahası özgürlüğünün sağlanabilmesi adına geliştirilen "hava gücü" (*air force*) yeni askeri güç aracına dönüşmüştür. Bilhassa II. Dünya Savaşı sonrası dönemde hava sahası ötesindeki dış uzay sahasının yeni bir müspet alan olarak keşfedilmesi ya da icat edilmesi, egemenliğin dikey sınırlarının icadını da beraberinde getirmiş ve dünyayı barış ve iletişimle yönetebilmenin temel hedefini bu sahaya kaydırmıştır.[322] Dış uzay sahasının uluslararası aktörler tarafından kullanılış bağlamı ise hızla ve potansiyel olarak farklı yönlerde gelişmiştir. Örneğin; ulusal ve uluslararası altyapıların kritik unsurlarının –medya, iletişim araçları, çevresel izleme vb.– sağlanabilmesi için uzaya dayalı teknolojilerin artan kullanımı, uzaya dayalı askeri destek unsurlarına artan bağımlılığı da beraberinde getirmiştir. Aynı zamanda da dış uzay sahasının erişim ve kullanımına ilgi duyduğunu iddia eden aktörler; devletleri,

---

[320] John A. Vosburgh, "Where Does Outer Space Begin?", *American Bar Association Journal*, Cilt 56, Sayı 2, Şubat 1970, s. 135.
[321] J. F. McMahon, "The Legal Aspects of Outer Space", *The World Today*, Cilt 18, Sayı 8, Ağustos 1962, s. 330.
[322] James Hay, "The Invention of Air Space, Outer Space, and Cyberspace", Editörler: Lisa Parks & James Schwoch, *Down to Earth: Satellite Technologies, Industries, and Cultures*, Rutgers University Press, New Jersey 2012, s. 28.

bölgesel örgütleri ve özel girişimleri de kapsayacak şekilde hızla çoğalmıştır.[323] Dış uzayın tecrübe edilmesiyle kozmosun muazzam büyüklüğü siyasallaşarak farklılaşmış ve rekabet edilebilir hale evrilmiştir. Bu durum sadece dış uzay teknolojilerine ve gelişmelerine yönelik daha titiz ve detaylı ampirik sosyal bilim araştırmalarını ve teori geliştirilmesini kolaylaştırmakla kalmamış, aynı zamanda da küresel müştereklerin devam eden özelleştirme ve militarizasyon süreçlerinin risklerini de ortaya çıkarmıştır.[324] Bilimsel ve teknolojik gelişmelerin dış uzay sahasına kadar uzanması ve yeni riskleri doğurması neticesinde uluslararası hukukun da dış uzay sahasına yayılması gerekli kılınmış ve 1967 yılında "Dış Uzay Anlaşması" (*The Outer Space Treaty, OST*)[325] imzalanmıştır. Uluslararası hukuk alanında dış uzay hukuku ilkelerinin temelini oluşturması ve dış uzay sahasının yönetimi açısından ilk en önemli belge olan *OST*, Birleşmiş Milletler Dış Uzayın Barışçıl Amaçlarla Kullanımı Komitesi'nde (*United Nations Committee on the Peaceful Uses of Outer Space, UN-COPUOS*) ve ayrıca BM Genel Kurulu'nda (*United Nations General Assembly, UN-GA*) yapılan uzun müzakerelerin ve tartışmaların sonucunda gerçekleşmiştir.[326] Ardından da dış uzay sahasının kontrol, yönetim, ticaret ve istihbarat boyutlarına yönelik çok sayıda uluslararası anlaşma, işbirliği ve projeler devam edegelmiştir; ancak özellikle balistik silahlar, uzay fırlatıcıları ve füze savunma programı teknolojilerinde yaşanan hızlı ilerlemeler, dış uzay sahasının güvenliğini her şeyden önce gelen küresel bir güvenlik meselesi haline getirmiştir ve ciddiyetini de halen korumaktadır.[327] Öte taraftan ise dış uzay sahasına yönelik teknolojilerde yaşanan gelişmeler ışığında kara, deniz, hava ve dış uzay sahasını çeşitli şekillerde kapsayabilen ve elektromanyetik spektrumda kesişen

---

[323] Columba Peoples, "The Securitization of Outer Space: Challenges for Arms Control", *Contemporary Security Policy*, Cilt 32, Sayı 1, s. 76.
[324] Julie Michelle Klinger, "Environmental Geopolitics and Outer Space", *Geopolitics*, Cilt 24, Sayı 1, 2019, s. 2.
[325] United Nations, Office for Outer Space Affairs, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies", *https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html*, (Erişim Tarihi: 4 Şubat 2020).
[326] Biswanath Gupta & Ekta Rathore, "United Nations General Assembly Resolutions in the Formation of the Outer Space Treaty of 1967", *Astropolitics*, Cilt 17, Sayı 2, s. 77.
[327] Hugo L. E. Meijer, "Reflections on Politics, Strategy and Norms in Outer Space", *Defense & Security Analysis*, Cilt 25, Sayı 1, s. 94.

alanları kullanabilen benzersiz özelliklere sahip yepyeni bir saha yaratılmıştır: "Siber Uzay".

1.2. Siber Uzay Sahası

"Siber Uzay" (*Cyberspace*), kuşkusuz bugünün dünyasındaki kamu söyleminin en çok merak uyandıran ve düşündüren terimlerinin başında gelmektedir. Giderek genişleyen etkisinin lehinde ve aleyhinde güçlü argümanlar geliştirilmektedir. Örneğin; siber uzay sahası ile oluşturulan bağlantısallık (*connectivity*) halinin, insanların düşünme biçimlerinden temel insan doğasına dek "her şeyi değiştirdiği" şeklindeki büyük boyutlu etkisel yaklaşımlar olduğu kadar, insanların her zaman yaptıkları şeyleri sadece biraz daha farklı şekillerde yapabilme kolaylığı sağladığı şeklindeki küçük boyutlu etkisel yorumlar da söz konusudur.[328] Kara, hava, deniz ve dış uzay sahası gibi küresel müşterekler ile birlikte siber uzay sahası da önemli bir stratejik alan olarak tanımlanmaktadır. Buna karşın, birçok açıdan diğer sahalara kıyasla farklılıklar göstermektedir. Öne çıkan en dikkat çekici özelliği "tamamen insan yapımı tek ortam" olmasına dayanmaktadır. Dolayısıyla siber uzay sahası tanımlamalarında "yapaylık" (*artificiality*) söz konusudur. Her ne kadar bilgisayarlar, akıllı telefonlar vb. teknolojik araçlar arasındaki etkileşimi destekleyen altyapı boyutu insandan bağımsız salt teknolojik alan olarak sunulsa da çıkış noktası itibariyle tüm teknolojik ve makinesel araçlar ve altyapılar insanlar tarafından geliştirilmektedir. Bu sebeple siber uzay sahasının insanlar tarafından yapılan makineler katmanın üzerinde insan-makine iletişim katmanlarının bulunduğu ve siber uzay sahasının tamamen insanlık tarafından inşa edildiği söylemi yerinde bulunmaktadır.[329]

"Siber" (C*yber*) kelimesinin tarihsel ve felsefi kökeni genellikle Platon'un "Devlet"indeki mağara alegorisine dayandırılmakla birlikte modern çağ açısından semantik kimliğinin dayanağını iletişim ve kontrol teorisi çalışmalarını meşhur kılan Norbert Weiner'in *Cybernetics: Or Control and Communication in the Animal and*

[328] David J. Betz & Tim Stevens, "Chapter Three: Cyberspace and War", *Adelphi Series, Cyberspace and the State: Toward a Strategy for Cyber-power*, Cilt 51, Sayı 424, 2011, s. 75.
[329] David J. Betz & Tim Stevens, "Chapter One: Power and Cyberspace", *Adelphi Series, Cyberspace and the State: Toward a Strategy for Cyber-power*, Cilt 51, Sayı 424, 2011, s. 35.

Machine[330] isimli eseri oluşturmaktadır. Sibernetik ve uzay kavramlarını birbirine bağlayan ve çoğunlukla "Siber Uzay" olarak bilinen yeni etkileşim alanının ilk resmi adlandırmasının kaynağı olarak ise William Gibson'ın *Neuromancer*[331] adlı romanı gösterilmektedir.

İnsan etkileşimi açısından yeni bir alan haline gelen siber uzay, gücün dönüşümü ve yayılması analizinin ayrılmaz bir parçası olarak kabul görmektedir. Teknolojinin karma karakteri, deniz altındaki kablolar ve ulus-devletlerin topraklarında konumlandırılan fiziksel cihazlar arasındaki bilgi aktarımına dayanan ulusötesi sanal bir yapıya dayanmaktadır. Diğer stratejik sahalara –kara, deniz, hava ve dış uzay– kıyasla yapaylık özelliği bulunan siber uzayın yapısı değiştirilebilmektedir.[332] Siber uzaya yönelik çeşitli ülkelerin strateji belgelerinde yapılan tanımlamalara bakıldığında ise bir tutarlılık olduğu tespit edilmiştir. Örneğin; 2018 tarihli ABD Siber Güvenlik Stratejisi belgesine göre Siber Uzay; "İnternet, telekomünikasyon ağları, bilgisayarlar, bilgi ve iletişim sistemleri, gömülü işlemciler ve denetleyiciler dâhil olmak üzere birbirine bağlı bilgi teknolojisi altyapısı ağı"[333] olarak tanımlanmıştır. Yine 2018 tarihli Kanada Ulusal Siber Güvenlik Strateji belgesinde ise Siber Uzay; "birbirine bağlı bilgi teknolojisi ağları tarafından oluşturulan elektronik dünya ile bu ağlardaki bilgiler ve üç milyardan fazla insanın fikir, hizmet ve dostluk alışverişi için birbirine bağlandığı küresel bir müşterek"[334] şeklinde ifade edilmiştir. Diğer taraftan kendisini "dijital/dijitalize toplum" (*digitalised society*) olarak tanımlayan İngiltere'nin Ulusal Siber Güvenlik Stratejisi belgesine bakıldığında Siber Uzay sahasının "İnternet, bilgisayarlar ve akıllı telefonların ötesinde diğer siber-fiziksel veya akıllı sistemlerin –güç şebekeleri, hava trafik kontrol sistemleri, uydular, tıbbi teknolojiler, endüstriyel tesisler, trafik ışıkları

---

[330] Norbert Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine*, The Massachusetts Institute of Technology Press, 4. Basım, Massachusetts 1985, ss. 11-12.
[331] William Gibson, *Neuromancer*, (The Sprawl – 1), Ace Science Fiction Books, New York 1984.
[332] Hannes Ebert & Tim Maurer, "Contested Cyberspace and Rising Powers", *Third World Quarterly*, Cilt 34, Sayı 6, 2013, s. 1054.
[333] U.S. Department of Homeland Security, "Cybersecurity Strategy", 15 Mayıs 2018, *https://www.dhs.gov/publication/dhs-cybersecurity-strategy*, (Erişim Tarihi: 9 Şubat 2020), s. 1.
[334] Government of Canada, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*, Public Safety Canada, ISBN: 978-0-660-26553-7, 2018, s. 34.

vb.– birbirine bağlandığı yeni teknolojik saha"[335] olarak tanımlandığı görülmektedir. Japonya'nın 2015 tarihli Siber Güvenlik Strateji belgesinde "Japonya'nın sosyo-ekonomik faaliyetlerinin önemli bir temeli" olarak nitelendirilen Siber Uzay sahası, "*ulusal sınırlara bakılmaksızın serbest fikir alışverişinin yapılabildiği yapay bir alan ve küresel olarak değiştirilen fikirlerden esinlenen entelektüel yatırımların ve yeniliklerin yarattığı sonsuz değerlerin dijital sınırı*"[336] şeklinde ifade edilmektedir. Türkiye'nin Ulusal Siber Güvenlik Strateji belgesinde ise Siber Uzay sahasının "tüm dünyaya ve uzaya yayılan bilgi sistemlerinden, bu sistemleri birbirlerine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam"[337] şeklinde geçtiği tespit edilmiştir.

Yakın zamana kadar Siber Uzay; rutin kararları, süreçleri ve arka plandaki koşulları belirtmek için kullanılan düşük politika (*low politics*) meselesi olarak görülmüştür. Buna karşılık 21. yüzyıl itibariyle siber uzay; devletlerin çıkarları ve temel değerleri için kritik öneme sahip olan ulusal güvenlik, ana kurumlar ve karar sistemleri ile ilgili yüksek politika (*high politics*) konusu haline gelmiştir. Çeşitli ülkelerdeki huzursuzluk dönemlerinde İnternetin kısıtlanması, gizli hükümet belgelerinin sanal ortamda sızdırılması, nükleer yeteneklerin azaltılması adına gerçekleştirilen saldırılarda siber tabanın kullanılması gibi çok sayıdaki örnek üzerinden bu durumun doğrulandığı görülmektedir.[338] Siber alanın sağladığı genellikle şeffaf olmayan ara bağlantılar ile Geleneksel Uluslararası İlişkiler ve güç politikaları, ulusal güvenlik, sınırlar gibi bir dizi kavram ve bunlara karşılık gelen gerçeklikler sorgulanır hale gelmiştir. Bu bağlamda Siber Uzay sahasının birçok özelliği, Çağdaş Uluslararası İlişkilere dair teoriyi, politikayı ve uygulamayı yeniden şekillendirmektedir. Tablo 12'de görüldüğü üzere; zaman, mekân, geçirgenlik, akışkanlık, katılım, ilişkilendirme, hesap verebilirlik ve aynı anda her yerde bulunabilme ile ilgili olan özellikleri en çok öne çıkan ve en ciddi kabul edilenler

---

[335] HM Government, "National Cyber Security Strategy 2016-2021", 1 Kasım 2016, *https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021*, (Erişim Tarihi: 9 Şubat 2020), s. 13.

[336] The Government of Japan, "Cybersecurity Strategy", 4 Eylül 2015, *https://www.mofa.go.jp/policy/page18e_000015.html*, (Erişim Tarihi: 9 Şubat 2020), s. 3.

[337] Republic of Turkey, Ministry of Transport Maritime Affairs and Communications, "2016-2019 National Cyber Security Strategy", 2016, *https://www.uab.gov.tr/siber-guvenlik*, (Erişim Tarihi: 9 Şubat 2020), s. 7.

[338] Chintan Vaishnav, Nazli Choucri & David Clark, *a.g.m.*, s. 561.

olmuştur. Bireysel olarak bakıldığında, yukarıda belirtilen her bir özelliğin ortak sosyal gerçeklik anlayışıyla ve Uluslararası İlişkilerin çağdaş anlayışıyla uyuşmadığı görülmekle birlikte müşterek olarak ele alındığında ise güçlü bir kopukluğa işaret ettiği tespit edilmektedir.[339]

Tablo-12: Siber Uzayın Özellikleri

Zamansallık (*Temporality*) – Geleneksel zamansallığın yerini neredeyse anlıklıkla değiştirir.
Fiziksellik (*Physicality*) – Coğrafya ve fiziksel konum kısıtlamalarını aşar.
Geçirgenlik (*Permeation*) – Sınırlara ve yetki alanlarına nüfuz eder.
Akışkanlık (*Fluidity*) – Sürekli değişimleri ve yeniden yapılandırmaları gösterir.
Katılım (*Participation*) – Aktivizm ve politik ifade önündeki engelleri azaltır.
Atıf (*Attribution*) – Aktörlerin kimliklerini ve eylem bağlantılarını gizler.
Hesap verebilirlik (*Accountability*) – Sorumluluk mekanizmalarını atlar.

Kaynak: Nazli Choucri, *Cyberpolitics in International Relations*, The Massachusetts Institute of Technology Press, Massachusetts 2012, s. 4.

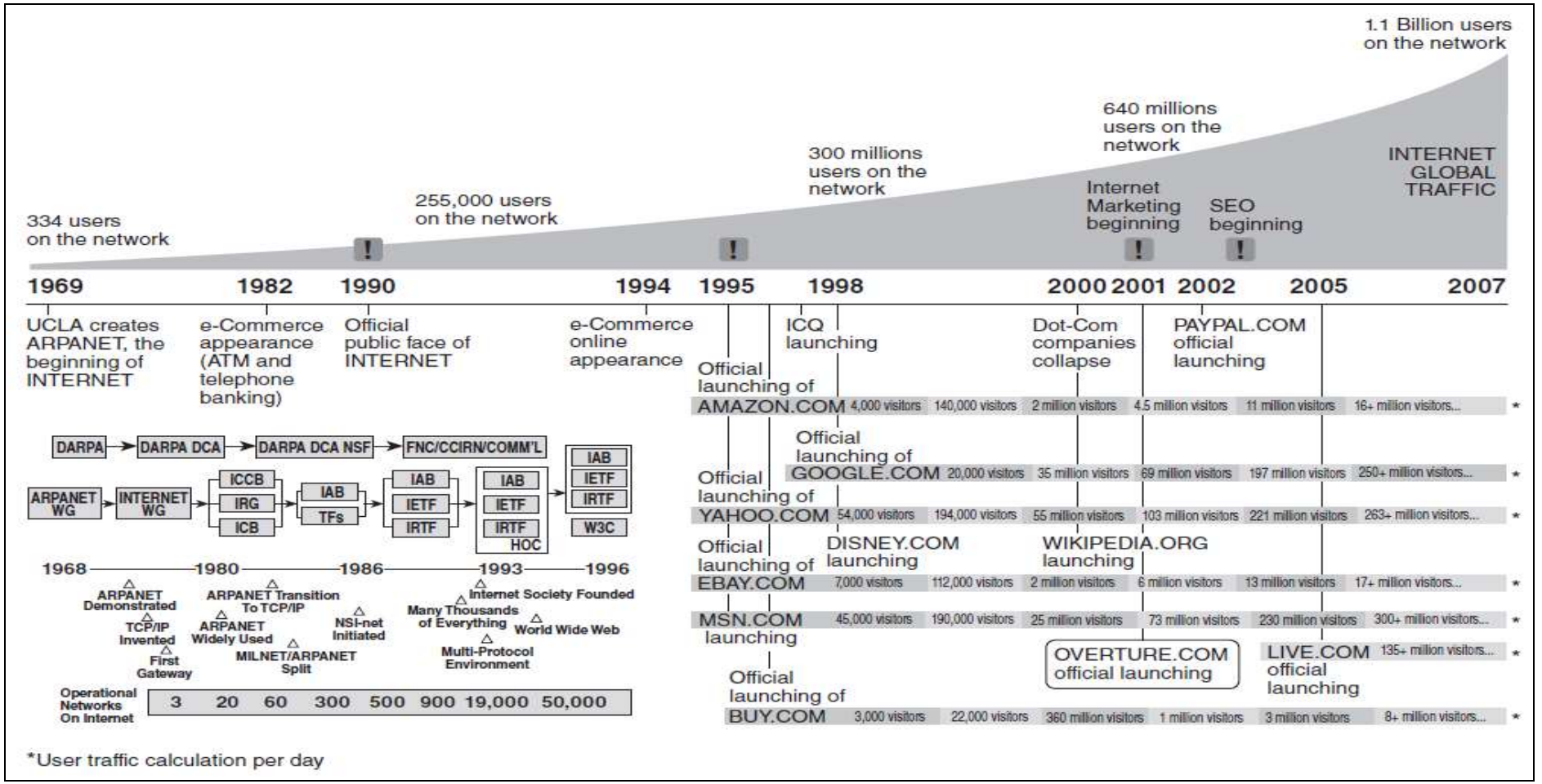
Siber alan, "sanal gerçeklik" (*virtual reality*) sahası olarak nitelendirilmektedir. "Sanal" (*virtual*) ile "gerçekte veya resmen olmasa da özünde ya da etkisinde öyle olmak"; "gerçek" (*real*) ile de "nesnel bir mevcudiyete sahip olmak ve aslında bir şey olarak var olmak" kastedilmektedir.[340] Manuel Castells, gerçeklik ile sembolik temsil arasında hiçbir ayrım olmadığı ve bütün toplumlarda da insanlığın sembolik bir ortamda varlığını sürdürdüğü gerçeğinden hareketle gerçekliğin her zaman sanal olduğunu belirtmektedir; çünkü sanallık, uygulamaları sembollerin katı semantik tanımlarından kaçan bir anlamla çerçeveleyerek algılamaktadır. İnsan söylemlerinin polisemik karakteri sayesinde insan zihnindeki mesajların karmaşıklığı ve hatta çelişkili kalitesi kendisini göstermektedir.

[339] Nazli Choucri, *Cyberpolitics in International Relations*, The Massachusetts Institute of Technology Press, Massachusetts 2012, ss. 3-4.
[340] "Virtual" için bkz.: William Little, H. W. Fowler & J. Coulson, *a.g.e.*, s. 2361.; "Real" için bkz.: William Little, H. W. Fowler & J. Coulson, *a.g.e.*, s. 1665.

Mesajların anlamının kültürel çeşitliliği, insanların birbirleriyle çeşitli boyutlarda – bazıları açık, bazıları ise örtülü olarak– etkileşime girmelerini sağlamaktadır. Bu nedenle, elektronik medya eleştirmenleri yeni sembolik ortamın "gerçekliği" temsil etmediğini iddia etmesine rağmen örtülü bir şekilde asla var olmayan "kodlanmamış" gerçek deneyim kavramını ima ederler. Dolayısıyla bütün gerçekler sembollerle iletilir ve insanlarla etkileşimli iletişimde, ortamdan bağımsız olarak tüm semboller atanan anlamsal anlamlarına göre bir miktar yer değiştirir. Bir anlamda, tüm gerçeklik sanal olarak algılanmaktadır.[341]

[341] Manuel Castells, *The Information Age: The Rise of Network Society (Volume 1)*, 2. Basım, Blackwell Publishers, Oxford 1996, ss. 403-404.

Tablo-13: Siber Uzayın Evrimi



Kaynak: Nazli Choucri, *Cyberpolitics in International Relations*, The Massachusetts Institute of Technology Press, Massachusetts 2012, s. 50.

Tablo 13'e bakıldığında siber uzay sahasının kilit kurumlar, ana sonuçlar ve operasyonel ağlar odaklı evriminin bir zaman çizelgesi bağlamında ve daha net anlaşılabilecek şekilde sunulduğu görülmektedir. Siber alanının haritalandırılması oldukça zor olmakla birlikte genellikle mekânsal modeller, sinir ağları, örümcek ağı benzeri sistemler ve çok katmanlı yapılar gibi çeşitli ifadelere ve modellemelere dayandırılmaktadır. 1969 yılı itibariyle başlayan siber uzay alanın inşa süreci 1990 sonrasında güçlü politik çıkarımlar göstererek öncelikle ekonomik aktivitelerin bu alan içerisindeki operasyonel ağlara katılmasını sağlamıştır. 2000 sonrası dönemde yaşanan gelişmeler ışığında ise sadece "21. Yüzyıl Siber Çağı"nı karakterize eden bölgesel sınırların geçirgenliği değil, aynı zamanda kimin iletim yaptığı, neyin iletildiği, ne zaman, nasıl ve hangi etkilerle gerçekleştiğine dair kontrol olanakları hakkındaki yaygın belirsizliklerin daha da derinleştiği evre başlamıştır. Dış uzay sahasında önemli aktör pozisyonuna gelebilmek için dış uzay teknolojilerinin yetkinliğinin elzem olması, bu sahanın doğrudan ilgili yetkin aktörlerce kontrol edilebilmesine sınırlılık getirirken, buna karşılık sanal bir etkileşim alanı olarak siber uzaya erişimin prensip olarak herkese açık olduğu görülmektedir.[342] Öte yandan bilgisayarlar ile insan operatörleri arasında iletişim ve bilgi alışverişi için dijital sinyallerin gönderildiği, alındığı ve işlendiği küresel bir ortam olarak siber uzayın işleyiş anlayışı, taşıdığı trafiğin kalitesine ve anlamına kayıtsız kalması gerektiğine dayanmaktadır. Dolayısıyla siber uzay araçlarının meydan okuma, güvensizlik, istikrarsızlık, suç ve rekabet adına kullanılabilmesi şaşırtıcı olmamaktadır.[343]

Bilgiye dair yaşanan değişimlerin her zaman güç algısı üzerinde önemli etkileri olmuştur ancak siber uzay sahasının tamamıyla insan inşası olan yepyeni bir yapay ortam özelliğinin ve gelecekte insanlığın bu saha içerisinde nasıl konumlandırılacağına dair belirsizliğin güç algısına yansımaları çok daha derin olmuştur. Siber alanın karakteristiği, aktörler arasındaki güç farklılıklarının bir kısmını azaltarak 21. yüzyılın küresel ilişkilerini belirleyen güç dağılımına önemli bir örnek sağlamaktadır. Uluslararası İlişkilerdeki en güçlü aktörlerin diğer stratejik sahalara –kara, hava, deniz ve dış uzay– kıyasla siber uzay sahasına hâkim olma

[342] Nazli Choucri, *a.g.e.*, ss. 49-51.
[343] Paul Cornish, "Governing Cyberspace Through Constructive Ambiguity", *Survival: Global Politics and Strategy*, Cilt 57, Sayı 3, Haziran-Temmuz 2015, s. 153.

olasılığı düşük kalmaktadır. Ayrıca siber alan, gücün yayılmasının iktidar eşitliği ya da hükümetlerin dünya siyasetindeki en güçlü aktörler olarak yer değiştirmesi anlamına gelmediğini de gözler önüne sermektedir.[344] Siber Uzay sahası, bireylerden devletlere kadar çok farklı şekillerde ve boyutlarda aktörlere sahiptir. Aaron Franklin Brantly, siber uzayın yapısını Hobbes'un egemen güç/hükümet yokluğu doğa durumu yerine, siber alandaki devletlerin üzerindeki çevresel kısıtlamaların, yapısal realizmdeki geleneksel anarşik kısıtlamara yakın olduğu şeklinde değerlendirmektedir. Öyle ki, devletlerin siber alandaki diğer devletlerin dijital sınırlarını ihlal etmesini engelleyecek hiçbir şey bulunmamaktadır ve bu sebeple devletler hem saldırı hem de savunma araçlarını geliştirmeye doğru kaymaktadır.[345]

Siber alan, yerelden uluslararası arenalara kadar bir dizi ekonomik, sosyal ve politik düzenlemeyi tetiklemekle kalmamış, devletlerin etkileşim biçimlerini yönlediren en büyük endişelerden biri olarak güvenlik algısını daha da ön plana çıkarmıştır. Bilgi ve iletişim teknolojileri ile mevcut hiyerarşileri tamamlayan yatay ağların gelişimi teşvik edilerek uluslararası örgütleri, üyelerini ve bilgi toplumunun diğer paydaşlarının içerisinde yer aldığı her türlü ilişki ağı derinden etkilenmiştir.[346] Bu bağlamda Siber Uzay, sadece açık ulusal güvenlik aygıtının öğelerinin bulunduğu operasyonel bir alan değil, aynı zamanda da ulusal potansiyele daha temel bir düzeyde erişim için bir yol olarak da nitelendirilmektedir.[347]

Diğer taraftan dış uzay sahası ile siber uzay sahasına kıyaslamalı olarak bakıldığında ise bugünün dünyasındaki ülkelerin ekonomileri, toplumları ve yaşam tarzlarının doğrudan bu iki sahanın erişimine ve kullanımına dayandığı görülmektedir. Herhangi bir ulusun egemenliği ya da yargı yetkisi dışında kalan müşterek alanlar olarak bu sahaların uluslararası ticaret, iletişim ve yönetişim sisteminin altındaki temelin parçaları olduğu dikkate alınmalıdır. Dış Uzay ile Siber

---

[344] Joseph S. Nye, Jr., *Cyber Power*, Harvard Kennedy School, Belfer Center for Science and International Affairs, Report, Massachusetts Mayıs 2010, s. 1.
[345] Aaron Franklin Brantly, "The Cyber Losers", *Democracy and Security*, Cilt 10, Sayı 2, 2014, s. 133.
[346] James N. Rosenau, "Information Technologies and The Skills, Networks, and Structures that Sustain World Affairs", Editörler: James N. Rosenau & J. P. Singh, *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, State University of New York Press, New York 2002, s. 281.
[347] Christopher Whyte, "Power and Predation in Cyberspace", *Strategic Studies Quarterly*, Cilt 9, Sayı 1, Bahar 2015, s. 101.

Uzay alanları, sahip oldukları benzersiz özellikler sebebiyle ayrı alanlar olarak nitelendirilse de aralarında çok güçlü bir bağ bulunmaktadır: "Bilgi" ve "İstihbarat". 21. yüzyılda ekonomik refah ve askeri gücün öne çıkan lokomotifleri artık "bilgi" ve "istihbarat" olarak gösterilmektedir. Bu doğrultuda küresel ve ulusal savunma bilgi altyapılarının ayrılmaz parçası haline evrilen Dış Uzay ve Siber Uzay sahaları, aktörlerin sahip oldukları saha yetenekleri kapsamında enerji, finans, ulaşım ve telekomünikasyon gibi hemen hemen her sektörde siber fiziksel varlıkları kontrol ederek küresel çapta bilgi ve istihbarat toplayabilmekte, üretebilmekte ve iletebilmektedirler.[348]

2. Siber Uzaya Dair Temel Kavramlar

21. yüzyılın belirsizlikler dolu bu yeni siber etkileşim alanı, mevcut Uluslararası İlişkiler terminolojisine ek olarak geliştirmiş olduğu kendi lisanıyla yepyeni bir saha sözlüğü oluşturmuştur. Bu sözlüğün kapsamındaki kavramların bir kısmı mevcut Uluslararası İlişkiler sözlüğünün siber alana uyarlaması şeklinde gerçekleşirken, bir kısmı da bu alanın benzersiz özelliklerine bağlı olarak sıfırdan türetilmiştir. Bu bağlamda söz konusu siber uzay sahasının daha idrak edilebilmesi adına en fazla ön plana çıkan kavramlar şu şekilde tespit edilmiştir: "İnternet"; "Siber Tehdit"; "Siber Saldırı"; "Siber Casusluk"; "Siber Suç"; "Siber Terör"; "Siber Savaş"; "Siber Güvenlik".

2.1. İnternet

21. yüzyıl, bilgi ve iletişim teknolojilerinin küresel olarak şüphesiz en etkileyici yayılma hızına ulaştığı dönem olmaktadır. İnternet, e-posta, uydu televizyonları ve mobil telefonlar gibi temel enstrümanlar sayesinde bilgi ve iletişim teknolojilerinin ilerlemesi ve birbirine olan bağlılığı giderek güçlenmekte ve derinleşmektedir. Bu süreçte ise en çarpıcı örneği tartışmasız "İnternet"

[348] Marc J. Berkowitz, "Shaping the Outer Space and Cyberspace Environments", Editör: Scott Jasper, *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, Georgetown University Press, Washington, D.C. 2012, ss. 157-158.

oluşturmaktadır.[349] İnternetin (*Internet*) ortaya çıkışına yönelik çok farklı görüşler bulunmakla birlikte genel kanı "nükleer saldırıya dayanabilecek bir iletişim olasılığı yaratmak için İnternetin temel olarak ABD askeri yetkilileri tarafından tasarlandığı" yönündedir. Buna karşın Jon Bing, bu kanının yanlış olduğunu ve aslında "nükleer savaş durumunda iletişim sorununun sadece orduyu değil, bilimsel topluluğun bazı bölümlerini de doğrudan endişelendirdiğini ve esasında bu endişe halinin iletişim ağı yapımında yarattığı zorlu sorunların" İnternetin gelişim hikâyesinin başlangıç noktasını oluşturduğunu belirtmektedir.[350] Benzeri görülmemiş teknolojik yeniliklerin en kapsamlı neticesi olarak İnternet, başta mühendisler ve bilgisayar bilimciler olmak üzere çok farklı alanlardan ve açılardan ele alınmıştır. İnternetin başarısının en önemli yönlerinden biri olarak ise coğrafi olarak dünyanın dört bir yanına dağılmış bilgisayar ağlarının birbirine eş zamanlı bağlanmasını sağlayan yönetim ve yönetişim düzenlemelerinin oluşturulması gösterilmektedir.[351] Buna karşın, başlangıçta bilgisayar ağlarının makine, kurum ve proje türlerine özgü olduğu ve İnternetin ortaya çıktığı dönemde bu ağların ağı şeklinde geliştirildiğinin de belirtilmesi gerekir. Yani programcıların müşteri hedefleri doğrultusunda özellikle tek bir bilgisayar için oluşturdukları işletim sistemleri ve benzer şekilde mühendisler ve mimarlar tarafından kendi özel amaçları için muazzam çeşitlilikte inşa edilen her ağ, İnternetin ortaya çıkmasıyla birlikte birbirine bağlanmıştır.[352]

Yukarıda da belirtildiği üzere İnternetin başlangıç noktasını oluşturan endişe halinden yola çıkarak sürecin ilerlemesindeki odak noktası, ABD Savunma Bakanlığı'nın (*U.S. Department of Defense, DoD*) ARPANET'i finanse etmesine dayanmaktadır. "ARPA", İleri Araştırma Projeleri Ajansı'nın (*Advanced Research Projects Agency*) kısaltmasıdır ve ilerleyen süreçte "DARPA" yani Savunma İleri Araştırma Projeleri Ajansı'nın (*Defense Advanced Research Projects Agency*)

---

[349] Johan Eriksson & Giampiero Giacomello, "Introduction: Closing the Gap Between International Relations Theory and Studies of Digital-Age Security", Editörler: Johan Eriksson & Giampiero Giacomello, *International Relations and Security in the Digital Age*, 1. Basım, Routledge, New York 2007, s. 1.

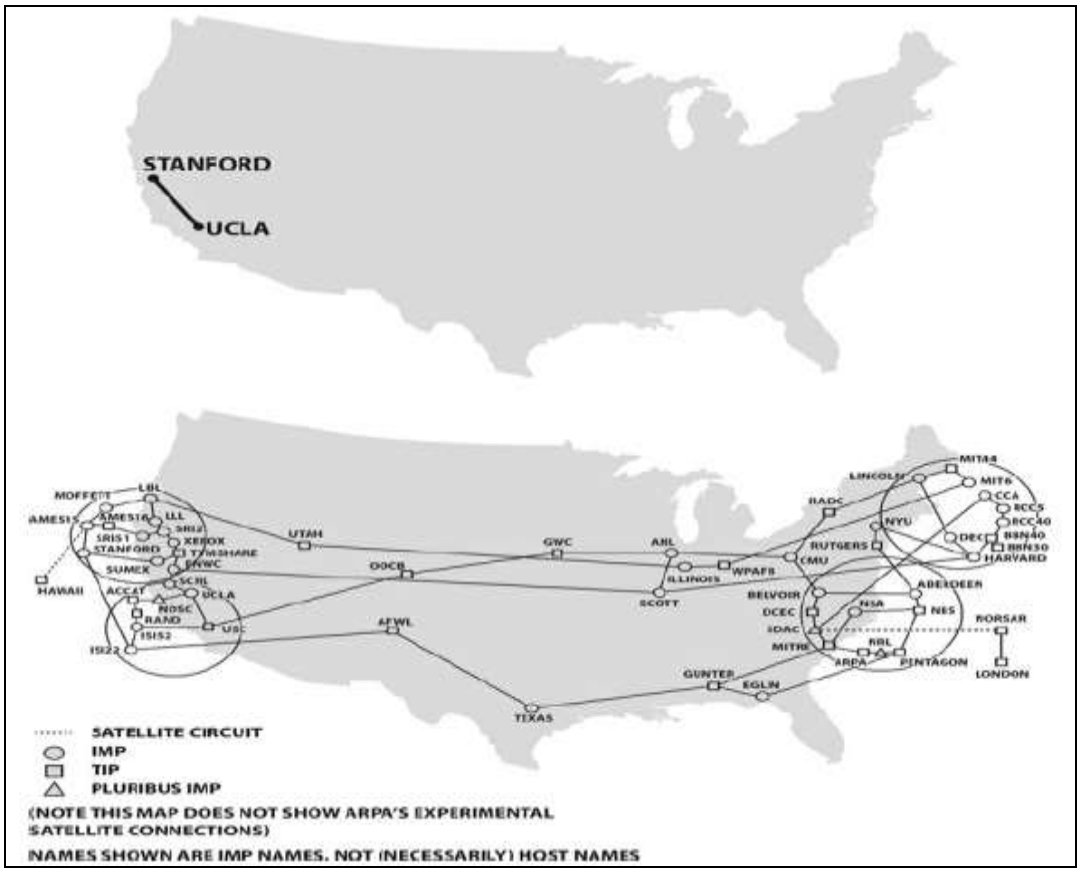
[350] Jon Bing, "Building Cyberspace: A Brief History of Internet", Editörler: Lee A. Bygrave & Jon Bing, *Internet Governance: Infrastructure and Institutions*, 1. Basım, Oxford University Press, New York 2009, s. 8.

[351] Marcus Franda, *Governing The Internet: The Emergence of an International Regime*, 1. Basım, Lynne Rienner Publishers, Colorado 2001, s. 1.

[352] Finn Brunton, *Spam: A shadow History of the Internet*, 1. Basım, The Massachusetts Institute of Technology Press, Massachusetts 2013, s. 2.

kısaltması şeklinde revize edilmiştir. "NET" ise İngilizce'de "ağ" anlamına gelen *network* kelimesinin kısaltmasını temsil etmektedir. 1969 yılında çalışmalarına başlanan ARPANET'in donanım ve yazılım mühendisleri ekipleri, dört farklı lokasyondaki –Stanford Araştırma Enstitüsü (*Stanford Research Institute*), Los Angeles ve Santa Barbara'daki Kaliforniya Üniversitesi yerleşkeleri ve Utah Üniversitesi– bilgisayarları mükemmel bir ağ olarak yapılandırmış ve bugünün İnternet ağının mihenk taşını oluşturmuşlardır.[353]

Tablo-14: ARPANET: Aralık 1969 (ÜST) ve Temmuz 1977 (ALT)



Kaynak: Damien Van Puyvelde & Aaron F. Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace*, 1. Basım, Polity Press, Cambridge 2019, s. 12.

[353] Stephen M. Marson, "A Selective History of Internet Technology and Social Work", *Computers in Human Services*, Cilt 14, Sayı 2, 1997, s. 36.

Tablo 14, ARPANET ağının 1969 yılında 2 düğümden (bağlantı noktası, *node*) 1977 yılında 55'e kadar büyüdüğünü göstermektedir. Bu düğümlerin her biri, yönlendirici olarak kabul edilebilecek bir işlemciyi temsil etmektedir ve araştırma üniversiteleri, enstitüler, ulusal laboratuvarlar, askeri ve istihbarat kurumlarında konumlandırılmışlardır. 1977 yılının haritası ise işlemcileri hem sabit hatlara hem de uydu bağlantılarına bağlayan bir ağın gelişmekte olan karmaşıklığını gözler önüne sermektedir.[354] Öte yandan ARPANET'in İnternete evrilmesinde üç önemli teknik gelişme dikkat çekmektedir: İletim Kontrol Protokolü/İnternet Protokolü (*Transmission Control Protocol/Internet Protocol* [TCP/IP]) geliştirilmiş; Xerox firması tarafından EtherNet'in geliştirilmesine yol açan uzun bir deney serisi tamamlanmış; ve yüksek öğretim kurumları arasında ağ kullanımını en üst düzeye çıkarmak için DARPA tarafından düşük maliyetli bir TCP/IP geliştirilmesine yönelik anlaşmalar yapılmış ve sonrasında da alan adı sistemini (*domain name system, DNS*) getirerek ABD'de üniversiteler için "edu", ticaret için "com", ordu için "mil" terimleri tanıtılmıştır.[355]

Ağ oluşturmanın (*networking*) giderek yaygınlaşmasıyla birlikte artan değeri, araştırmacıları yeni uygulamalar geliştirmeye yönlendirmiştir. İlk İnternet uygulamaları, iletişim araçlarına odaklanmış ve çevrimiçi olarak erişilebilir ve düzenlenebilir sayfalarda veya bültenlerde mesajlar yayınlanmaya ve yorumlanmaya başlamıştır. 1972 yılında bir bilgisayardan diğerine mesaj göndermek, okumak ve oluşturmak için yazılan programla "elektronik posta" (*e-mail*) doğmuş ve bir yıl içerisinde, ARPANET trafiğinin %73'ünü bu yeni uygulama oluşturmuştur.[356] 1980'lerden itibaren kişisel bilgisayarların hızla yayılması, ağlararası iletişime (*internetworking*) artan ilgiyi beslemiş ve araştırma merkezi olarak önceki temel uygulamasından uzaklaşarak giderek artan bir sosyal ağa doğru kaymayı teşvik etmiştir. Dolayısıyla teknolojik bir evrimin yanı sıra ağlararası iletişimin büyümesi, sosyo-kültürel bir olgu olarak da nitelendirilebilmektedir.[357]

---

[354] Damien Van Puyvelde & Aaron F. Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace*, 1. Basım, Polity Press, Cambridge 2019, s. 12.
[355] Brian Winston, *a.g.e.*, s. 331.
[356] David C. Mowery & Timothy Simcoe, "Is the Internet a US Invention? – An Economic and Technological History of Computer Networking", *Research Policy*, Cilt 31, Sayı 8-9, Aralık 2002, s. 1372.
[357] Damien Van Puyvelde & Aaron F. Brantly, *a.g.e.*, s. 15.

ARPANET, en başından beri ortak standartları rutin bir uygulama haline getirmeyi hedeflemiş ve böylelikle güçlü bir temel oluşturmuştur. Öyle ki 1982 yılında TCP/IP çalışma protokollerinin kullanımına geçildiğinde kurucu temeller tamamen yerleşmiş ve halkın daha geniş katılımına açık hale getirilmiştir.[358] Daha sonrasında ise ARPANET'in temel altyapısı, yeni kullanıcıları kapsayacak şekilde genişletilmek zorunda kalmış ve ABD'nin dışına doğru ağ genişlemesi yaşanmıştır. Aynı yıl, ARPANET'in ilk uluslararası bağlantı noktaları (*nodes*), Londra Üniversite Akademisi (*University College London*) ile Norveç Sismik Araştırma Kurumu (*Norwegian Seismic Array,* NORSAR) araştırma laboratuvarında kurulmuştur. Yine aynı dönem içerisinde iki tane önemli Avrupa araştırma merkezi –Avrupa UNIX Ağı (*European UNIX Network,* EUNet) ve Avrupa Akademik ve Araştırma Ağı (*European Academic and Research Network,* EARN)[359]– kurulmuştur. Avrupa'nın bu iki ağı, kendi protokollerini –EUNet, UNIX'ten UNIX'e Kopyalama Protokolü (*The UNIX to UNIX Copy Protocol*, UUCP) ve EARN ise Ağ İşi Girişi (*Network Job Entry*, NJE)– çalıştırmışlar ancak ARPANET ile aynı temel hizmetleri –e-posta, dosya aktarımı vb.– sunmalarına rağmen söz konusu alternatif standartlar TCP/IP protokol paketinin yaygın başarısını elde edememiş ve Avrupa ağları ARPANET'e kıyasla çok daha yavaş büyümüştür.[360]

ABD ordusunun orijinal bilgisayar ağı olan ARPANET'e olan sivil ağ erişiminin 1983 sonrasında giderek artması neticesinde ABD Savunma Bakanlığı tarafından sınıflandırılma getirilmiş ve askeri siteler için yeni bir "Askeri Ağ" (*Military Network*, MILNET) oluşturulmuştur. Böylelikle ARPANET'in sanayi, akademi ve devlet destekli sivil araştırmalar için tercih edilen bir platforma evrilmesi sağlanmıştır. Bu gelişme, kişisel bilgisayarların ve 1970'ler ile 1980'lerin bilgi işlem devriminin diğer yönlerinin gelişimiyle teşvik edilen yerel alan ağlarının (*local area networks*, LANs) ortaya çıkmasıyla yaklaşık olarak aynı zamanda gerçekleşmiş ve yerel bir bölgedeki bilgisayarları ağa bağlamak için basit ve ucuz bir yol sağlayan

---

[358] Congressional Digest Corporation, "Internet History: From ARPANET to Broadband", *Congressional Digest*, Cilt 86, Sayı 2, Şubat 2007, s. 37.
[359] EARN, "The History of the EARN Network", *https://earn-history.net/*, (Erişim Tarihi: 15 Şubat 2020).
[360] David C. Mowery & Timothy Simcoe, *a.g.m.*, s. 1375.

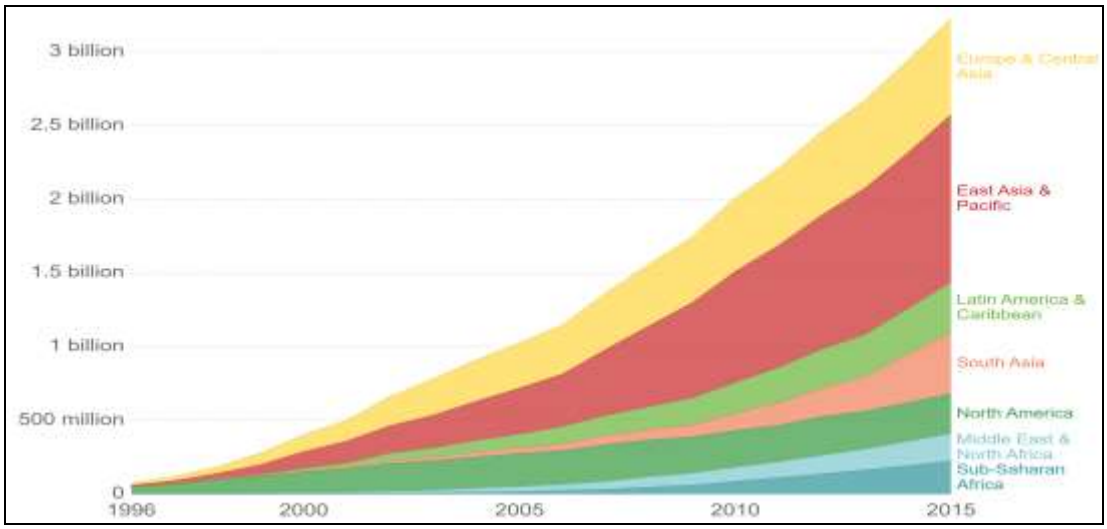
Ethernet sisteminin (*The Ethernet system*) hızla büyümesini mümkün kılmıştır.[361] 1985 yılında ABD Ulusal Bilim Vakfı (*The US National Science Foundation*, NSF), ülke çapında finanse ettiği süper bilgi işlem merkezlerini birbirine bağlamak ve ağ oluşturma (*networking*) üzerine ileri araştırma ve eğitim teşviki için kendi ağı olan "Ulusal Bilim Vakfı Ağı"nı (*National Science Foundation Network*, NSFNET) kurmuştur. İnternet bağlantısı için fon alan her kurumun NFSNET kullanması ve kullanıcılara erişim sağlamasının gerekliliği sayesinde birkaç yıl içerisinde NFSNET, ağlararası iletişim (*internetworking*) için ana merkez haline gelmiş ve 1990 yılında ARPANET'in hizmet dışı bırakılması söz konusu olmuştur. Bu bilimsel ağ için geliştirilen veri yolları ise nihayetinde İnternetin omurgasını oluşturmuştur.[362] İnternetin evrim sürecindeki en önemli gelişmelerden bir diğeri ise 1991 yılında, İsviçre'deki Avrupa Nükleer Araştırma Merkezi'nde (*Conseil Européen pour la Recherche Nucléaire,* CERN) çalışan iki fizikçi olan Tim Berners-Lee ve Robert Cailliau tarafından yazarların belgelerinin metinlerine resim ve grafik eklemesine izin veren multimedya yeteneklerini içeren ve okuyucuları diğer belgelere yönlendiren "bağlantılar" şeklinde belirtmelerine olanak tanıyan Hiper-Metin İşaretleme Dili (*Hypertext Markup Language*, HTML) ile beraberinde bir belge alma protokolü olan Hiper-Metin Transfer Protokolünün (*Hypertext Transfer Protocol*, HTTP) yayınlanması olmuştur. HTML ile HTTP, İnternetin geniş bir çapraz referanslı multimedya belge koleksiyonuna dönüşmesine vesile olmuş ve böylelikle hiper-metin belgelerinin İnternet üzerinden birbiriyle bağlantı kurabildiği, "Web" olarak da bilinen "Dünya Çapında Ağ" (*World Wide Web,* WWW) bilgi sistemi ortaya çıkmıştır.[363]

Öncesinde ARPANET, sonrasında da NSFNET'e artan ticari ilgi, ağlararası iletişimin (*internetworking*) doğasını değiştirerek araştırma merkezini popüler bir iletişim platformuna dönüştürmüştür. 1994 yılında, ABD Hükümeti tarafından NSFNET'in bölgesel ana bağlantılarının resmi kontrolünün özel sektöre çevrilmesine karar verilmiş ve sonrasında "Ticari İnternet Servis Sağlayıcıları" (*Commercial Internet Service Providers*, ISPs), telefon hatlarını kullanarak çevrimiçi bağlantı

[361] Marcus Franda, *a.g.e.*, s. 30.
[362] Damien Van Puyvelde & Aaron F. Brantly, *a.g.e.*, ss. 16-17.
[363] David C. Mowery & Timothy Simcoe, *a.g.m.*, ss. 1377-1378.

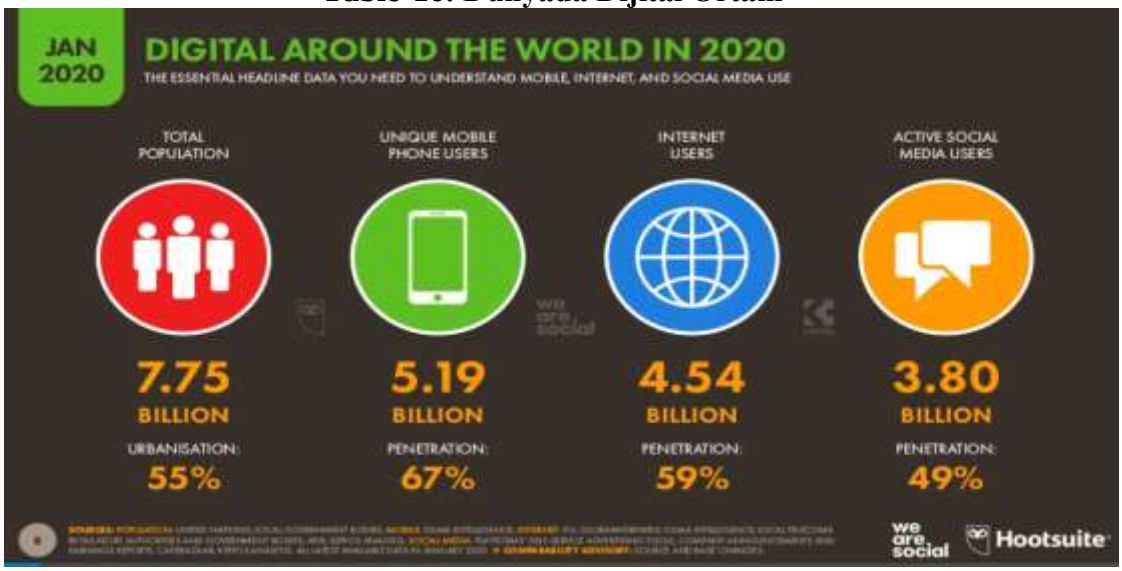
kurabilen bireysel kullanıcılara hizmetlerini sunmaya başlamışlardır. İnternetin yaygınlığı arttıkça da ticari donanım –bilgisayarlar, modemler vb.– ve yazılım –İnternet tarayıcıları (*browsers*) vb.– sağlayıcıları giderek çoğalmıştır.[364]

Tablo-15: Dünya Bölgelerine Göre İnternet Kullanıcı Miktarları (1990-2015)



Kaynak: Our World in Data, "Internet Users by World Region", *https://ourworldindata.org/*, (Erişim Tarihi: 16 Şubat 2020).

Tablo-16: Dünyada Dijital Ortam



Kaynak: We Are Social Inc., "Digital 2020: Global Digital Overview", *https://wearesocial.com/digital-2020,* (Erişim Tarihi: 17 Şubat 2020).

[364] Damien Van Puyvelde & Aaron F. Brantly, *a.g.e.*, s. 17.

1995 yılı, İnternetin ticari bir ortam olarak ortaya çıktığı yıl olarak adlandırılmakla beraber İnternet üzerinden sunulan hizmet çeşitliliğinin hızla arttığı ve bilgisayar kullanıcılarının ağa erişimini kolaylaştıran yeni uygulamalar sayesinde çevrimiçi alışverişin doğduğu süreçtir.[365] Hizmet çeşitliliğinin faydasıyla birlikte daha fazla gelişmeyi açıklayan "*www*" üzerinden kullanılabilirliğin birleşimi, Tablo-15'de de görüldüğü üzere İnternet kullanıcı miktarının dünyanın tüm bölgelerinde çok büyük seviyelere ulaşmasını sağlamıştır. Öte taraftan "*We Are Social*" platformunun 2020 yılına dair en güncel dijital dünya veri raporuna (Tablo-16) göre Ocak 2020 itibariyle yaklaşık 7.7 milyarlık dünya nüfusunun %59'u (yaklaşık 4.5 milyar) İnternet kullanıcısı olup Ocak 2019'a kıyasla İnternet kullanıcı sayısında yaklaşık %7'lik (yaklaşık 298 milyon) artış yaşanmıştır. Mobil kullanıcı sayısına bakıldığında ise 2020 yılında dünya nüfusunun yaklaşık %67'sine (yaklaşık 5.1 milyar) karşılık geldiği ve 2019 yılına kıyasla %2.4'lük (yaklaşık 124 milyon) artış yaşandığı görülmektedir.[366] Tüm bu veriler göstermektedir ki; dünya her geçen gün İnternete eklemlenmekte ve sosyo-kültürel bir olgu olarak İnternetin belirleyiciliği ve etki sahası giderek derinleşmektedir.

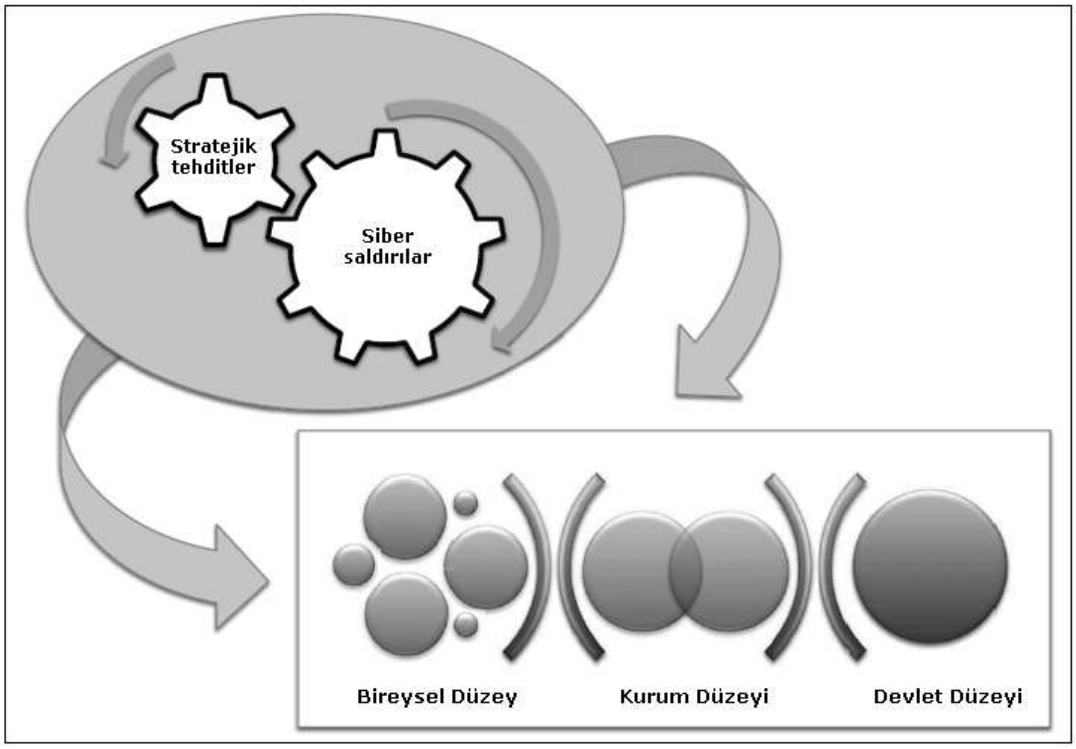
2.2. Siber Tehdit ve Siber Saldırı

Tehditler sadece insan ilişkilerini değil, her türlü alana dair her türlü sistem ya da organizasyon içerisindeki aktörlerin ilişkilerini doğrudan ya da dolaylı olarak etkilemektedirler. Uluslararası İlişkiler açısından bakıldığında ise çeşitli ifadeler içerisinde kullanılan "tehdit" (*threat*) kavramı; aktörlerin hamlelerinin, davranışlarının ve karşı davranışlarının, pozitif ve negatif yaptırım etkilerinin göz önünde bulundurularak tehdit-vaat ayrımının yapılmasına ve zorlama derecesine göre değişerek söz konusu derecelerin tarafların birbirlerinin yetenekleri ve niyetleri hakkındaki algıları üzerinden belirlendiği genel kabulüne dayandırılmaktadır.[367] Siber uzay sahasındaki ilişkilerde kullanılan "siber tehdit" (*cyber threat*) kavramı ise yine aynı sahada sıklıkla ifade edilen "siber nefret" (*cyber hate*) kavramı gibi

[365] Jon Bing, *a.g.m.*, s. 38.
[366] We Are Social Inc., "Digital 2020: Global Digital Overview", *https://wearesocial.com/digital-2020*, (Erişim Tarihi: 17 Şubat 2020).
[367] David A. Baldwin, "Thinking About Threats", *The Journal of Conflict Resolution*, Cilt 15, Sayı 1, Mart 1971, ss. 72-73.

kolayca tanımlanamamakla birlikte çoğunlukla bilgisayar kullanıcılarının psikolojik yaralanmalarına ve suçlarına yönelik tercih edilmektedir. Siber tehditler; suç çeteleri, teröristler, bilgisayar korsanları, hasmane devletler ve diğer kötü niyetli aktörler tarafından ağlararası iletişimin kritik altyapılarına ve İnternet sistemlerine saldırmayı hedefleyen eylem algıları olarak tanımlanmaktadır. "Ağ Sistemleri Çağı" olarak da betimlenen 21. yüzyıl, kamu ve özel sektörler dahil olmak üzere güvenlik sistemleri ve altyapılar açısından güvenlik açığı duygusunu öne çıkarmış ve siber uzay sahası aktörleri tarafından saldırı unsurlarının doğasının ve karakterinin değişerek siber tehditlerin daha sofistike hale gelmesine vesile olmuştur.[368]

Tablo-17: Aktörlere ve Kritik Altyapılara Yönelik Siber Tehditler



Kaynak: Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security In Cyberspace*, EPFL Press, Lausanne 2013, s. 137.

[368] Imran Awan, "Cyber Threats and Cyber Terrorism: The Internet as a Tool for Extremism", Editörler: Brian Blakemore & Imran Awan, *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*, Routledge, New York 2016, ss. 21-22

Kritik altyapıların tehdit edilmesi, ideolojilerin yayılması ya da enformasyon manipülasyonu gibi çeşitli yollarla ekonomik, siyasal ve sosyal istikrarsızlıkların siber uzay sahası üzerinden yaratılabilme olasılığının giderek daha kolay hale gelmesi gibi bir dizi stratejik siber tehdit halinin başta devletler olmak üzere uluslararası sistem içerisindeki tüm aktörler tarafından gerçek anlamda ciddiye alınması elzemdir. Tablo-17 üzerinden yorumlandığında kötü niyetli muhalif unsurlar, düşmanca eylemleri gerçekleştirebilmek adına bilgi ve iletişim teknolojilerini en sert şekilde kullanabilmekte ve çevrimiçi sayfalar üzerinden fotoğraflar, röportajlar, eğitim videoları vb. paylaşımlar yaparak yeni taraftarlar edinebilmektedirler. Bunların yanı sıra yeni finansman kaynakları bulunarak siber uzay sahası dışında da büyük zararlar verebilmek için bilgi toplama ve zarar yaratma durumları söz konusu olabilmektedir.[369]

Enformasyon ya da bilgi, bir çeşit fenomen soyutlaması olarak ele alınmalı ve dolayısıyla teknolojiden farklı düşünülmelidir; ancak bu durumun aksine eldeki enformasyon ile neler yapılabileceği ve özellikle ne kadar hızlı yapılabileceği ise doğrudan teknolojiye bağlıdır. Dolayısıyla siber tehditler, küresel bilgi altyapısının kötü amaçlı kullanılabilme açığının ve yüksek olasılığının sonuçları olarak yorumlanmakta ve mevcut ile gelecekteki teknolojik çevrenin karakteristiğinin tehditlerin algısı üzerindeki güçlü etkisine dayanmaktadır. Mevcut ve gelecek zaman dilimine ek olarak siber tehditlerin tarihsel boyutu da söz konusudur; çünkü teknolojik altyapılar, gerçekleştirilen yeni gelişmelerle birlikte sürekli değişim içerisindedir ve yaşanan değişimlerle birlikte özelliklerinin de değişmesine bağlı olarak tehdit algıları da sürekli değişmektedir.[370] Bu hızlı ve devamlılık gösteren değişim süreçleri içerisinde siber tehditlerin nüfuz ettiği çok sayıda alan söz konusu olmasına rağmen ön plana dört tanesi çıkmaktadır: Devlet destekli siber saldırı tehditleri; ideolojik ve politik aşırılık tehditleri; ciddi organize suç tehditleri; ve alt düzey/bireysel suç tehditleri.[371] Siber uzaya dair tehditler, yukarıda belirtilen kategorilerden daha fazlasına sığdırılabilmesine rağmen belirtilen bu dört alan, siber

[369] Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security In Cyberspace*, EPFL Press, Lausanne 2013, s. 137.
[370] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, 1. Basım, Routledge, New York 2008, s. 19.
[371] Paul Cornish, David Livingstone, Dave Clemente & Claire Yorke, *On Cyber Warfare: A Chatham House Report*, The Royal Institute of International Affairs, Londra Kasım 2010, s. 5.

uzay sahası asimetrilerilerinin sadece devletlerle sınırlı kalmayıp çok sayıda aktörü bünyesinde barındırdığı ve psikolojik durumun öne çıktığı kimi durumlarda aktörlerin saldırgan amaçlarını gerçekleştirebilmek için sanal araçları karşılıklı kullanabileceklerinin anlaşılabilmesi adına yararlı bir çerçeve sağlamakta ve "saldırı" vurgusunu öne çıkarmaktadır. [372]

Bu bağlamda "siber saldırı" (*cyber attack*) terimi, siber uzay sahasında meydana gelen çeşitli zararlı faaliyetleri –bilgisayarlardaki ve ağlardaki bilgilerin imha edilmesi, bozulması, tahrip edilmesi, bilgisayarların tehlikeye atılması vb.– tanımlamak için kullanılmaktadır. Bu tür saldırılar sadece bilgisayarlar ve ağlar ile sınırlı kalmamakta, aynı zamanda bunlarla bağlantılı olan sistemlere, tesislere, materyallere ya da insanlara doğrudan ve dolaylı etkiler yaratabilmektedirler. Bunun en klasik örneği olarak; hava trafik kontrol sistemine yapılabilecek bir siber saldırının, amacı doğrultusunda doğrudan etkiler yaratarak hava trafiğini etkileyebileceği, aynı zamanda da dış etkiler bağlamında maddi yıkıma ve insan kaybına neden olabilecek kazalar yaratabileceği gösterilmektedir.[373] Kayıtlara geçen ilk devlet destekli ve ulusal altyapılara yönelik siber saldırı, 1982 yılında ABD Başkanı Ronald Reagan'ın onayıyla Sibirya'daki Rus boru hattına yönelik bir SCADA[374] saldırısı şeklinde gerçekleşmiştir. Soğuk Savaş dönemi gerilimleri bağlamında SSCB'nin gaz arzına ve Rus ekonomisine Batıdan gelen gaz gelirlerine zarar vermek ve gücünü zayıflatmak üzerine tasarlanan bu boru hattı saldırısı, pompaları, türbinleri ve vanaları çalıştıran boru hattı yazılımına zarar vererek pompa hızları, valf ayarları ve basınç değeri dengelerini bozmuştur.[375] Günümüzde İnternet ortamının ulaşmış olduğu genişleme ve derinleşme dikkate alındığında, bu alanın siber saldırılar karşısındaki savunmasızlığı daha da belirginleşmektedir. İnternette

---

[372] Aynı yerde.

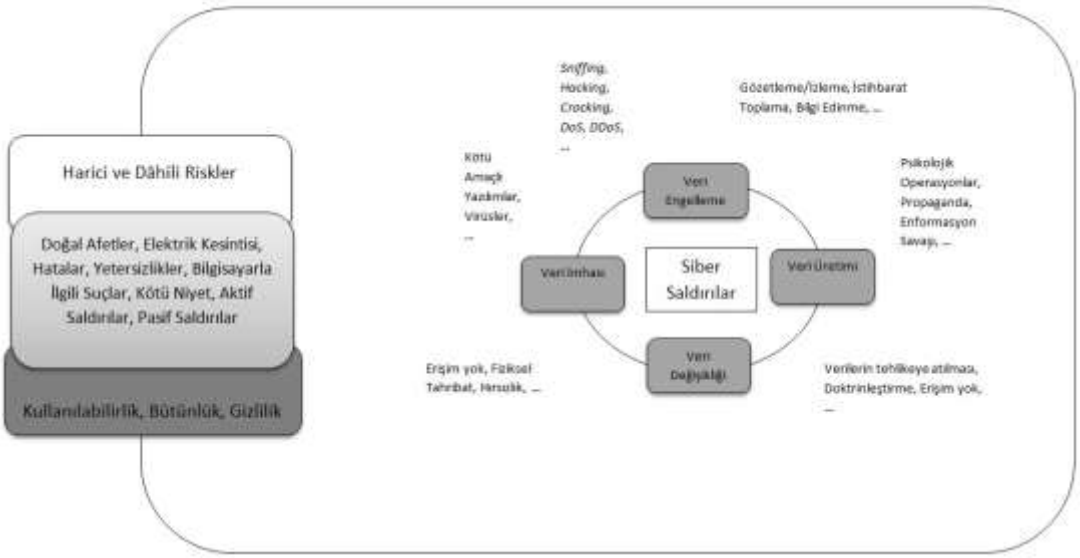
[373] Nicholas Tsagourias, "Cyber Attacks, Self-defence and The Problem of Attribution", *Journal of Conflict & Security Law*, Cilt 17, Sayı 2, 2012, s. 229.

[374] Gözetleyici Kontrol ve Veri Toplama (*Supervisory Control and Data Acquisition*, SCADA) sistemleri, çok çeşitli bilgisayar ve iletişim teknolojilerini kullanan dağıtım yönetim sisteminin (*distribution management system*, DMS) ve enerji yönetim sisteminin (*energy management system*, EMS) önemli parçalarından kabul edilmektedir. Özellikle enerji endüstrisindeki düzensiz ve geniş ortamlardaki bilginin kontrol ve yönetimini merkezileştiren bu sistem sayesinde operasyon, karlılık, müşteriyi elde tutma, pazar avantajı ve büyümeyi güvence altına alma gibi konularda büyük kolaylıklar sağlanmaktadır. Detaylı bilgi için bkz.: Bin Qiu, Hoay Beng Gooi, Yilu Liu & Eng Kiat Chan, "Internet-Based SCADA Display System", *IEEE Computer Applications in Power*, Cilt 15, Sayı 1, ss. 14-19.

[375] Paul Cornish, David Livingstone, Dave Clemente & Claire Yorke, *a.g.e.*, ss. 6-7.

kullanılan iletişim protokollerinin çoğu, siber saldırı amaçlarına hizmet etmek için kötüye kullanılabilmektedir. Bu nedenle İnternet üzerinden bağlanan herhangi bir sistem, potansiyel olarak doğrudan siber saldırıların hedefi olabilmektedir.

Tablo-18: Güvenlik İhlalleri ve Etkileri



Kaynak: Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security In Cyberspace*, EPFL Press, Lausanne 2013, s. 45.

Teknolojinin kötü amaçlarla kullanılması ve yeterli güvenlik önlemlerinin bulunmaması nedeniyle yaşanabilecek çeşitli sorunların bazıları Tablo-18'de tanımlanmıştır. Bilgisayar teknolojilerinde yaşanan son derece hızlı ve önemli gelişmelere rağmen temel İnternet teknolojileri –TCP/IP iletişim protokolleri, IP adresi vs.– halen ilk günkü gibi kullanılmaktadır ve başlangıç altyapılarında total değişimler yapılmadan, güncellemeler üzerinden yeni hizmetler ve uygulamalar ortaya çıkmaya devam etmektedir. Başlangıçtaki İnternet teknolojilerine entegre edilmeyen güvenlik ve veri koruma çözümleri, İnternetin şimdiki kullanımının orijinal konseptinden sapmış olmasının bir sonucu olarak nitelendirilmektedir. Dahası, her yeni teknolojik gelişmenin hatalar ve açıklar barındırma olasılığı giderek daha fazla olmakla birlikte teknolojik ortamın karmaşıklığının muazzam genişliği, güvenlik açıklarını kaçınılmaz olarak ortaya çıkarmaya devam edecektir.[376]

[376] Solange Ghernaouti, *a.g.e.*, ss. 44-45.

Netice olarak siber tehditlerin sadece sanal saldırılar şeklinde sınırlandırılması yanlış yönlendirici olabilmektedir. Bilgi ve teknoloji altyapılarına yönelik saldırı araçları hem fiziksel hem de siber tabanlı olabilir. Aynı durum hedefler için de söz konusudur ve enformasyon altyapılarının –ulusal ya da küresel– karmaşık yapısından dolayı tam olarak ne olduğunun anlaşılabilmesi kolay değildir. Bunun altında yatan temel neden; teknolojilerin sadece kolay kavranabilen fiziksel bileşenlere –yüksek hızlı, etkileşimli, dar bant ve geniş bant ağları, uydu, karasal ve kablosuz iletişim sistemleri, bilgisayarlar, televizyonlar, telefonlar, radyolar vb.– sahip olmamakla birlikte altyapılardan geçen bilgilere, içeriklere ve bunlardan oluşturulan ve servis edilen hizmetlere de sahip olmasıdır.[377]

Tablo-19: Altyapı Tehdit Matrisi

ARAÇ	**HEDEF**	
	Fiziksel	**Siber**
Fiziksel	**Kazıcı yükleyici (beko loder) bir iş makinesi ile bir telekomünikasyon kablosunun koparılması.**	**Elektronik bileşenlerin istikrarını bozmak için elektromanyetik titreşim ve radyo frekanslı silahların kullanılması.**
Siber	**Belediye kanalizasyonunu kontrol eden bir SCADA sistemine girilmesi. / Bir uçağı düşürmek için hava kontrol sistemine yanıltma (*spoofing*) saldırı yapılması.**	**Kritik bir hükümet ağına saldırı yapılması. / Genel aktarmalı telefon ağına (*public switched telephone network*, PSTN) truva atı yerleştirilmesi.**

Kaynak: Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, 1. Basım, Routledge, New York 2008, s. 23.

[377] Myriam Dunn, "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)", *Internationl Journal of Critical Infrastructures*, Cilt 1, Sayı 2-3, 2005, s. 263.

Son olarak Myriam Dunn tarafından "altyapı tehdit matrisi" (*infrastructure threat matrix*) olarak adlandırılan ve bilgi altyapılarının hedef ya da araç olarak kötü amaçlı kullanımını içeren dört tür saldırıya bakmakta fayda görülmektedir: Tablo-19'da sunulan bu matrise göre siber tehdit tartışmalarında yer alan bilgisayar korsanları (*hackers*), bilgi altyapılarına saldırabilecek bilgi, beceri ve araçlara sahip olup yukarıdaki matriste son iki kategoriye girmektedirler. Ayrıca bilgi ve teknoloji altyapılarının fiziksel ve sanal bileşenleri arasında kesin ayrım yapabilmenin her geçen gün giderek zorlaştığı siber tehdit tartışmalarında, bilgisayar korsanlığı sadece teknolojik olarak yetenekli kişiler tarafından değil, aynı zamanda teröristler ya da devletler veyahut da teknolojik olarak yetenekli ve kötü niyetli aktörler tarafından gerçekten kötü amaçlar için kullanılabilen bir *modus operandi* olarak kabul edilmektedir.[378] Bu bağlamda kötü niyetli grup ya da oluşumlar tarafından finanse edilebilecek teknolojik altyapı bilgisine sahip bireylerin, ulusal ya da küresel boyutlarda sosyal, ekonomik ve siyasi hasarlar verebilme olasılığı, tehdit algılarını ve saldırı eylemlerini sürekli olarak etkilemektedir.

2.3. Siber Casusluk ve Siber Suç

"Siber Casusluk" (*Cyber Espionage*), siber uzay sahasındaki ağlara yönelik düşmanca eylemlerden bir diğeri olarak kabul edilmektedir. "Siber Sömürü" (C*yber-Explotation*) olarak da kullanımı tercih edilen siber casusluk kavramı, siber sahada çeşitli stratejiler, taktikler ve araçlar kullanılarak istihbarat toplanması kabiliyetidir. Daha spesifik olarak siber casusluk; "avantaj elde etmek ya da maddi getiri sağlamak için rakip aktörler hakkında hassas bilgilere erişmek amacıyla bilgisayar operasyonlarının ve dijital iletişim faaliyetlerinin kasıtlı olarak kullanılması" şeklinde tanımlanmaktadır.[379] Siber saldırılarda karşı tarafın bilgisayar sistemleri ve ağlarının kullanılamaz ya da güvenilemez hale getirilerek daha az yararlı hale getirilmesi gibi yıkıcı amaçlar söz konusuyken, siber casuslukta daha tahribatsız bir durum söz konusudur. Buna göre siber casusluk eylemleri, elde edilmek istenen gizli

[378] Myriam Dunn Cavelty, *a.g.e.*, ss. 22-23.
[379] Certified Management Consultant and Strategic Advisor with the Technolytics Institute, "Cyber Espionage Targets Sensitive Data", SIP Trunking Report, 29 Aralık 2008, *http://sip-trunking.tmcnet.com/topics/security/articles/47927-cyber-espionage-targets-sensitive-data.htm*, (Erişim Tarihi: 20 Şubat 2020).

bilgilere ulaşılmasına izin veren mümkün mertebe en küçük müdahaleler ile gerçekleştirilmektedir. Örneğin; bir bilgisayar virüsü, ağına bulaştığı bilgisayarın çalışma sürecine hiçbir zarar vermeksizin sabit diskinde arama yaparak kredi kartı bilgileri içeren tüm belgeleri tarayabilir ve e-posta kutusundaki tüm bilgileri toplayabilir.[380] Yani ağın normal işleyişini kullanıcının bakış açısından rahatsız etmeyecek şekilde, fark edilmeden verilere ulaşabilme hedefi söz konusudur. 21. yüzyıl, kötü amaçlı yazılımların büyümesiyle birlikte inovasyon hızını gör ardı etmenin giderek zorlaştığı bir süreç haline gelmiştir. Çoğu durumda da casusluğun politik veya ekonomik amaçlarla belirli bir devlete, hükümete ya da kuruma atfedilmesi neredeyse imkânsız olabilmektedir. Örneğin; çeşitli kaynaklarda Çin'de bilgisayar korsanlarının giderek daha aktif ve etkili hale geldiği belirtilse de bunlar üzerinde devlet desteğinin olup olmadığına dair kesin bilgiler resmi kaynaklarla sınırlı kalmakta ve destek kapsamına dair spekülasyonlardan öteye geçememektedir. Öyle ki, her geçen gün ortaya çıkan kötü amaçlı yeni yazılım şekilleri, siber zararın çoğalmasını ve yayılmasını neredeyse anlık seviyelere indirmiştir.[381]

Öte yandan siber casusluk, diğer siber aktivite biçimleriyle –siber terörizm ve siber savaş gibi çok şiddetli ve yıkıcı eylemlerin yanı sıra siber vandalizm ya da siber saldırı gibi daha küçük ölçekli ve düşük şiddetli eylemler– karıştırılabilmektedir. Bu eylemlerin teknik yönleri, siber casusluğun sadece casusluk olup olmadığını ya da ağları savunmakla görevli olan aktörler ve devlet düzenleyicileri açısından tehdit algılarının ve ölçeklerinin belirlenebilmesini karmaşıklaştırmaktadır.[382] Ek olarak ise siber casusluk kavramının klasik casusluk kavramıyla hem benzerlikler hem de farklılıklar taşıdığı görülmektedir. Buna göre klasik casusluk; "casuslar, ajanlar ya da yasa dışı izleme cihazları aracılığıyla askeri, siyasi, ticari veya diğer gizli bilgilerin edinme süreci" olarak tanımlanmaktadır.[383] Bu noktada siber casusluk, gizli ulusal bilgilerin edinme yolu olarak yukarıdaki klasik tanım kapsamına girerken, ülkelerin istihbarat bilgileri toplamak adına ataşeler ve casuslar gönderdiği geleneksel casusluk

[380] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force", *Journal of National Security Law & Policy*, Cilt 4, Sayı 63, 2010, s. 63.
[381] Nazli Choucri, *a.g.e.*, ss. 142-143.
[382] Luke Pelican, "Peacetime Cyber-Espionage: A Dangerous But Necessary Game", *CommLaw Conspectus*, Cilt 20, Sayı 2, 2012, s. 365.
[383] Encyclopædia Britannica, "Espionage: International Relations", *https://www.britannica.com/topic/espionage*, (Erişim Tarihi: 21 Şubat 2020).

anlayışına uymamaktadır; çünkü siber casusluk, geleneksel casusluk anlayışından çok daha müdahaleci olup devlet dışı aktörler tarafından hedeflenen ülkelerin ya da aktörlerin altyapılarını zayıflatabilecek veya başka bir devlete saldırı başlatabilecek şekilde gerçekleştirilebileceğinden geleneksel casusluktan daha yüksek bir tehdit ve endişe unsuru taşımaktadır.[384] Dolayısıyla siber casusluk, özellikle Uluslararası İlişkilerde siber savaştan çok daha yaygın olan önemli bir sorun olarak addedilmektedir. Modern bilgi sistemlerinin dağılmış ve büyük ölçüde birbirine bağlı doğası, gizlilik vasfındaki bilgilerin korunmasını zorlaştırmakta ve ağlara bağlı makinelerde her zamankinden daha fazla depolanan verilerin, yine her zamankinden daha kolay ve hızlı aktarılmasını, depolanmasını, gizlenmesini ve manipüle edilmesini mümkün kılmaktadır. Bunun en klişe örneklerinden biri olarak ise on yıl önceki süper bilgisayarlardan daha fazla bilginin serçe parmak boyutundaki USB belleklerde kolaylıkla taşınıp saklanabilmesi gösterilebilmektedir.[385]

Casusluğun uluslararası düzeyde kanunen yasaklanmadığının hatırlatılmasında fayda bulunmaktadır. Uluslararası hukuk kapsamında casusluğa her zaman izin verilmiş olmasına rağmen, yerel düzeydeki ulusal yasalar çerçevesinde neredeyse evrensel olarak yasadışı ilan edilmiştir ve çok sert şekilde cezalandırılmaktadır.[386] Bununla birlikte hedef sistemlerdeki yerleşik verilerin izinsiz giriş eylemi ile değiştirilmiş olması, siber casusluğu yasaklanmış bir bölgesel egemenliğin ihlali olarak nitelendirmek için yeterli görülmemektedir; ancak zararın önemsiz olduğu ve bir devletin bir başka devletin siber altyapısına karışmış olduğu gerçeğinin, her zaman bölgesel egemenlik ilkesinin ihlali anlamına gelen yabancı topraklar üzerinde bir yargılama yetkisi olarak değerlendirilmesi gerektiği söylenmektedir.[387] ABD yönergeleri, ordunun bilgisayar kodlarını başka bir devletin ağına iletmesine pasif olması şartıyla izin vermektedir; yani daha sonraki bir tarihte zarar vermek için etkinleştirilebilecek virüs ya da solucan içermemelidir. Öyle ki,

---

[384] Anna Wortham, "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?", *Federal Communications Law Journal*, Cilt 64, Sayı 3, 2012, s. 658.
[385] Gary McGraw, "Cyber War is Inevitable (Unless We Build Security In)", *Journal of Strategic Studies*, Cilt 36, Sayı 1, 2013, s. 111.
[386] Richard W. Aldrich, "How Do You Know You Are At War In The Information Age?", *Houston Journal of International Law*, Cilt 22, Sayı 2, 1999, s. 250.
[387] Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies*, Cilt 89, Sayı 1, 2013, s. 129.

yazılımlar çoğunlukla çift kullanım –hem bilgileri çalmak hem de yıkıcı saldırılar gerçekleştirmek– özelliğine sahiptirler. Başlangıç aşamasında bilgi toplamak için kullanılan yazılım kodları yeniden programlanabilir ve sonrasında da son derece yıkıcı ajanlara dönüştürülebilmektedirler.[388] Bu bağlamda en fazla öne çıkan örneklerden biri olan "W32.Duqu" isimli kötü amaçlı yazılım (*malware*), Ekim 2011'de keşfedilmiş ve özellikle kritik altyapı varlıklarının operatörleriyle karşı karşıya kalan siber güvenlik tehditlerine medyada dikkat çekmiştir. Bu yazılım, silahlandırılmış bilgisayar kodu olmamakla birlikte endüstriyel kontrol sistemleri ve kritik altyapı varlıkları hakkında istihbarat bilgileri toplamak üzere tasarlanmıştır. Çoğunlukla Avrupa ve Orta Doğu olmak üzere coğrafi olarak çok dağınık yayılan ve çok az sayıda tespit edilen bu yazılımın bulaşma ömrünün 30 gün olduğu ve sonrasında kendisini bulaştığı makineden sildiği tespit edilmiş ancak hedefleri tespit edilememiştir. Gelecekteki olası saldırılara hazırlanmak adına bilgi topladığına inanılan bu yazılım, siber casusluğun birçok insanın düşündüğünden çok daha zorlu bir siber güvenlik sorunu olduğunu gözler önüne sermiştir.[389]

Uluslararası İlişkilerde siber casusluğun giderek yükselişi, hükümetlere karşı casusluk ve şirketlere karşı ekonomik casusluğun yaygınlığı ile birleşerek etkili strateji ve kurallardan yoksun bir bağlamda yeni zorluklar yaratmaktadır. Bundan dolayı bir taraftan devletler kendi ulusal ceza hukuklarında casusluğa karşı sert cezalar getirerek yasaklarken, diğer taraftan da diğer devletlere dair casusluk faaliyetlerini derinleştirmektedirler. Söz konusu bu gerçek, ulusal yasakların casusluğu caydırmadığını ve ülkelerin geleneksel ve ticari casuslukları düzenleyen uluslararası yasal kuralları geliştirmediği ya da geliştirilmesini teşvik etmediği anlamına gelmektedir. Ayrıca siber casusluk faaliyetleri, Uluslararası İlişkilerdeki güç anlayışı ve güç kullanımıyla ilgili politik, askeri ve istihbarat hesaplamalarına siber kabiliyetlerin derinlemesine yerleşmesine yardımcı olmaktadır.[390]

Öte yandan siber uzay sahası, casusluk ile suç arasındaki ilişkiyi de dönüştürmektedir. "Siber Suç" (*Cyber-Crime*), en az bir bilgisayar ve ağ içermekte

---

[388] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, 1. Basım, Oxford University Press, Oxford 2014, s. 66.
[389] Gaute Wangen, "The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism", *Information*, Cilt 6, Sayı 2, 2015, ss. 190-191.
[390] David P. Fidler, "Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous Than You Think", *International Journal of Critical Infrastructure Protection*, Cilt 1, Sayı 5, 2012, s. 29.

olup yasadışı faaliyetlerden oluşmaktadır. Bilgisayarlar kullanılarak geleneksel suçlar işlenebilmektedir ancak Siber Suçlar; kimlik avı, e-dolandırıcılık ve virüsler gibi daha spesifik suç türlerinden meydana gelmektedir. Bilgisayarlar bir suçun işlenmesinde kullanılabilmekte ya da hedef pozisyonunda yer alabilmektedirler. Dolayısıyla en geniş anlamda siber suçlar; "İnternet gibi modern telekomünikasyon ağları –sohbet odaları, elektronik postalar, duyuru panoları, gruplar vb. ile sınırlı olmayan tüm ağlar– ile cep ve akıllı telefonların (Bluetooth, SMS, MMS vb.) bilinçli bir şekilde doğrudan ya da dolaylı olarak bireylere ve gruplara yönelik tüm fiziksel zararları, mental zararları, kayıpları, hasarları" şeklinde tanımlanabilmektedir.[391] Buna karşın, 1990 öncesi dönemdeki teknoloji suçlarını ifade etmek için "siber suç" yerine "bilgisayar suçları" (*computer crimes*) terimi kullanılmıştır; çünkü bu dönemde İnternet ağı bulunmamakta ve ana bilgisayarlar ile diğer bilgisayarlar arasında küresel çaplı bağlantı kurulamamaktadır. Dolayısıyla ana bilgisayarlara erişim izni, seçilmiş kişi ya da gruplarla sınırlı kalmaktadır. Bu dönemin en fazla öne çıkan bilgisayar suçları türü ise ana bilgisayarlara erişim izni olan kişilerin kendilerine maddi fayda sağlamak amacıyla işledikleri mali suçlar şeklinde gerçekleşmiştir.[392] 1990 sonrasında ise İnternet ağının gelişmesiyle birlikte siber suç terimi, teknoloji kullanımı ile işlenen geleneksel suçların yanı sıra İnternet teknolojisi sonucu ortaya çıkan yeni suçları –bilgisayar manipülasyonu ile dolandırıcılık, çevrimiçi sahtekârlık, bilgisayar verilerinin veya programlarının zarar görmesi ya da değişiklik yapılması, ağ sistemlerine yetkisiz erişim, yasal olarak korunan bilgisayar programlarının izinsiz çoğaltılması vs.– tanımlamak için kullanılır hale gelmiştir.[393]

Siber suçlar, üç geniş eylem kategorisine ayrılmaktadır: Bunlardan birinci kategori, "bilgisayarla ilgili siber suçlar" (*computer-related cybercrimes*) olarak adlandırılmaktadır. Bilgisayarların suç için sadece araç olduğu, geleneksel suç faaliyetlerini yürütmek için verilerin manipüle edildiği sahtecilik ve hırsızlık gibi suçlar bu kapsamdadır. İkinci kategori olan "içerik tabanlı siber suçlar" (*content-based cybercrimes*) ise bilgisayar ve iletişim teknolojilerinin yasadışı veri dağıtımını

[391] Bella Anderson, *Cybercrime: Criminal Threats from Cyberspace*, White Press Academic, Los Angeles 2018, s. 1.
[392] Majid Yar & Kevin F. Steinmetz, *Cyber Crime and Society*, 3. Basım, Sage Publications, Londra 2019, s. 9.
[393] Alana Maurushat, "From Cybercrime to Cyberwar: Security Through Obscurity or Security Through Absurdity?", *Canadian Foreign Policy Journal*, Cilt 19, Sayı 2, s. 120.

kolaylaştırdığı telif hakkı ihlali ve çocuk pornografisi gibi suçları içermektedir. "Bilgisayar bütünlüğü suçları" (*computer integrity offences*) olarak isimlendirilen son kategori, İnternete bağlı bilgisayarların, sistemlerin ve üzerinde işlenen verilerin bütünlüğünü, kullanılabilirliğini ve gizliliğini tehlikeye atan bilgisayar korsanlığı (*hacking*) ve virüs bulaştırma eylemlerini kapsamaktadır.[394] Özellikle son kategori, hem bireysel kullanıcılar hem de uluslararası aktörler açısından güvenlik ve güvenlik açığı endişelerini gündeme getirmektedir. Bu bağlamda 2001 yılında imzalanan ve 2004 yılında yürürlüğe giren "Avrupa Konseyi Siber Suçlar Sözleşmesi" (*The Council of Europe's Convention on Cybercrime*), siber suçlara yönelik anlaşmaya taraf ülkelerin ulusal kanunlarındaki mevzuatların, hükümlerin ve diğer önlemlerin uyumlu hale getirilerek uluslararası işbirliklerinin teşvik edilmesi açısından son derece faydalı olmuştur.[395] Öyle ki çok taraflı bir siber suç enstrümanına üyelik hali, ulusal ceza ve usul hukukunun yeterliliğinin arttığı algısına karşılık gelmekle birlikte söz konusu alanlardaki mevcut çok taraflı hükümlerin genellikle etkili sayıldığını göstermektedir. Ek olarak ise sözleşmeye taraf olmayan ülkeler üzerinde dolaylı etkiler yaratarak mevzuatlarına yönelik modeller oluşturabilmektedir. Uluslararası düzeydeki bu dağınık durum ve ulusal yasaların siber suçlar, yargı temelleri ve işbirliği mekanizmaları açısından çeşitliliği, farklı tematik ve coğrafi kapsamı olan birden çok siber suç enstrümanının varlığıyla ilişkili olabilmektedir.[396]

Netice olarak siber suçlar, siber uzay sahasındaki tartışmasız en ciddi endişe unsuru olarak nitelendirilmektedirler. Kötü amaçlı yazılımların giderek çoğalması, göreceli kullanım kolaylığı ve çevrimiçi anonimlik ile bir araya gelince suç unsuru teşkil eden faaliyet ve çabaların da hızla yükselmesine vesile olmuştur. İstatistiki olarak bakıldığında; 2018 yılı itibariyle siber suçların dünyada yarattığı total maliyet 2,7 Milyar Dolara ulaşmış ve siber olanaklara dayanan yıllık toplam şikayet sayısı

---

[394] Ian Walden, "Crime and Security in Cyberspce", *Cambridge Review of International Affairs*, Cilt 18, Sayı 1, Nisan 2005, s. 52.

[395] Council of Europe, "Convention on Cybercrime", No: 185, 23 Kasım 2001, Budapeşte, *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185*, (Erişim Tarihi: 23 Şubat 2020).

[396] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, New York Şubat 2013, s. 72.

350 bini aşmıştır.[397] Uluslararası İlişkiler içerisindeki aktörlerin altyapılarını ve sistemlerini siber suç saldırılarına karşı koruyabilmeleri için küresel harcamaların artmaya devam edeceği ve 2021 yılından itibaren yılda ortalama 6 trilyon dolar seviyelerine ulaşılacağı öngörülmektedir.[398] Dolayısıyla siber suçların diğer geleneksel suçlara kıyasla daha kârlı hale geldiği görülmektedir ve küresel ilişkilerde siber suçların yıllar geçtikçe daha da büyük çaplı endişe unsuru haline evrileceği düşünülmektedir.

2.4. Siber Terör ve Siber Savaş

"Terörizm" (*Terrorism*), kendisini çeşitli şekillerde gösterebilen çok yönlü bir olgudur ve devletler tarafından üzerinde yasal kabulü bulunmayan, genelgeçer tatmin edici tanımlamadan uzak muğlaklığı ile ön plana çıkmaktadır. Birçok aktör –bireyler, gruplar, devletler– kasıtlı bir terör-şiddet stratejisi bağlamında cinayet, mülkün yok edilmesi, adam kaçırma vb. suç teşkil eden davranışları, yerel ve uluslararası çevrelerde, ideolojik, dini, siyasi vb. çeşitli amaçlar doğrultusunda sergileyebilmektedirler. Bu durum, ulusal ve uluslararası düzeydeki karar vericilerin ve kanun yapıcıların terörizm kavramına ortak bir tanımlama getirememelerine rağmen soruna yönelik eşit derecede çeşitli yaklaşımlar benimsenmesine yol açmaktadır.[399]

Soğuk Savaş sonrası dönemdeki Uluslararası İlişkilerde devletler açısından en büyük endişelerden biri olarak "teröristlerin nükleer, biyolojik, kimyasal ve siber teknolojileri silah haline getirmesi" gösterilmiştir. Küresel teknolojik yayılmanın giderek hızlanması ve terörist motivasyonların sivillere büyük çaplı ölüm ve zarar vermeye kayması neticesinde söz konusu endişeler hâsıl olmuştur; ancak yüksek teknolojili terörizm kapsamında siber teknolojiler diğerlerine kıyasla farklılık

---

[397] Federal Bureau of Investigation, Internet Crime Complaint Center, "2018 Internet Crime Report", *https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2018-internet-crime-report*, (Erişim Tarihi: 24 Şubat 2020).

[398] Iman Ghosh,"This is the Crippling Cost of Cybercrime on Corporations", World Economic Forum, 7 Kasım 2019, *https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity*/, (Erişim Tarihi: 24 Şubat 2020); Pierluigi Paganini, "Cybercrime Statistics in 2019", Security Affairs, 18 Ocak 2020, *https://securityaffairs.co/wordpress/96531/cyber-crime/cybercrime-statistics-in-2019.html*, (Erişim Tarihi: 24 Şubat 2020).

[399] Sébastien Jodoin, "Terrorism as a War Crime", *International Criminal Law Review*, Cilt 7, Sayı 1, 2007, ss. 78-80.

göstermektedir. Öyle ki nükleer, biyolojik ya da kimyasal maddelere kıyasla daha kolay erişilebilir, daha az maliyetli ve riskli olan siber teknolojiler, istihbarat toplanmasından propaganda yayılmasına ya da finansal kaynaklarının artırılmasına kadar çok çeşitli sonuç spektrumu sunmaktadır.[400] Bu bağlamda "Siber Terörizm" (*Cyberterrorism*), "bilgisayar ağ araçları kullanılarak kritik ulusal altyapılara –enerji, ulaşım, devlet işlemleri vs.– zarar verilmesi veya sonlandırılması" şeklinde tanımlanabilmektedir. Siber terörizmin dayanağı olarak devletlerin ve kritik altyapıların işletilebilmesi için bilgisayar ağlarına daha bağımlı hale gelmesi ve beraberinde yeni güvenlik açıklarının ortaya çıkması gösterilmektedir. Bilhassa siber terörizmin anonimlik, büyük hasar verebilme potansiyeli, psikolojik etkisi ve medya cazibesi gibi özellikleri dikkate alındığında 21. yüzyıl teröristleri açısından oldukça cezbedici bir seçenek olarak kabul edilmektedir.[401]

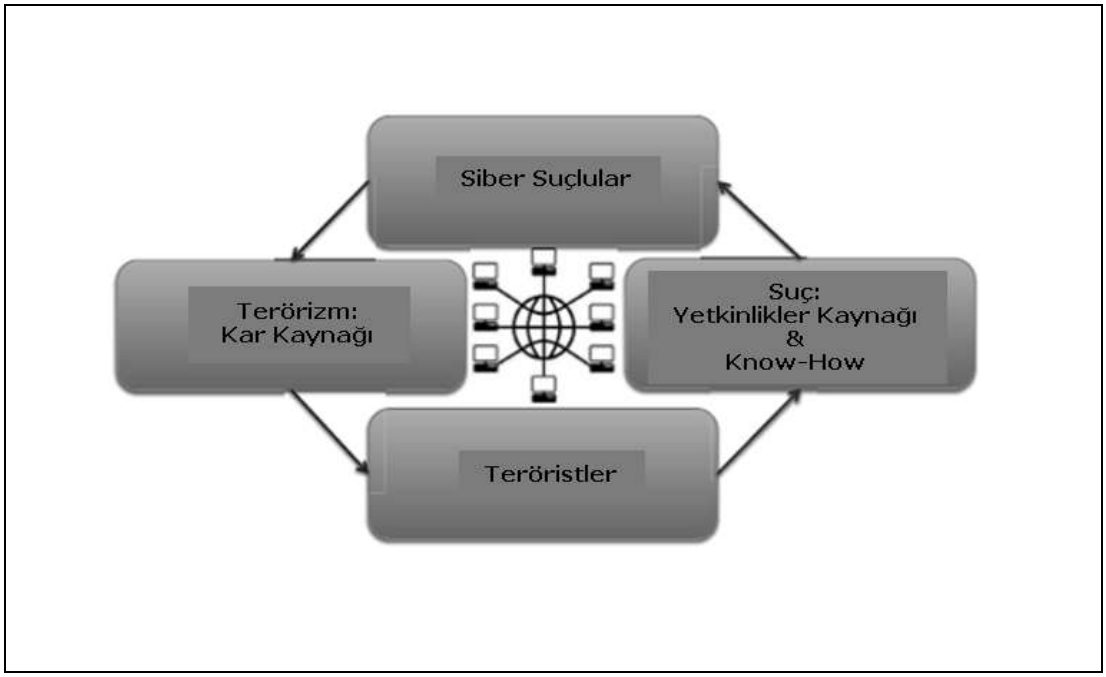
Siber terörizm, terörizmin siber uzay sahasına yakınsaması olarak ele alınabilmektedir. Genel olarak devlet dışı aktörler tarafından hükümetlere ya da toplumlara çeşitli hedefler doğrultusunda baskı uygulanması ve korku yaratılması için bilgisayar tabanlı saldırıların gerçekleştirilmesi veya saldırı tehditleri oluşturulması şeklinde anlaşılabilmektedir. Bu noktada siber uzay sahası, terörist eylemlerin gerçekleştirilebilme aracı haline gelmektedir ve sadece kişilere ve fiziksel mülkiyetlere değil, kimliklere ve dijital mülkiyetlere yönelik de yıkım ve bozulma eylemleri gerçekleştirilebilmektedir.[402] Bilgi devriminin en önemli neticelerinden biri olan İnternet, birçok açıdan terörist faaliyetler ve operasyonlar için ideal ortamı sağlamaktadır. İnternetin son derece düşük maliyetlerle dünya çapında iletişim sağlayabilmesi, teröristlerin komuta ve kontrol altyapıları için İnterneti önemli bir iletişim aracı haline getirmektedir. Yine potansiyel hedefler ve silah sanayi gibi önemli alanlarda bilgiler toplanabilmektedir. Ek olarak ise terörist propagandaları için İnternetin bir çeşit platform olarak kullanımı tercih edilebilmektedir.[403]

---

[400] David P. Fidler, "Cyberspace, Terrorism and International Law", *Journal of Conflict & Security Law*, Cilt 21, Sayı 3, 2016, s. 476.
[401] Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?", *Studies in Conflict & Terrorism*, Cilt 28, Sayı 2, 2005, s. 130.
[402] Lee Jarvis & Stuart Macdonald, "What Is Cyberterrorism? Findings From a Survey of Researchers", *Terrorism and Political Violence*, Cilt 27, Sayı 4, 2015, ss. 659-662.
[403] Abraham R. Wagner, "Terrorism and the Internet: Use and Abuse", Editörler: Mark Last & Abraham Kandel, *Fighting Terror In Cyberspace*, World Scientific Publishing, Singapur 2005, s. 7.

Siber terörizm ile siber suç faaliyetleri tanımlanırken motivasyon ve eylem bölümlerinin ayrılması gerekmektedir. Motivasyon açısından siber terörizm açıkça farklıdır ve eylemlerini desteklemek için spesifik bir gündem ile çalışmaktadır. Ayrıca siber suç ile siber terörizm finansal veya ekonomik amaçlarla ayırt edilebilmektedirler. Bu doğrultuda siber suçluların eylemleri para kazanma amacıyla bireylere ya da gruplara zarar verebilirken, siber teröristlerin eylemleri ulusal güvenlik ve kamu güvenliğine yönelik zararlar teşkil edebilmektedir.[404] Herhangi bir suçun siber terörizm kapsamına girebilmesi için işleniş biçimi olarak siber nitelikte, amaç ve yarattığı sonuçlar açısından ise terör suçu niteliğinde olması gerekmektedir.[405]

Tablo-20: Terörizm ile Suç Arasındaki Korelasyon



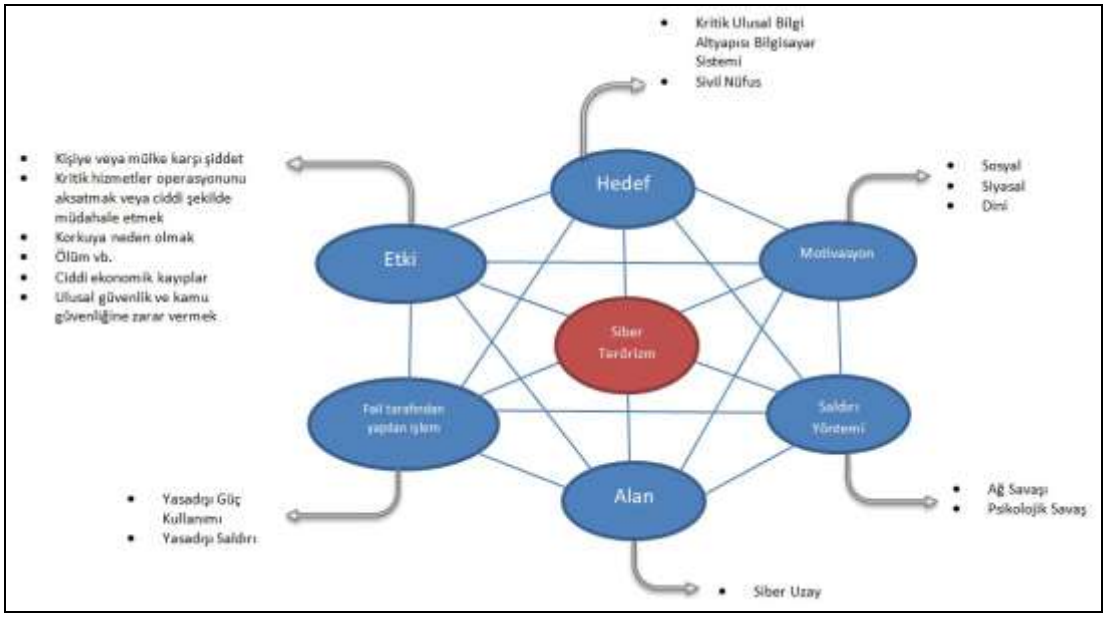
Kaynak: Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security In Cyberspace*, EPFL Press, Lausanne 2013, s.171.

[404] Rabiah Ahmad & Zahri Yunos, "A Dynamic Cyber Terrorism Framework", *International Journal of Computer Science and Information Security*, Cilt 10, Sayı 2, 2012, s. 151.
[405] Naki Sarıkavak, "Siber Terörizmi Anlamak", *Milli Güvenlik ve Askeri Bilimler Akademik Dergisi,* Cilt 2, Sayı 6, İlkbahar 2015, s. 74.

Tablo 20'de de görüldüğü üzere İnternet, suçlular ile teröristler arasında özellikle finansal işlemlerde bağlantı sağlamaktadır. Suçlu unsurlar ile terörist unsurlar, finansal hedeflere ulaşmak ve teknik yeterlilikleri paylaşmak için siber uzay sahasında işbirliği yapmaktadırlar. Özellikle teröristler, siber suçluların yeteneklerini ve sağlayabilecekleri hizmetleri kendi faaliyetlerini finanse etmek için kullanabilmekte ve böylelikle ihtiyaç duydukları bilgi işlem gücüne erişebilmektedirler.[406]

Siber terörizmin dinamik çerçevesi (Tablo-21) kapsamında kritik altyapıların birbiriyle daha bağımlı olması, maksimum düzeyde bozulmalara izin veren hedeflerin seçilebilmesini teröristler açısından kolaylaştırmaktadır.

Tablo-21: Dinamik Siber Terörizm Çerçevesi



Kaynak: Rabiah Ahmad & Zahri Yunos, "A Dynamic Cyber Terrorism Framework", *International Journal of Computer Science and Information Security*, Cilt 10, Sayı 2, 2012, s. 154.

Siber terörizmin arkasındaki motivasyon güçleri insanları ve aldıkları kararları etkileyebilecek olan sosyal, politik ve dini perspektiflerdir. Siber teröristler çok çeşitli araçlar ve teknikler aracılığıyla hedeflenen sistem üzerindeki güvenlik

[406] Solange Ghernaouti, *a.g.e.*, s. 171.

açıklarından yararlanarak ağ savaşı veya psikolojik savaş şeklinde saldırabilmektedirler. Bu doğrultuda bilinçli olarak yasadışı saldırılar veya güç kullanımı uygulanmaktadır ve hedef unsurları hükümetler, kurumlar, mülkler ya da kişiler olabileceğinden yaratacağı etkiler oldukça ciddi ve ağır olabilmektedir.[407]

Diğer yandan "Siber Savaş" (*Cyber War*) teriminin kullanımına bakıldığında; askeri uzmanlarca "kinetik etki" olarak da yorumlanan fiziksel dünyaya yansıyan dolaylı ve sonuçsal etkiler söz konusudur. Örneğin; düşman olarak addedilen devletin insansız hava aracının komuta ve kontrol sistemine kötü amaçlı yazılımların bulaştırılmasıyla tam kontrolün ele alınması ve aracın yanlış hedeflere saldırmasının sağlanması ya da aracın kendisini imha etmesi, siber savaş eylemleri kapsamında nitelendirilmektedir. Hedeflenen amaç doğrultusunda güç kullanılması anlamına gelen "savaş", siber uzay sahasının sanal araçları kullanılarak siber-fiziksel etkiler yaratıyorsa "siber savaş" halini almaktadır.[408] Siber savaş tartışmalarındaki zorluğun kaynağı olarak siber uzay sahasındaki saldırı, savunma ve şiddet kavramlarının çözülmesi zor doğası gösterilmektedir. Herhangi bir saldırının siber savaşın parçası olup olmadığının belirlenebilmesi için şu üç önemli özelliğin incelenmesi gerekmektedir: Örgütsel kaynağı ve coğrafi kökeni (Eylemin arkasında devlet var mıdır?); Sonuçları (Saldırı, hasara neden olabilir mi? Can ve mal kaybı yaratabilir mi?); ve Karmaşıklık düzeyi (Saldırı, devletler için mevcut koordineli kaynaklar ve karmaşık planlamalar gerektiriyor mu?).[409] Eğer yapılan saldırı, yukarıda belirtilen bu üç özelliği barındırıyorsa siber savaş kapsamında ele alınabilmektedir.

Siber savaşlar, bilgisayarların yararlılığına ya da ağların kötüye kullanımının caydırılmasına bakılmaksızın devletler arasında veya devlet ile devlet-dışı aktörler arasında sürekli olarak devam etmektedir. Özellikle askeri ve stratejik açıdan yaklaşıldığında siber savaşların çelişkili ve benzersiz bir boyutu belirmektedir: Bir taraftan siber alanın benzersizliği ve spesifik formu korunurken, diğer taraftan ise askeri ve stratejik her şey için bilgisayarlara, ağlara ve iletişim araçlarına bağımlılık yaratarak diğer etki alanlarını da işgal etmekte ve kendi formuna dinamik olarak

---

[407] Rabiah Ahmad & Zahri Yunos, *a.g.m.,* s. 154.
[408] Gary McGraw, *a.g.m.*, s. 112.
[409] Lior Tabansky, "Basic Concepts in Cyber Warfare", *Military and Strategic Affairs*, Cilt 3, Sayı 1, Mayıs 2011, ss. 82-83.

dahil etmektedir.[410] İşte bu bağlamda, askeri ve ekonomik faaliyetlerin desteklenebilmesi adına karmaşık siber sistemlere bağımlılığın sürekli artması, özellikle büyük devletlerde devlet dışı aktörler ve düşman devletler tarafından sömürülebilecek yepyeni güvenlik açıklarının devamlı yaratılmasına vesile olmaktadır. Siber savaşlarda da bu tarz güvenlik zaafiyetleri, büyük sonuçların doğmasına neden olabilmektedir. Fiziksel dünyadaki savaşların kaynak, araç ve devinim maliyetlerinin yüksekliği, siber savaşlarda söz konusu değildir. İnternetin güvenlikten ziyade kullanım kolaylığı için tasarlanmış olması ise saldırı unsurlarının savunma unsurları üzerinde avantajlı olmasını sağlamaktadır. Stratejilere ve hedeflere uygun olarak kullanılabilecek araçların fazlalığı, esneklik ve hızla yeniden oluşturulabilme kabiliyetleri, siber savaşlarda savunmanın en önemli bileşenleri olarak öne çıkmaktadır.[411] Siber savaşa dair en ilginç örneklerden biri olarak; Eylül 2007'de İsral'e ait F-15 ve F-16 jetlerinin Suriye'deki Deyrizor şehrinde bulunan nükleer tesisi bombalaması gösterilmektedir.[412] Buna göre İsrail İstihbarat ve Özel Operasyonlar Enstitüsü'nün (MOSSAD) bilgisayar korsanı ajanları tarafından Suriye'nin hava savunma sistemine siber saldırı yapılmış ve iletişim ağları istila edilerek sistem yöneticisi devralınmış ve sensörlerin yaklaşan uçakları göremeyecek şekilde yönlendirilmesi sağlanmıştır.[413] Söz konusu bu örnek olayda, siber saldırı alanının aşılarak kinetik etkiye açık şekilde dönüştüğü ve karmaşık bir süreçle tahribat yaratıldığı gözler önüne serilmekte ve siber savaş tanımı karşılanmaktadır.

Son olarak siber savaş eylemleri ifade edilirken kullanılan "Siber Silah" (*Cyberweapon*) terimine değinmekte yarar görülmektedir. Siber silahlar, yazılımdır ve insanlar tarafından yazılmaktadırlar veyahut da insanlar tarafından yazılıp konfigüre edilen yazılımlar üzerinden yazılabilmektedirler. Talimatların işlenebilmesi için bilgi işlem donanımına ihtiyaç söz konusudur ve hedef sistemin

---

[410] Stephen J. Cimbala & Roger N. McDermott, "A New Cold War? Missile Defenses, Nuclear Arms Reductions, and Cyber War", *Comparative Strategy*, Cilt 34, Sayı 1, 2015, s. 106.
[411] Joseph S. Nye, Jr., *a.g.e.,* ss. 4-5.
[412] Gary McGraw, *a.g.m.*, s. 112.
[413] Sharon Weinberger, "How Israel Spoofed Syria's Air Defense System", Wired, *https://www.wired.com/2007/10/how-israel-spoo/*, (Erişim Tarihi: 26 Şubat 2020); Mark Mazetti & Helene Cooper, "U.S. Confirms Israeli Strikes Hit Syrian Target Last Week", The New York Times, 12 Eylül 2007, *https://www.nytimes.com/2007/09/12/world/middleeast/12syria.html*, (Erişim Tarihi: 26 Şubat 2020); BBC News, "Israel Admits Striking Suspected Syrian Nuclear Reactor in 2007", 21 Mart 2018, *https://www.bbc.com/news/world-middle-east-43481803,* (Erişim Tarihi: 26 Şubat 2020).

açık kusurlarını kullanmaktadırlar. Siber silahlar, hedef sistemlerde güncel olarak savunucuların farkında olmadığı güvenlik açıklarından yararlanabilen ve istenen etkiyi eksiksiz olarak yaratabilen, hem taktiksel hem de operasyonel öneme sahip temel araçlardır. Öyle ki, eğer doğru bit doğru bilgisayarda doğru zamanda çevrilirse, bir ülkenin tüm elektrik şebekesi karanlığa itilebilir.[414] Netice olarak, yukarıda paylaşılan tüm bilgiler göstermektedir ki; uluslararası aktörler açısından siber uzay sahasında "siber güvenlik" inşası son derece önemlidir ve hatta üstünlük elde edebilmenin esas yolu olarak görülebilmektedir. Herhangi bir ülkenin ya da aktörün saldırgan siber yetenekleri, kalıcı olarak etkisiz hale getirilememektedir.[415] Siber alanın dinamikliğine bağlı olarak sürekli ortaya çıkan yeni güvenlik açıkları, Uluslararası İlişkilerde siber güvenliğin önemini stratejik olarak her geçen gün arttırmaktadır.

2.5. Siber Güvenlik

"Güvenlik" (S*ecurity*) kavramı, II. Dünya Savaşı sonrası dünyada yeni bir öncü konsept olarak 1970'lere kadar askeri gündem üzerinden değerlendirilmiş, 1970 sonrasında ise süper güçler arasındaki nükleer ilişkilerin olgunlaşmasıyla birlikte uluslararası güvenlik gündeminin askeri ve politik odağında giderek genişlemiş, 1990'lardan itibaren ise askeri güç ve devletler arası stratejik ilişkiler eksenli baskın güvenlik anlayışının; ekonomik güvenlik, çevresel güvenlik, toplumsal güvenlik, insani güvenlik, gıda güvenliği gibi çeşitlenmelere evrildiği görülmüştür.[416] Toplumsal anlamdaki temel değişiklikler, beraberinde insanlık adına yeni güvenlik sorunlarını ve dolayısıyla yeni güvenlik türlerini oluşturmuştur. Bu sert değişim süreci; bilimsel bilgide yaşanan büyüme, durmaksızın devam eden teknolojik yenilikler ve bunların yayılması, küresel pazarlar, kültürel olarak farklı toplumlar ile farklı sosyal sistemler ve değerler arasında artan temas ve çatışmalardan kaynaklanmaktadır. 11 Eylül 2001 Terör Saldırıları sonrasında ABD tarafından

---

[414] Timo Kiravuo & Mikko Särelä, "The Care and Maintenance of Cyberweapons", Editörler: Jari Rantapelkonen & Mirva Salminen, *The Fog of Cyber Defence*, National Defense University, Publication Series 2, Article Collection No 10, Helsinki 2013, s. 218.
[415] Gary McGraw, *a.g.m.*, s. 117.
[416] Ken Booth, *Theory of World Security*, 1. Basım, Cambridge University Press, New York 2007, s. 96.; Barry Buzan & Lene Hansen, *The Evolution of Internationsal Security Studies*, 1. Basım, Cambridge University Press, New York 2009, ss. 1-2.

terörizme karşı başlatılan küresel savaş, güç ve insani amaçlarda yaşanan söz konusu tektonik değişimlerin arka planına karşı tam olarak kavranabilmektedir.[417] Özellikle 9/11 Terör Saldırıları, bir zamanlar sadece (ya da çoğunlukla) devlet kontrolünde olan teknolojinin, artık devlet dışı aktörlerin yıkıcı güçlerinin eline kolaylıkla geçebildiğini ve mesafelerin etkilerinin ortadan kalktığını en net şekilde göstermiştir.[418] Dolayısıyla güvenlik üzerindeki devlet tekeli, "dijital bağlantı çağı" olarak da nitelendirilen 21. yüzyılda zayıflamıştır; çünkü ağlara bağlı olan her şey saldırıya uğrayabilir ve sızmalara karşı savunmasız kalabilmektedir. Bu bağlamda siber alanın güvenliği ile dijital ve hesaplamalı teknolojilerden kaynaklanan tehdit fırsatları ifade edilmektedir. Tüm güvenlik çerçevelerinde kusursuz ve eksiksiz korumanın gerçekleştirilebilmesi oldukça zor olmakla birlikte hesap tabanlı sistemlere dayanan siber sahanın güvenliğinin kusursuz olarak sağlanabilmesi ise neredeyse imkânsızdır. Tüm elektronik cihazların bir şekilde ağ bağlantısına sahip olması ve siber saha içerisindeki devletlerin kritik altyapılarından ulusal endüstrilere, bireylerden şirketlere kadar aktörel çeşitliliğin fazla olması, karmaşık bir güvenlik ve koruma sorununu öne çıkarmaktadır.[419]

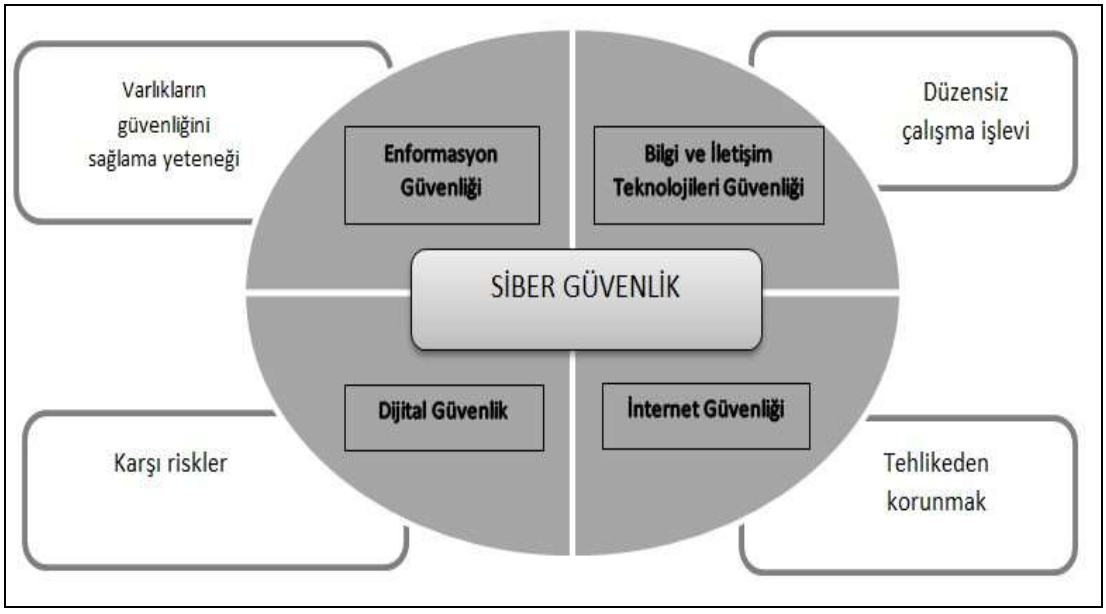
9/11 Terör Saldırıları sonrası dönemde İnternetin önemli bir yaşam biçimi haline gelmesi ve yaşanan son teknolojik gelişmeler ışığında vatandaşların, şirketlerin ve hükümetlerin karşılıklı etkileşimler yaratabilmesi ve işbirlikler oluşturabilmesi, dijital altyapılara olan yoğun bağımlılığı daha da arttırmıştır. Artan bu bağımlılık hali sayesinde dijital altyapılar, ulusal refah ve güvenliğin sağlanabilmesi için korunması gereken ulusal varlıklardan biri haline evrilmiş ve siber uzay sahası, daha fazla aktörün içerisinde doğrudan yer alabildiği uluslararası rekabet sahalarından birine dönüşmüştür.[420] Bu bağlamda Uluslararası Telekomünikasyon Birliği (*International Telecommunication Union*, ITU) tarafından

---

[417] Edward A. Kolodziej, "Security and International Relations", 1. Basım, *Cambridge University Press*, New York 2005, s. 49.
[418] Joseph S. Nye, Jr. & David A. Welch, *Understanding Global Conflict and Cooperation: An Introduction to Theory and History*, 10. Basım, Pearson, Boston 2017, s. 2.
[419] Brandon Valeriano & Ryan C. Maness, "International Relations Theory and Cyber Security: Threat, Conflict, and Ethics in an Emergent Domain", Editörler: Chris Brown & Robyn Eckersley, *The Oxford Handbook of International Political Theory*, 1. Basım, Oxford University Press, New York 2018, ss. 260-261.
[420] Sherali Zeadally, Gregorio Martinez & Han-Chieh Chao, "Securing Cyberspace in the 21st Century", *Computer*, Cilt 46, Sayı 4, s. 22.

Siber Güvenlik (C*yber Security*); "siber ortamı, kuruluşları ve kullanıcıların varlıklarını –bağlı bilgi işlem aygıtları, personeller, altyapı, uygulamalar, hizmetler, telekomünikasyon sistemleri, siber ortamda iletilen ve depolanan veriler– korumak için kullanılabilecek araçlar, politikalar, güvenlik konseptleri ve önlemleri, yönergeler, risk yönetim yaklaşımları, eylemler, eğitimler, en iyi uygulamalar, teminatlar ve teknolojilerin toplanması" şeklinde tanımlanmaktadır.[421] Dolayısıyla bu terim, siber alanla ilgili tüm risklerin azaltılmasına ve çözümlenmesine yönelik bir durumu ve süreci ifade etmektedir. Bu doğrultuda da olası bir tehdide karşı politik, teknik, idari, yasal ve diğer tüm önlem çeşitlerini içermektedir. Güvenli bir siber alanda bütünlük, gizlilik ve bilgi güvenilirliği ile birlikte kuruluşların ve kullanıcıların varlıkların korunması ve güvenlik özelliklerinin sürdürülmesi söz konusudur.[422]

Tablo-22: Siber Güvenlik Kapsamındaki Güvenlik Kavramları

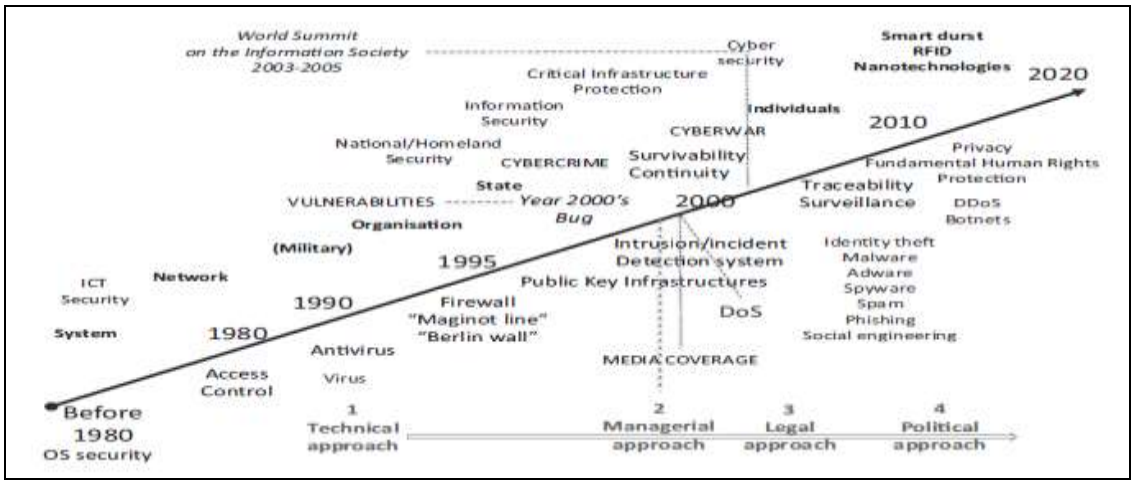


Kaynak: Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security In Cyberspace*, EPFL Press, Lausanne 2013, s. 330.

[421] International Telecommunication Union, *Series X: Data Networks, Open System Communications and Security – Telecommunication Security; Overview of Cybersecurity*, ITU-T X.1205, 04/2008, s. 2.
[422] Birgit Mitterlehner, "Cyber-Democracy and Cybercrime: Two Sides of the Same Coin", Editörler: Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos, *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*, 1. Basım, Springer, New York 2014, s. 210.

Öte yandan, Tablo 22'de de görüldüğü üzere siber güvenlik kavramıyla ilişkili olarak kullanılan pek çok terimin –bilgi ve iletişim teknolojileri güvenliği, enformasyon güvenliği, dijital güvenlik, İnternet güvenliği– ana unsurunu dijital verilerin ve bilgilerin güvenliği oluşturmaktadır. Günlük faaliyetlerde bilgi ve iletişim teknolojilerinin kullanımı ile ilişkili risklere cevap niteliğinde olan siber güvenlik, veri/bilgi/enformasyon/istihbarat risklerini kabul edilebilir asgari seviyelere indirgeyerek kontrol altına almayı hedeflemektedir. Bu sebeple de devletler, kurumlar, BİT teknolojileri ve İnternet teknolojileri ile ilgilenen bireyler açısından en genel anlamıyla siber güvenlik, veri/bilgi/enformasyon/istihbarat/altyapı güvenliği anlamına gelmektedir.[423] Öyle ki bilginin güvenliği, mevcut biçimine ya da konumuna bakılmaksızın, bilginin kendisinin korunması adına BİT güvenliği kavramları üzerine genişledikçe, siber güvenliğin de bilgi güvenliği ve BİT güvenliğinin genişlemesi olarak görülmesi olağandır. Bu nedenle siber güvenlik; kişi, kurum ya da devletlerin bilgilerinin veya bilgi sistemleri kaynaklarının korunmasından daha fazlasıyla ilgili olmaktadır. Dolayısıyla siber ortamda kaynak kullanan aktörlerin ve genel olarak topluma ait olan varlıkların korunması da doğrudan siber güvenlik kapsamına dâhildir.[424]

Tablo-23: Bilgi ve İletişim Teknolojileri (BİT) Güvenliğini Evrimi



Kaynak: Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security In Cyberspace*, EPFL Press, Lausanne 2013, s. 333.

[423] Solange Ghernaouti, *a.g.e.*, ss. 329-330.
[424] Rossouw von Solms & Johan van Niekerk, "From Information Security to Cyber Security", *Computers & Security*, Cilt 38, 2013, s. 101.

1990'ların ortalarına kadar özellikle mühendisler tarafından teknik bir sorun olarak görülen siber güvenlik, ilk işletim sistemlerinin (*operating systems, OS*) ordu, bankacılık ve genel finans gibi hassas alanlarda kritik uygulamalar için ayrılmış erişim kontrol mekanizmalarındaki yapılandırma yönetimi ve performans izlemenin yanı sıra ağ yönetiminin de ayrılmaz bir parçası olarak "ağ güvenliği" şeklinde teknolojik bir yaklaşımla tanımlanmıştır (Tablo-23, I. Aşama). 2000'lerdeki bilgi teknolojilerinin teknik bir alandan yönetim alanına evrilme süreci, teknolojik ve enformasyonel risk yönetimine yol açmış (Tablo-23, II. Aşama), ancak söz konusu enformasyonel güvenlik yönetimi, BİT altyapılarının suç amaçlı giderek artan kötüye kullanımlarının –yasadışı dinleme, sistem müdahaleleri, kötü amaçlı yazılımların yayılması, güvenlik açıklarından sızıntılar vb.– üstesinden gelememiş ve yönetim güvenliği sınırlarının mevzuata taşınmasına katkıda bulunmuştur (Tablo-23, III. Aşama). Buna karşın, cezai davranışları caydırıcı ve yasadışı eylemleri cezalandırıcı yasal kurumlar ve yasaların oluşturulması, belirli bağlamlarda koruma sağlamakla birlikte yine de suç eylemlerini tamamen önleyememektedir. Ek olarak BİT güvenliği hükümet, diplomasi ve askeri konularda büyük endişe kaynağı oluşturduğundan, siyasi boyut tarafından bilgi güvenliğinin teknik, yönetimsel ve yasal yaklaşımları tamamlanmaktadır (Tablo-23, IV. Aşama). Dolayısıyla siber güvenlik, doğrudan devlet egemenlikleri, ulusal güvenlik ve vatandaşların güvenliğiyle ilgili olmaktadır.[425] Bu bağlamda da ülkelerin kendi kritik altyapılarının yararlı ya da zararlı kullanımına yönelik daha güçlü bir kontrol kurarak kendi güvenlik seviyelerini yükseltmeleri beklenebilmektedir.[426] Devletler, daha güçlü siber yetenekler geliştirdikçe, onları sadece düşman devlet ya da unsurlara karşı değil, aynı zamanda siviller üzerinde de kullanabilmektedirler. Örneğin; Birleşik Krallık merkezli bir şirket tarafından geliştirilen *FinFisher* isimli karmaşık bir casus yazılım, Mısır, Bahreyn ve Uganda'daki baskıcı rejimler tarafından satın alınarak casusluk amacıyla kullanılmıştır.[427] Diğer durumlarda da siber suçlar için

[425] Solange Ghernaouti, *a.g.e.,* ss. 331-333.
[426] Eneken Tikk, "Ten Rules for Cyber Security", *Survival: Global Politics and Strategy*, Cilt 53, Sayı 3, Haziran-Temmuz 2011, s. 122.
[427] Nick Hopkins & Jake Morris, "UK Firm's Surveillance Kit 'Used to Crush Uganda Opposition'", BBC News, 15 Ekim 2015, *https://www.bbc.com/news/uk-34529237*, (Erişim Tarihi: 2 Mart 2020).

geliştirilmiş olan inovasyonlar, hükümetler tarafından yabancı ajanların ve hatta kendi vatandaşlarının gözetlenmesinde yeniden kullanılabilmektedir.[428]

Sonuç olarak; hükümetler ve şirketler, siber uzay sahası içerisindeki konumlarını, sistemlerini, vatandaşlarını, çalışanlarını ve müşterilerini güvence altına almaya ve tehditlere karşı korumaya çalışmaktadırlar. Siber uzay alanındaki karmaşık yapı göz önünde bulundurulduğunda, güvenlik adına işbirliği elzem olmaktadır. Siber saldırıların önlenebilmesi ve uygun şekillerde müdahale edilebilmesi konusundaki işbirliği, dünyanın çeşitli ülkelerindeki hükümetlerin ve ekonominin tüm sektörlerindeki şirketlerin siber güvenlik politikalarının ayrılmaz bir parçası haline gelmiştir. Siber güvenlik olaylarının yönetimi için mevcut kurumsal çerçeve, her geçen gün dâhil olan aktörlerle –ağ operatörleri, İnternet servis sağlayıcıları, işletmeler, satıcılar, kolluk kuvetleri, kritik altyapı operatörleri, hükümetler, askeri kurumlar, siyasetçiler, diplomatlar, hukukçular vb.– birlikte daha da genişlemektedir.[429] Genişleyen kurumsal çerçeveye bağlı olarak geliştirilen siber yetenekler, geleneksel olmayan nitelikte yeni olarak adlandırılabilecek caydırılık unsuru da oluşturmaktadır. "Siber Caydırıcılık" (*Cyber Deterrence*), rakip aktörlerin bilgi teknolojilerine karşı siber yeteneklerin saldırı tehdidi olarak kullanılması şeklinde tanımlanabilmektedir. Dolayısıyla devletler, bilgi ve iletişim teknolojilerine ne kadar bağımlı olurlarsa, yeni aktörler tarafından ileri teknoloji ile tehdit edilebilirler ve siber yetenekleri zengin olan baskın devletlere karşı siber saldırı yelpazesi geniş olacağından savunmasız kalma olasılıkları artmaktadır.[430] Siber güvenlik teknolojisinin karmaşık yapısı ve giderek artan siber güvenlik tehditleri göz önüne alındığında, politika yapıcıların sürekli olarak en son ve en güncel tehdide nasıl tepki verileceğine ilişkin kararlarla karşı karşıya kalması söz konusu olacaktır. Bununla birlikte, siber güvenlik önlemlerine ilişkin kararların teknoloji uzmanlarına devredilmesi sıklıkla söz konusu olduğundan, politika yapıcıların verdiği kararların gerçekten pratiğe alınıp alınmadığı kontrolü zorlaşmaktadır. Çeşitli alternatif

---

[428] Damien Van Puyvelde & Aaron F. Brantly, *a.g.e.*, s. 149.
[429] Nazli Choucri, Stuart Madnick & Jeremy Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives", *Infromation Technology for Development*, Cilt 20, Sayı 2, 2014, s. 118.
[430] Sandra Gaycken & Maurizio Martellini, "Cyber as Deterrent", Editör: Maurizio Martellini, *Cyber Security: Deterrence and IT Protection for Critical Infrastructures*, Springer, Cham 2013, ss. 3-4.

yaklaşımların örgütsel etkisine ağırlık verme şansı ise söz konusu olmayabilir.[431] Netice olarak; siber güvenliğin tüm boyutlarındaki *know-how* (belirli bir şeyin nasıl yapılacağının tam bilgisi)[432] eksikliği, dijital bölünmeyi genişleten ciddi altyapı eksikliği oluşturacağı gibi, siber güvenlik kültürünün desteklenmesi ise güvenli ve kapsayıcı bir bilgi toplumu inşasına katkı sağlayabilecektir. Bu nedenle, uygulanacak güvenlik önlemlerinin kapsamı ve niteliği ile ilgili kararlar almak için güvenlik ihtiyaçlarının doğru şekilde belirlenmesi gereklidir. Küresel güvenlik anlayışı ise siber güvenliğe multidisipliner ve sistemik bir yaklaşım benimseterek teknolojik ve enformasyonel risklerin en düşük seviyelerde tutulabilmesine vesile olmaktadır.[433]

3. Siber Uluslararası İlişkiler

"Siber Uluslararası İlişkiler" (*Cyber International Relations*), 20. yüzyılın sonundan bugüne değin siber uzay sahasının dikkat çeken büyümesi ve genişlemesiyle birlikte geleneksel uluslararası sistemde meydana gelen değişimlere ve yeniliklere bağlı yeniden yapılandırma ve dönüşüm halini belirtmektedir. Geleneksel uluslararası sisteme bakıldığında, egemen devletler arasındaki etkileşimin büyük güçler ve güç politikaları üzerinden egemenlik temel ilkesi odaklı olduğu ve sistem içerisindeki tüm aktörlerin devletlerin türevi olduğu ve devletler tarafından meşrulaştırıldığı anlayışı söz konusudur.[434] Devletler, 21. yüzyıl Uluslararası İlişkilerinde de hâkim aktör olmaya devam etmektedirler ancak giderek çeşitli devlet dışı aktörlerin baskılarına ve sınırlamalarına maruz kalmaktadırlar. Soğuk Savaş sonrası süreçte ABD'nin mevcut hegemonyasını konsolide etmesi ve uluslararası sistem içerisinde artan bağımsız devlet sayısı[435], uluslararası toplumda yeni iddiaların artmasına, yeni siyasi hedefler ve küresel ölçekli yeni rekabetler ile yeni bölgesel güç merkezlerinin oluşmasına, dolayısıyla yeni normların geliştirilmesine ve çeşitli işlev

---

[431] Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt & Joseph Weiss, *Cyber Security Policy Guidebook*, 1. Basım, John Wiley & Sons, Inc., New Jersey 2012, s. 39.
[432] William Little, H. W. Fowler & J. Coulson, *a.g.e.*, s. 1093.
[433] Solange Ghernaouti, *a.g.e.*, ss. 352-353.
[434] Robert A. Denemark, "World System History: From Traditional International Politics to the Study of Global Relations", *International Studies Review*, Cilt 1, Sayı 2, Yaz 1999, ss. 44-46.
[435] II. Dünya Savaşı sonrası 55 bağımsız egemen devlet varken, bu sayı günümüz itibariyle 195'e ulaşmıştır ve 193'ü BM üyesidir. Detaylı bilgi için bkz.: The Nations Online Project, "Independent States of the World", *https://www.nationsonline.org/oneworld/states.htm*, (Erişim Tarihi: 6 Mart 2020).

ve sorumluluklara sahip uluslararası örgütlerin çoğalmasına vesile olmuştur. Bunların yanı sıra, hiyerarşik güç ilişkileri ile karakterize edilen 20. yüzyılın geleneksel –iki kutuplu, çok kutuplu veya tek kutuplu– sistemleri, farklı asimetriler ve nispeten zayıf hiyerarşilerle karakterize edilen yeni yapısal biçimlere yavaş yavaş yol açmaya başlamıştır.[436] Böyle bir ortamda siber uzay sahasının genişlemesi ile tetiklenen birçok değişiklik üzerine çok disiplinli ve disiplinlerarası yaklaşımların, analizlerin ve tartışmaların giderek artması, sistemin daha da komplike bir hal almasına neden olmaktadır.[437] Siber Uluslararası İlişkiler ortamının belirsizliği, alanın yeniliğinden ziyade hassas, karmaşık ve anonim doğasına atfedilmekle birlikte uluslararası öngörülebilirlik ve istikrar elde edilmesi adına şeffaflığı arttıran ve işbirliği için gerekli tedbirleri alan, siber alanda kabul edilebilir davranışlar ortaya koyan normatif yaklaşımları öne çıkarmaktadır.[438] Giderek karmaşıklaşan sosyal, politik, ekonomik ve çevresel zorluklar neticesinde parçalanmış bilgi ya da basit bir temel araştırma bilgi birikimi üzerinde bile tam hâkimiyetin yetersiz kaldığı bu dönemde; hükümetler, akademiler ve özel sektörde faaliyet gösteren Uluslararası İlişkiler profesyonelleri, disiplinlerarası ve çok disiplinli politika ile ilgili bilgilere erişimin ve bunların harmanlanmasının etkili sorun çözme ve karar verme mekanizmaları için son derece kritik öneme sahip olduğunun giderek daha fazla farkına varmaktadırlar.[439] Bu bağlamda Vaishnav ve arkadaşları tarafından söz konusu önemin farkında ve disiplinlerarası bir perspektifle siber uzay sahasının "yeni" Uluslararası İlişkilerin "yeni" etkileşim sahası olduğuna dair on tespit son derece dikkat çekicidir:

1- Bu yeni gerçeklik alanının en belirgin özelliği, egemenlik ilkesi ve egemen devletlerin talep ve yetenekleri tarafından şekillenen uluslararası bir sistemde özel sektörün baskınlığıdır.

---

[436] Chintan Vaishnav, Nazli Choucri & David Clark, *a.g.m.*, ss. 562-563.
[437] Melania-Gabriela Ciot, "Cyberspace and The New World Order", *Studia Universitatis Babes-Bolyai-Studia Europaea*, Cilt 62, Sayı 2, s. 5.
[438] Chelsey Slack, "Wired yet Disconnected: The Governance of International Cyber Relations", *Global Policy*, Cilt 7, Sayı 1, Şubat 2016, s. 72.
[439] Sean S. Costigan & Chris Pallaris, "Knowledge Ecologies in International Affairs: A New Paradigm for Dialog and Collaboration", Editörler: Sean S. Costigan & Jake Perry, *Cyberspaces and Global Affairs*, Ashgate Publishing, Farnham 2012, s. 283.

2- Uluslararası İlişkileri tanımlayan ve oluşturan ana aktör olarak devlet, siber alanı tam anlamıyla kontrol edemez ve kendisini bu yeni siber gerçekliklerin sonuçlarından yalıtamaz.
3- Güvenliğe yönelik siber tehditlerin artan kanıtları, siber uzay sahasının siyasallaşmasını ve politika söylemlerindeki konumunu güçlendirmektedir.
4- Yeni tür asimetriler –özellikle daha zayıf aktörlerin daha güçlü aktörleri ne ölçüde etkileyebileceği ve tehdit edebileceği– ve yeni tür simetriler – daha zayıf aktörlerin daha güçlü aktörlerin bilgisayarlarına sızabilmesi– ortaya çıkmaktadır.
5- Yeni aktörlerin oluşması ve siber güce erişmesi, geleneksel uluslararası karar verme ortamlarını potansiyel olarak önemli şekillerde etkileyebilmekte ve değiştirebilmektedir.
6- Siber alanları yönetmek için oluşturulan yeni kurumlar ile geleneksel uluslararası organizasyonlar arasındaki artan yetki ve kontrol tartışması, zaten yeterince sıkıntılı olan uluslararası hesap verilebilirlik meselesini meşruiyet ve sorumluluk üzerinden yeni gerilimlerle daha da karmaşık hale getirmektedir.
7- Çeşitli siber çatışma türleri, yeni yöntem ve tezahürleri için potansiyeller ile belirginleşmektedir.
8- Siber alanın belirsizliğini azaltmak ve giderek daha fazla anarşik olarak algılanan bu ortama bir düzen ölçütü getirilmesi adına siber işbirliği türleri giderek artmakta ve çeşitlenmektedir.
9- Sivil toplumun siber tabanlı mobilizasyonu ve potansiyel olarak güçlendirilmesi söz konusudur.
10- Etki alanlarında yaşanan kesişmeler, "küresel bilgi toplumu" üzerine çeşitli organizasyonların gerçekleştirilmesine gerekçeler sağlamaktadır.[440]

Yukarıda sunulan tespitler göstermektedir ki; siber uzay sahası artık çıkar rekabetlerinin yaşandığı, çeşitli çıkar gruplarının kapsamında yer aldığı,

[440] Chintan Vaishnav, Nazli Choucri & David Clark, *a.g.m.*, ss. 563-565.

hükümetlerin çeşitli çatışmalar ve çekişmelerle kısıtlanabildiği oldukça karmaşık bir güç rekabet sahasıdır. Bu sahanın yapısı ve kapsamı, sürekli olarak, yeniden ve yoğun şekilde çok sayıda aktör tarafından tartışılmakta, oluşturulmakta ve tekrardan şekillendirilmektedir. Dolayısıyla siber uzay sahasının politik belirginliği artık daha fazla görmezden gelinemeyecek boyutlara ulaşmıştır.

3.1. Siberpolitik

Uluslararası İlişkilerde devlet istikrarını anlama konusundaki geleneksel yaklaşımlar, 19. ve 20. yüzyıllardaki deneyimlerden türetilmiştir; ancak siber dünya, devlet istikrarı ve kırılganlık dinamiklerini değiştiren etkileşimler, güç ve baskı için yeni mekanizmalar sağlamaktadır.[441] Devletler, dünya sahnesinde yine baskın aktör konumunda bulunmakta fakat aktör sayısı çok daha fazla ve dolayısıyla tam kontrolün sağlanması da bir o kadar zor görünmektedir. Joseph Nye'ın da belirttiği üzere; ülkeler içi ve ülkeler arası nüfusun büyük bir kısmı bilgiden gelen güce artık erişebilir pozisyona gelmiştir.[442] Giderek artan teknolojik yenilikler ve müdahaleler, bireylerin ve toplumların yaşamlarını derinden etkilemekte ve köklü değişimleri beraberinde getirmektedir. Öte yandan siber olanaklı teknolojilerin mevcut gerçeklikleri ne ölçüde değiştirdiği tartışmalı olmakla birlikte politika perspektifinden bakıldığında siber alan, geçmişte açık örneği olmayan yeni koşullar – sorunlar ve fırsatlar– yaratmakta ve yeni yönetişim modellerinin ortaya çıkmasına önemli ölçüde katkı sağlamaktadır. Bu durum, politikanın gittikçe daha etkileşimli hale gelmesine ve geleneksel politika anlayışlarının yeniden tanımlanmasına vesile olmaktadır. Yeni teknolojiler ve teknoloji yoğunluklu gündelik yaşam sayesinde sıradan vatandaşlar, sivil müdahalelerde benzersiz yollar edinmektedirler. Böylelikle de sivil toplum güçlendirilmekte ve teknoloji aracılı yeni kamusal alanlar geliştirilmektedir. İnternetin ve teknolojinin, demokrasilerde siyasal iletişimi

[441] Daniel Goldsmith & Michael Siegel, "Cyber Politics: Understanding the Use of Social Media for Dissident Movements in an Integrated State Stability Framework", *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, IEEE, 2012, s. 1321.
[442] Joseph S. Nye, Jr., *a.g.e.*, s. 1.

canlandırmak için son derece önemli ve bir o kadar da savunmasız bir potansiyele sahip olduğu ayrıca savunulmaktadır.[443]

Harold Laswell'in belirttiği üzere politika çalışması, nüfuz ve nüfuzu elde etmek için gerekenlerden en iyi şekilde yararlanan nüfuz sahiplerinin incelenmesi anlamına gelmektedir. Nüfuz, hiyerarşinin şekillendirdiği koşulların yani değerlerin göreceli olarak paylaşılmasıyla alakalıdır ve farklı değerler kullanılarak farklı sonuçlar elde edilebilir. Nüfuzun değerlerin göreceli paylaşılmasından farklı terimlerle tanımlanmasıyla da yeni sonuçlar elde edilebilmekte ya da değerlerle ilgili çelişkiler söz konusuysa değerlerin nasıl etkilenebileceğine dair bir yargıyı belirtmek için de kullanılabilmektedir.[444] Politikanın her alandaki değerleri etkileme, şekillendirme ve kontrolüne yönelik ilgisi, siber uzay sahasının politika ile birleşimi sonrasında temel ilkeler üzerinden daha da güçlenerek tezahürlerinin genişlemesine vesile olmuştur. Siber alanın siyaset ve politik davranış üzerindeki tüm etkilerinin tanımlanması oldukça zor olmakla birlikte araştırmacılar tarafından birtakım yaklaşımlar ortaya konulmaya başlamıştır. Örneğin; 2000'lerin başında geliştirilen "Sanal Devlet" (*Virtual State*) kavramı, özü itibariyle teknoloji, bilgi ve sermaye gücünün toplanarak küresel etki kaynaklarına dönüştürülmesi fikrine dayanmaktadır. Bölgesel nüfuz, ticari ve askeri güç rekabetine dayanan geleneksel politika temellerinin sorgulanarak eğitim, beceri, bilim, teknoloji ve bilgi yönetimi gibi yeni parametrelerle değişmekte ve bilgiye yapılan yatırımları ulusal güç ve sosyal etkinliğin kaynağına dönüştürmektedir.[445] Bu bağlamda "siber alanların kullanımının imkân sağladığı eylemler ile kimlerin neyi, ne zaman ve nasıl elde ettiğini belirleyen insan etkileşimlerinin birleşimi" olarak tanımlanan "Siberpolitik" (*Cyberpolitics*), dünya çapında etkiler yaratmış ve yeni çıkarların, yeni Uluslararası İlişkiler kalıplarının ve küresel uyum ile kurumsal tepkilerin yeni biçimlerinin ortaya çıkmasına yol açmıştır. Ayrıca alternatif dünya görüşleri ve politika pozisyonları

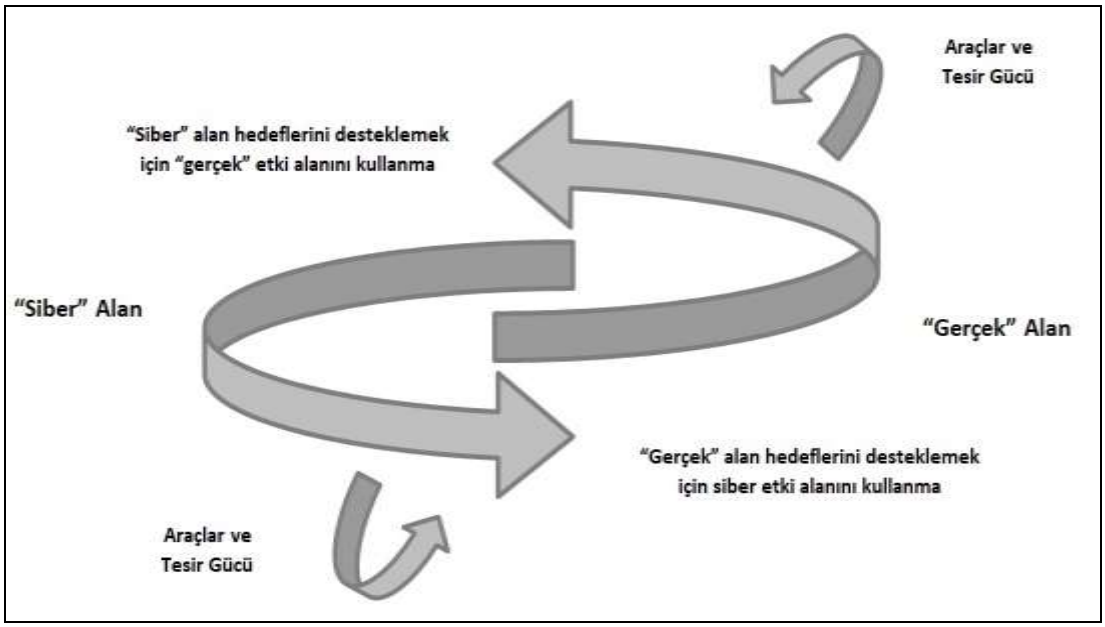
---

[443] Sabu Thomas, "'Cyber Protests and Electronic Disobedience': Examinig Non-Violence in Times of Cyber Politics", *Gandhi Marg*, Cilt 34, Sayı 3&4, Temmuz-Aralık 2012, s. 294.
[444] Harold D. Lasswell, *Politics: Who Gets What, When, How*, McGraw Hill, New York 1936, ss. 1-19.
[445] Richard N. Rosecrance, *The Rise of The Virtual State: Wealth and Power in the Coming Century*, 1. Basım, Basic Books, New York 1999, ss. 3-5.

üzerinde tartışmalara yol açan siberpolitik, değişen uluslararası güç ve nüfuz ortamının temel özelliklerini tespit edebilecek kadar yaygınlaşmaya başlamıştır.[446]

Siberpolitik içerisinde iki farklı süreç söz konusudur: Bir taraftan kinetik ya da geleneksel alandaki politikayı şekillendirmek için siber alan ya da çevrimiçi mekânlar kullanılırken, diğer taraftan ise siber uzay sahasının yapılandırılması için geleneksel enstrümanlar kullanılmaktadır. Tablo 24'te de görüldüğü üzere bu şekildeki ilişkiler, sanal olduğu kadar gerçek ve gerçek olduğu kadar da sanal olan çok çeşitli davranış ve davranış kalıplarını kapsamaktadır. Nazli Choucri'ye göre siberpolitiğin bu çift yönlü oluşum şekli, politikanın gerçek ve sanal alanlar arasındaki kapsayıcı etkileşimlerini ve ortak etkileşim alanı olarak siber uzay sahasındaki bağlantılar sayesinde gerçek ve sanal politikanın yaygınlığı ile söz konusu alanlardaki hedefler doğrultusunda çeşitli sanal alanların kullanımının yaygınlığını öne çıkarmaktadır.[447]

Tablo-24: Siberpolitiğin Tezahür Şekli



Kaynak: Nazli Choucri, *Cyberpolitics in International Relations*, The Massachusetts Institute of Technology Press, Massachusetts 2012, s. 12.

[446] Nazli Choucri, *a.g.e.*, s. 11.
[447] *A.g.e.*, s. 12.

Teknolojik değişim, bilgi ve iletişim altyapısının geliştirilmesi ve siber uzay sahasına yönelik uygulamaların çoğaltılması, siyaset teorisi alanındaki bağlantılarda yenilikçi kullanımları beraberinde getirmiş ve siberpolitik kapsamında sürdürülebilir kalkınma ve sürdürülebilirliğe yönelik ortaya çıkan stratejilerle ilgili küresel güç politikalarında bilgi teknolojileri uygulamalarını yeni bilgi üretim ve kullanım biçimi olarak öne çıkarmaktadır.[448] Bu nedenle siber uzay sahası, politik imalardan yoksun, yalıtılmış sanal ve teknik bir alan olarak düşünülmemelidir. Aksine; politika oluşturma, siyasi süreçler, seçimler ve devlet-toplum ilişkileri üzerinde belirleyici etkilere sahip etkili bir tartışma, çıkarların ve etkileşimin eklemlenmesi için yeni bir saha olarak tartışmalı bir şekilde önem kazanmış ve alışılagelmişin dışında farklı araçlarla siyaset için yeni bir mücadele alanı olarak ortaya çıkmıştır.[449]

21. yüzyılda İnternet, kitlelerden destek ve yetki alabilme süreçlerinde açıkça etkiye sahip pozisyona gelmiştir. Siyaseti etkileyen bu yeni iletişim ortamının en göze çarpan örneği olarak dünyanın en pahalı seçim politikalarının da yürütüldüğü ABD gösterilmekle birlikte İnternetin politik gerçekler üzerindeki derin etkileri başta Birleşik Krallık, Çin, Avustralya, Kanada, Estonya, Malezya olmak üzere çeşitli devletlerin iç siyasal süreçleri ile İnternet arasında gelişen bağdan kaynaklanan siyasi evrimler üzerinden tespit edilmektedir. E-devlet, e-seçim gibi uygulamaların hayata pratik olarak yansıtılması, sistem açıklarından kaynaklı iç ve dış sıkıntılar oluşabilmesi ya da çevrimiçi özgür konuşmaların sansürlenebilmesi adına ülke çaplarında güvenlik duvarlarının kurulmasının tercih edilmesi gibi örnekler, bütün dünyada siyasetin ve siyaset pratiğinin İnternet kaynaklı değişimler yaşadığını gözler önüne sermektedir. Bu bağlamda İnternet, Siyaset Bilimcilerin ve Uluslararası İlişkiler Uzmanlarının konularına yaklaşma, inceleme ve analiz etme biçimlerini değiştirmektedir. Öyle ki 21. yüzyılın Siyaset Bilimcileri ve Uluslararası İlişkiler Uzmanları, bir dizüstü bilgisayar ve İnternet bağlantısıyla dünyanın her yerinden

[448] Nazli Choucri, "Introduction: CyberPolitics in International Relations", *International Political Science Review*, Cilt 21, Sayı 3, 2000, s. 245.
[449] Iole Fontana, "Disentangling the Cyber Politics – Cyber Security Nexus: The New Challenge of Global Politics", *Global Affairs*, Cilt 3, Sayı 1, 2017, ss. 1-2.

saniyeler içerisinde birbirleriyle iletişim kurabilmekte ve tarihin hemen hemen her döneminden hemen hemen her konuda bilimsel çalışmalara erişebilmektedirler.[450]

Diğer taraftan siber uzay sahasının genişlemesiyle birlikte politika, medya ve kültür arasındaki ayrım giderek bulanıklaşmaktadır. Siberpolitikte bireysel aktörler, siber alanda itaatkâr vatandaş özneleri olmayı çok sayıda pratik üzerinden kendi kendilerine gerçekleştirebilmekte ve farklı politik konuları mümkün kılarak kendilerini eleştirilerin özneleri haline getirebilmektedirler. Bu noktada siberpolitik, "yeni medya" (*new media*) teknolojisi tarafından doğrudan belirlenmemekle birlikte sürekli etki yaratabilmek için sosyal ve kolektif olarak "yeni medya"nın uygulanması gerekliliğine dayanmaktadır.[451] Yeni medya, insani ve insan dışı doğa anlayışlarının çevrimiçi ortamda nasıl etkilendiğini ve dönüştüğünü göstermektedir. "Web 2.0" olarak adlandırılan *Wikipedia, YouTube* vb. uygulamalar ve teknolojiler ile "sosyal medya" olarak adlandırılan *Facebook, Twitter* vb. platformların birleşimini ifade eden "yeni medya", bireysel aktörlerin siber uzay alanı içerisinde çevrimiçi içerik oluşturmasına, derecelendirmesine, değişiklik yapabilmesine ve paylaşımda bulunabilmesine olanak tanımaktadır. Dolayısıyla yeni medya, İnternet kullanıcılarının en azından olası eylem sınırları dâhilinde ürettikleri veya tükettikleri çevrimiçi faaliyetleri, hizmetleri, alanları ve bilgileri birlikte yaratabilmelerini sağlamaktadır. Bundan dolayı yeni medya, insanların doğayı nasıl gördükleri, hayal ettikleri ve anladıkları dâhil olmak üzere birçok sorunu ve dinamiği çok boyutlu olarak derinlemesine etkilemekte ve değiştirmektedir.[452] İnternetin giderek daha fazla multimedya içermesi; görüntülerin, seslerin, videoların ve diğer kültürel formların yayılmasına olanak sağlamaktadır. Dahası, bilgisayar teknolojisi ve ağlarının kullanımı –tıpkı radyo ve televizyon medyasının onlarca yıl önce olduğu gibi– siyasetin normal ve olağan bir yönü haline evrilmektedir. Bununla birlikte ise siberpolitik için bilgisayar ve İnternet aracılı teknolojinin kullanılması, ana akım medyadan dışlanan sesler ve gruplar için yeni siyasi mücadele alanları açmakta ve

---

[450] Dylan Kissane, "Revolution in Political Affairs", *Central European University Political Science Journal*, Cilt 5, Sayı 4, Aralık 2010, ss. 487-488.
[451] Shih-Diing Liu, "The Cyberpolitics of The Governed", *Inter-Asia Cultural Studies*, Cilt 14, Sayı 2, 2013, s. 268.
[452] Bram Büscher, Stasja Koot & Ingrid L. Nelson, "Introduction. Nature 2.0: New Media, Online Activism and The Cyberpolitics of Environmental Conservation", *Geoforum*, Cilt 79, Sayı 100, 2017, s. 111.

böylece muhalefet gruplarının müdahale potansiyelini genişleterek demokratikleşme kapsamını da potansiyel olarak genişletmektedir.[453] Bu anlamda siberpolitik, yeni teknolojilere göre politikayı yeniden gözden geçiren ve özellikle İnternetin gelişmesine ve etkilerine odaklanan yepyeni bir paradigma olarak iletişimi kilit unsur haline getirmektedir. Siberpolitiğin yapılanma ekseninin merkezi problemini kamusal alan ve güç sorununun kesişim noktasına inşa edilmesi oluşturmaktadır. Hız sorunu ile siyasi zamansallık ve çağdaş teknolojilerin yakınlığı arasındaki yetersizlik, politik görünürlüğü teknolojik arabuluculuk formlarına mecbur kılmaktadır. Bundan dolayı teknik yaklaşım ve yeni medya, 21. yüzyılın politik kavramsal başlangıcının merkezi karakterleri olarak kabul edilmekte ve siberpolitiğin analiz araçları ve çoklu perspektifler şeklindeki güçlü ifadesiyle yeni bir sosyallik biçimine yol açmaktadır.[454]

3.2. Dijital Diplomasi / Siber Diplomasi

"Diplomasi" (*Diplomacy*) kavramının çeşitli anlamları bulunmakla birlikte genel olarak anlaşılabilmesi açısından öne çıkan iki yaklaşım söz konusudur: Makro perspektiften bakıldığında diplomasi, uluslararası sistemin işleyişinin merkezinde bulunan ve anlaşmazlıkların diyalog ve müzakere yoluyla çözümlenmesine vesile olan bir iletişim sürecini ifade etmektedir. Mikro perspektiften bakıldığında ise diplomasi, bir dış politika aracı veya devletlerin ve uluslararası aktörlerin kendi işleyişlerinde yürüttüğü bir temsil, iletişim ve müzakere mekanizması olarak anlaşılmaktadır.[455] I. Dünya Savaşı öncesindeki geleneksel diplomasinin yapısı son derece kişisel, resmi, yavaş ve genellikle gizlilikle korunmaktayken, I. Dünya Savaşı sonrası ortaya çıkan "yeni diplomasi", öncelikli olarak diplomatik süreçlerin medyaya ve kamuya açıklanmasıyla ilgili olmuştur. 1918'de ABD Başkanı Woodrow Wilson tarafından I. Dünya Savaşı'nın en önemli nedeni olarak gösterilen

---

[453] Douglas Kellner, "Globalisation, Technopolitics and Revolution", *Theoria: A Journal of Social and Political Theory*, Cilt 48, Sayı 98, Aralık 2001, s. 16.

[454] Constantino Pereira Martins, "What is Cyberpolitics?", Nova University of Lisbon, Lizbon Aralık 2013, *https://www.academia.edu/7554424/What_is_Cyberpoliticsi*, (Erişim Tarihi: 12 Mart 2020), ss. 8-11.

[455] Beata Surmacz, "New Technologies in Diplomacy", Editörler: Monika Szkarlat & Katarzyna Mojska, *New Technologies as a Factor of International Relations*, Cambridge Scholars Publishing, 1. Basım, Newcastle upon Tyne 2016, s. 74.

geleneksel gizli diplomasinin medyaya ve kamuoyuna maruz kalmasıyla "yeni" formuna evrilmesi, dış politikanın oluşturulması ve diplomasinin yürütülmesinde çok büyük etkiye sahip olmuştur. Söz konusu bu dramatik değişim, öncelikle siyaset, uluslararası ilişkiler ve kitle iletişimindeki birbiriyle bağlantılı devrimsel değişikliklerin neticesinde gerçekleşmiştir.[456] II. Dünya Savaşı sürecinde ise ABD'nin Mihver Devletlerin propaganda saldırısına karşı deniz aşırı enformasyon programlarına birincil katılım göstermesi, modern elektronik diplomasinin başlangıcının önemli bir yönü olarak nitelendirilmiştir. Yurt içinde ve yurt dışında kamuoyunu etkilemek için radyo ve televizyon yayıncılığı ile diğer teknolojilerin kullanılmaya başlanması ve giderek yayılması, günümüzde "kamu diplomasisi" (*public diplomacy*) olarak adlandırılan kamusal iletişim süreci ve politikasının oluşmasını hızlandırmıştır. 1930'ların sonlarında ABD'nin küçük ölçekte başlayan faaliyetleri, 1945 sonrasında ABD'yi o zamana kadar görülen en büyük küresel bilgi kaynakları ağından sorumlu noktaya getirmiştir.[457] Soğuk Savaş döneminde ilerleyen teknolojik gelişmeler ışığında gündelik hayatın parçası haline gelen kitle iletişim teknolojileri, kamu diplomasisi ofislerini, programlarını ve politikalarını yaygın hale getirmiştir. Soğuk Savaş'ın sona ermesinden bu yana ise hükümetlerin dış politika hedeflerini gerçekleştirmek için bilgiyi kullanma biçimleri değişmiştir. Dijital bilgi ve iletişim teknolojileri devrimi ile birlikte kamu diplomasisinde yaşanan büyüme, "dijital diplomasinin" (*digital diplomacy*) veya "siber diplomasinin" (*cyber diplomacy*) ortaya çıkması için ideal koşulları yaratmıştır.[458]

Bu bağlamda "dijital diplomasi/siber diplomasi"; siber uzay sahasıyla ilgili ulusal çıkarları güvence altına almak için diplomatik kaynakların kullanılması ve diplomatik işlevlerin yerine getirilmesi olarak tanımlanmaktadır. Genellikle diplomatik gündeme yönelik referanslar içeren ulusal siber güvenlik stratejilerinde bu tür menfaatler tanımlanmaktadır. Dijital diplomasi gündeminin baskın konuları

---

[456] Eytan Gilboa, "Real-Time Diplomacy: Myth and Reality", Editör: Evan H. Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, McGill-Quenn's University Press, Londra 2002, s. 84.

[457] Wilson Dizard, Jr., *Digital Diplomacy: U.S. Foreign Policy in the Information Age*, 1. Basım, Praeger Publishers, Connecticut 2001, ss. 21-22.

[458] Stuart Murray, "Evolution, Not Revolution: The Digital Divide in American and Australian Contexts", Editörler: Corneliu Bjola & Marcus Holmes, *Digital Diplomacy: Theory and Practice*, 1. Basım, Routledge, New York 2015, s. 130.

arasında çoğunlukla siber güvenlik, siber suç, siber alanda güven inşası, İnternet özgürlüğü ve İnternet yönetişimi gibi hususların olduğu tespit edilmiştir.[459] Bilgi ve iletişim teknolojileriyle birlikte diğer elektronik araçların diplomatik enformasyon, iletişim, temsil, müzakere vb. diplomatik faaliyetlerde uygulanmasından kaynaklanan bu yeni diplomasi türünde geleneksel diplomasi anlayışı hâkim olmakla birlikte biçim ve stratejilerde değişim söz konusudur. Bu değişim doğrultusunda da geleneksel diplomatik çabaların güçlendirilmesi, teknoloji temelli politika çözümlerinin geliştirilmesi ve siber aktivizmin teşvik edilmesi sağlanmaktadır.[460]

Öte taraftan, Corneliu Bjola'ya göre dışişleri bakanlıklarındaki dijital girişimlerin diplomasi pratiğinde bir devrim şeklinde yayılması, diplomatik teorideki değişim yönetimi açığı açısından mükemmel bir fırsat olarak görülmelidir; çünkü dijital teknolojiler, firmalardan bireylere ve hatta devletlere kadar işlerin yönetim biçimlerini çoktan değiştirmiştir. Hükümetler ve uluslararası kuruluşlar artık sosyal medyanın uluslararası ilişkilerin nasıl izlenebileceği konusunda potansiyel bir oyun değiştirici olduğunun farkına varmaktadırlar.[461] Temelde diplomatik misyonun dijitalleştirilmesi, İnternet aracılığıyla hizmet veren diplomatik misyonların artması nedeniyle hizmetleri rekabetçi kılmaktadır. Bu noktada dijital iletişim teknolojileri, devletlerin zorluklarını ve diplomatik çıkarlarını karşılayan dış politika oluşturma mekanizmalarına girerek ülkelerin katılımını arttırma potansiyeline sahiptir. Diplomasi, dijital teknoloji tarafından sağlanan uluslararası etkileşimi gösteren elektronik girdi ve çıktıların tümünü kapsamakta ve uluslararası etkileşimlerde İnternet odaklı teknolojinin her yerde bulunmasını doğrulamaktadır.[462] Diğer taraftan ise dijital teknolojinin uluslararası sistemdeki güç dengesini hiyerarşik devlet tabanlı yapılardan merkezi olmayan ağlara kaydırdığı gerçeği, diplomasinin dijital alanda varoluşsal bir sorunla karşı karşıya olabileceği gerçeğini de akıllara getirmektedir. Bunun nedeni olarak ise, dijital teknolojilerin hem küresel sistem içerisinde yeni bir

---

[459] André Barrinha & Thomas Renard, "Cyber-Diplomacy: The Making of an International Society in the Digital Age", *Global Affairs*, Cilt 3, Sayı 4-5, 2017, s. 355.
[460] Jesse Lichtenstein, "Digital Diplomacy", The New York Times Magazine, 16 Temmuz 2010, *https://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html*, (Erişim Tarihi: 14 Mart 2020).
[461] Corneliu Bjola, "Introduction: Making Sense of Digital Diplomacy", Editörler: Corneliu Bjola & Marcus Holmes, *Digital Diplomacy: Theory and Practice*, 1. Basım, Routledge, New York 2015, s. 4.
[462] Eugene N. Nweke, "Diplomacy in Era of Digital Governance: Theory and Impact", *Information and Knowledge Management*, Cilt 2, Sayı 3, 2012, ss. 23-24.

aktör katmanını güçlendirmesi hem de mevcut kurumları, oluşumları ve devletleri tehdit etmesi gösterilmektedir. Dolayısıyla dijital diplomasi, devletlerin diğer devletleri etkilemeye çalıştığı araç setine yeni bir eklenti olarak tanımlanabildiği gibi, daha radikal perspektiften bakıldığında da devletlerden ziyade dijital aktörleri etkilemeye yönelik diplomasi hedeflerinin stratejik bir uzantısı olarak da yorumlanabilmektedir.[463]

Bireysel diplomatlar ile dijital teknoloji arasında kurulan ilişkinin, öncüllerinin telefon, daktilo, telgraf, radyo, televizyon ve ilk bilgisayarlar ile olan ilişkilerinden daha farklı düşünülmesi gerekmektedir. 21. yüzyılın en büyük inovasyonlarından biri olarak nitelendirilen sosyal medyanın ortaya çıkışıyla – *Friendster* (2002); *LinkedIn* (2003); *Myspace* (2003); *Facebook* (2004); *YouTube* (2005); *Reddit* (2005); *Twitter* (2006); *WhatsApp* (2009); *Instagram* (2010); *Pinterest* (2010); *Snapchat* (2011); *Google+* (2011)[464]– birlikte diplomasi ve teknoloji arasındaki ilişkide tamamen yeni dinamikler söz konusu olmuş ve etki boyutu çok fazla genişlemiştir.[465] Öyle ki, geçmiş yıllarda dışişleri bakanları tarafından sosyal medya platformlarının potansiyelinin daha fazla dış politika alanında kullanılabilmesi adına büyük yatırımlar söz konusu olmuştur. Dijital aktörler tarafından tasarlanmış karmaşık bir dizi aracın, hükümetler ve diplomatik aktörlerce diğer aktörlerle etkileşimde bulunmak ve sosyal, politik ve ekonomik alanlardaki çıkarlarıyla sistematik hale getirebilmek için nasıl başarılı şekilde kullanılabileceği yönünden alternatif arayışlarda bulunulmuştur.[466] Sosyal medyanın bu hızlı gelişimi ve yaygınlaşması, diplomatik iletişimde birbiriyle ilişkili değişimler dizisi üretmiştir. Özellikle 2010 yılında başlayan Arap Baharı sürecinde sosyal medyanın sivil halk hareketlerinde oynamış olduğu stratejik rol, coğrafi ve politik

---

[463] Corneliu Bjola, "Digital Diplomacy – The State of the Art", *Global Affairs*, Cilt 2, Sayı 3, 2016, s. 298.

[464] Christopher McFadden, "A Chronological History of Social Media", Interesting Engineering, 16 Ekim 2018, *https://interestingengineering.com/a-chronological-history-of-social-media*, (Erişim Tarihi: 15 Mart 2020).; Zenesys, "Social Media Evolution", 24 Haziran 2019, *https://www.zenesys.com/infographics/social-media-evolution*, (Erişim Tarihi: 15 Mart 2020).; Phrasee, "The History of Social Media: A Timeline", *https://phrasee.co/the-history-of-social-media-a-timeline/*, (Erişim Tarihi: 15 Mart 2020).

[465] Martin Lister, Jon Dovey, Seth Giddings, Iain Grant & Kieran Kelly, *New Media: A Critical Introduction*, 2. Basım, Routledge, New York 2009, s. 175.

[466] Jan Melissen & Emilie V. De Keulenaar, "Critical Digital Diplomacy as a Global Challenge: The South Korean Experience", *Global Policy*, Cilt 8, Sayı 3, Eylül 2017, s. 298.

kısıtlamaların ötesindeki uzak kitle ile bilgi paylaşım imkânı sağlaması gibi çeşitli tecrübeler, dijital teknoloji ve sosyal medya platformlarının diplomasi açısından son derece verimli bir araç olarak kullanılabileceğini göstermiştir.[467] Özellikle *Twitter*, *Facebook* ve *YouTube* gibi sosyal medya platformları, kamu diplomasisinin hedeflerini kökten değiştirmemekte, aksine onu dijital diplomasinin bileşeni haline getirerek gelişen bilgi ortamındaki kitlelerle etkileşimi kolaylaştırmak için yeni araçlar sunmaktadır. Bu açıdan dijital diplomasi literatürü, sosyal medyanın verimli ve etkili kullanımının, ülkelerin göstereceği katılım ve diyalog yoluyla olumlu imaj oluşturmalarına yardımcı olabileceğini düşündürmektedir.[468] Sosyal medya, "sosyal" kelimesinin iki yönlü iletişim ve konuşma imasına dayandığı için çok sayıda politikacı ve diplomat tarafından içinde yer alınması gereken bir kanal olarak görülmektedir. Sosyal medya konuşmalarında kullanılan bir *hashtag* (#), gazete gibi geçmişin sona eren paradigmalarının yayınlama araçlarının aksine, politik söylemde devam eden ve sona ermeyen medya konuşmalarına işaret etmektedir. Bu durumda yayıncılık, zaman içerisinde gelişen ve asla sona ermeyen akıcı bir faaliyete dönüşmektedir.[469] Dolayısıyla sosyal medya, sadece bilgi yayma amaçlı bir platformunun çok ötesine geçerek halkın ne düşündüğünün daha hızlı dinlenebilmesini sağlamakta ve iki yönlü iletişime katılarak uzun vadede kamu diplomasisinin etkilerini en üst düzeye çıkarmanın anahtar unsuru olarak göz önünde bulundurulmalıdır. Hedef kitle ile sosyal medya aracılığıyla ilişki kurulması, geleneksel diplomasinin sınırlarının aşılmasının bir yoludur ve ülkeler ile halk arasındaki karşılıklı anlayışı yükseltmekte ve ortak çıkarları arttırmaktadır.[470]

Dijital diplomasi, günümüzde artık bir dış politika şartı haline gelmiştir. Öyle ki devletler, devlet dışı aktörler ve bireyler, aynı çevrimiçi alanda güç ve nüfuz için rekabet etmektedirler. Düzgün ve efektif kullanılması halinde dijital diplomasi,

---

[467] Neil Collins & Kristina Bekenova, "Digital Diplomacy: Success at Your Fingerprint", *Place Branding and Public Diplomacy,* Cilt 15, Sayı 1, Mart 2019, s. 2.

[468] Muhammed Ittefaq, "Digital Diplomacy via Social Networks: A Cross-National Analysis of Governmental Usage of Facebook and Twitter for Digital Engagement", *Journal of Contemporary Eastern Asia*, Cilt 18, Sayı 1, Yaz 2019, s. 50.

[469] Andreas Sandre, *Digital Diplomacy: Conversations on Innovation in Foreign Policy*, The Rowman & Littlefield Publishing, Maryland 2015, ss. 104-105.

[470] Sejung Park, Dahoon Chung & Han Woo Park, "Analytical Framework for Evaluating Digital Diplomacy Using Network Analysis and Topic Modeling: Comparing South Korea and Japan", *Information* Processing *and Management*, Cilt 56, Sayı 4, 2019, s. 1469.

ülkelerin dış politika hedeflerini ilerletmesine ve uluslararası erişimlerini genişletmesine yardımcı olabilecek önemli bir tamamlayıcıdır. Sosyal medyanın dünyanın her yerindeki insanlarla gerçek zamanlı etkileşim kurabilme fırsatı ve artan katılım, diplomasinin amaçlarını ilerletebilme alanları sağlamaktadır. Ek olarak sosyal medyanın erişilebilme kolaylığı ve diğer yöntemlere kıyasla düşük maliyeti, mevcut kamu diplomasisi çabalarının ana hedefi olan genç nüfusa ulaşmada kilit kanal olmaktadır. Öte taraftan dijital teknolojiler, özellikle bilgi toplama ve işleme, konsolosluk faaliyetleri, acil durumlar ve felaketler sırasındaki iletişim hususlarında kamu diplomasisine son derece faydalı olabilmektedirler.[471]

Diğer yandan ise söz konusu gelişmelerin diplomatların uluslararası olaylarla ilgili bilgi ortamını yönetme kabiliyetini erozyona uğrama riski de bulunmaktadır. Web, özel casus uyduları, kötü amaçlı bilgisayar yazılımları, gazeteciler ile diğer sivil toplum kuruluşları tarafından kullanılan ileri teknoloji mobil iletişim cihazları, elçiliklerin, istihbarat kurumlarının ve gözetim teknolojilerinin ağına meydan okumaktadırlar. Özellikle krizler esnasında ileri teknolojiler kullanan haber kuruluşları ile sosyal medya paydaşları, hükümet kanallarını ve kaynaklarını kullanan diplomatlar ile hemen hemen aynı bilgi seviyelerine sahip olmaktadır. Bu gibi durumlarda yetkililerin politika gündemleri ve olayların kamusal yansımaları üzerinde kontrol sahibi olma yetenekleri giderek azalmaktadır. Öyle ki "CNN Etkisi" (*CNN Effect*) olarak da adlandırılan ve 1990'ların başından bu yana yetkililerin haber medyası üzerindeki politika kontrolünün potansiyel kaybını ifade eden bu terim, artık devam eden olayların bilgisi ve analizi için yetkililere olan bağlılığın kırılması sonucu ortaya çıkmıştır. Dolayısıyla diplomatların hem kendi ülkelerinde hem de dünya sahnesindeki bilgi ve enformasyona erişimlerinden doğan otorite pozisyonu kaybolmaktadır.[472]

Netice olarak dijital diplomasinin klasik diplomasinin yerini almak yerine, doğru şekilde uygulanması halinde devletlerin Uluslararası İlişkiler ve dış polikadaki çalışmalarını daha hızlı ve düşük maliyetle güçlendirebilecek stratejik bir araç olarak

---

[471] Olubukola S. Adesina, "Foreign Policy in An Era of Digital Diplomacy", *Cogent Social Sciences*, Cilt 3, Sayı 1, 2017, s. 10.

[472] Steven Livingston, "The New Media and Transparency: What Are the Consequences for Diplomacy?", Editör: Evan H. Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, McGill-Quenn's University Press, Londra 2002, ss. 110-111.

düşünülmesinde fayda vardır.[473] Dijital diplomasi, geleneksel diplomasinin fiziksel varlığını tamamlayıcı ve genişletici olmakla birlikte diplomatların azalan klasik nüfuz imajlarını, barındırdığı ve sunduğu yeni fırsatlarla tam tersine çevirebilir.[474] Ayrıca diplomatların geleneksel görevlerinin ötesinde *Google, Facebook* vb. İnternet şirketlerinin liderleri, teknoloji girişimcileri veya sivil toplum kuruluşları gibi devlet dışı aktörlerle etkileşimlerde bulunabilmektedirler. Hatta teknoloji yoluyla diplomasi, diğer ülkelerde zorluk yaşayan ötekilerin seslerinin güçlendirilmesine katkı sağlayabilir konuma evrilmiştir.[475]

3.3. Siber Güç

Güç, daha önce de belirtildiği üzere, kapsam ve etki alanları açısından bakıldığında çok boyutlu bir kavramdır. Gücün kapsamı, içerdiği hedefler ve etkilenen sorun alanları üzerinden anlaşılmaktadır. Gücün etki alanı ise gücün potansiyel etkinliği ile ilgili olan ağırlık, oluşturduğu etki değerleri olarak maliyet ve etki yaratma enstrümanı olarak araçsal boyutlardan oluşmaktadır.[476] Bu bağlamda siber teknoloji, aktörlerin çıkarlarını gözetmeleri için yeni, düşük maliyetli ve ağırlıklı araçlar sağlamaktadır; ancak uzun yıllar süren çabalara ve milyarlarca dolar yatırım yapılan geliştirilmiş teknolojilere rağmen "siber güç" konsepti hala anlaşılması zor bir çerçevededir.[477] 21. yüzyılda siber uzay sahasının insan etkileşimi için yepyeni alan haline gelmesi, onu gücün geçiş ve yayılma analizlerinin ayrılmaz bir parçası haline getirmiştir. Teknolojinin karma karakteri, fiziksel cihazlar üzerinden konumlandırılan ulusötesi sanal bir yapıdan oluşmaktadır. Diğer stratejik alanlardan –kara, deniz, hava ve dış uzay– farklı olarak siber uzay sahasının yapay ve değiştirilebilir niteliği, siber gücün kapsam ve etki alanlarının her geçen gün giderek genişlemesine ve derinleşmesine vesile olmaktadır.[478] Bu bağlamda "siber güç" (*cyber power*) kavramı çok farklı boyutlarda ve farklı perspektiflerde çeşitli

[473] Olubukola S. Adesina, *a.g.m.*, s. 11.
[474] Ilan Manor & James Pamment, "Towards Prestige Mobility? Diplomatic Prestige and Digital Diplomacy", *Cambridge Review of International Affairs*, Cilt 32, Sayı 2, 2019, s. 95.
[475] André Barrinha & Thomas Renard, *a.g.m.*, s. 355.
[476] Jelle van Haaster, "Assessing Cyber Power", *8th International Conference on Cyber Conflict (CyCon)*, IEEE, 2016, s. 11.
[477] Lior Tabansky, "Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy", *8th International Conference on Cyber Conflict (CyCon)*, IEEE, 2016, s. 52.
[478] Hannes Ebert & Tim Maurer, *a.g.m.*, s. 1054.

şekillerde tanımlanabilmektedir: Joseph Nye'a göre siber güç; "*siber alanın elektronik olarak birbirine bağlı bilgi kaynaklarını kullanarak tercih edilen sonuçları davranışsal olarak elde etme yeteneği*" şeklinde tanımlanmaktadır. Bu nedenle siber güç, siber alan içerisinde tercih edilen sonuçları üretmek için kullanılabileceği gibi siber alan dışındaki diğer alanlarda da tercih edilen sonuçları yaratmak için de kullanılabilir.[479] Benzer şekilde Daniel T. Kuehl tarafından da siber güç, tüm operasyonel ortamlarda ve güç enstrümanları arasında avantajlar yaratmak ve olayları etkilemek için siber uzay sahasının kullanılması yeteneği olarak tanımlanmaktadır. Ona göre siber uzay sahası karmaşık bir ortamdır ve siber güç ise daima bu ortamı kullanma yeteneğinin bir ölçüsüdür. Bu doğrultuda teknoloji bariz bir faktördür; çünkü siber uzay alanına girme yeteneği, onu kullanmayı mümkün kılan şeydir ve söz konusu teknoloji sürekli değişirken, çeşitli kullanıcılar –devletler, toplumlar, devlet dışı aktörler– tarafından yeni teknolojilerin kullanılabilmesi için eski teknolojilerin üzerine yapılandırılırlar.[480] John B. Sheldon ise siber gücü, siber alan içerisinde ve dışarısında gerçekleşen siber operasyonların yarattığı stratejik etkilerin toplamı olarak tanımlamakta ve stratejik ortamı manipüle etme yeteneğinden kaynaklandığını vurgulamaktadır. Bu sebeple politikalara göre sürekli avantaj için genel durumun iyi yönetilmesi, siber gücün etkilerinin politika hedeflerine dönüştürülmesini gerekli kılmaktadır.[481] Dolayısıyla da siber gücün tam olarak anlaşılabilmesi adına siber güç ile siber uzayın karmaşık karakterinin kabul edilmesi gerekmektedir.

Siber güç –tıpkı siber savaşta olduğu gibi– siyasi, sosyal, askeri ve ekonomik güç dengesi sorunlarına bilinçli olarak uygulanabilmenin henüz başlangıç aşamalarında kabul edilmektedir. Buna karşın kümülatif etkilerinin, siber alanın büyük aktörlerinin yeteneklerinde nispeten iyi dengelenmesine bağlı olarak ılımlı olabileceği öngörülmektedir. Stratejik bir mesele olarak bakıldığında –örneğin; Arap Baharı sürecindeki ayaklanmalarda ve değişimlerde– iletişimin iyileştirilmesi yerine ana etkilerin yalnızca siber güç özelliklerinden çıkarılabilir hale evrildiği

[479] Joseph S. Nye, Jr., *a.g.e.*, ss. 3-4.
[480] Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", Editörler: Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz, *Cyberpower and National Security*, 1. Basım, National Defense University Press & Potomac Books, Virginia 2009, s. 38.
[481] John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War", *Strategic Studies Quarterly*, Cilt 5, Sayı 2, Yaz 2011, ss. 95-96.

görülmektedir.[482] Bu bağlamda aktörlerin siber güç durumuna ulaşabilmelerini ve pozisyonlarını koruyabilmeleri adına birbiriyle bağlantılı dört özellik öne çıkmaktadır:(1) Uygulanabilirlik, (2) Süreklilik/Devamlılık, (3) Dirençlilik/Esneklik, ve (4) Karşılıklı bağımlılık. Buna göre bir siber varlık, mevcutsa ve işleyebiliyorsa uygulanabilmektedir. Spesifik olarak ise siber gücün tüm bileşenlerine ve gücün dört boyutuna –diplomatik, bilgilendirici, askeri ve ekonomik– etki göstermelidir. Diğer taraftan, fiziksel dünyada bir varlığın tüm izlerinin silinmesi zor olmakla birlikte siber alanın değişken doğası dikkate alındığında varlığın sürekliliği oldukça zor olabilmektedir. Çeşitli saldırılarla siber varlıkların çalışması engellenebilir, altyapısı zarar görebilir ya da yazılımları ve verileri dijital ortamlarda silinebilir. Bu nedenle siber gücün uygulanabilirliği yanında sürekliliği de esastır. Üçüncü özellik olan direnç gösterme ya da esneklik ile siber alanın dinamik ve kararsız boyutu vurgulanmaktadır. Buna göre pek çok faktörden –teknolojinin karmaşıklığı, bağlanabilirliği ve yakınsaması, insan kaynaklı hatalar ve tehditler, doğal afetler, kazalar, elektrik kesintileri vb.– dolayı koşullarda doğabilecek değişikliklere direnme, soğurma, iyileşme veya başarılı bir şekilde adapte olma yeteneği bulunmalıdır. Son özellik olan karşılıklı bağımlılık ise siber uzay sahasının dağınık doğası ve bu alandaki varlıkların simbiyotik ilişkisine dayanmakta ve özellikle ekonomik, diplomatik ve askeri ilişkilerdeki güç denkleminde daha da önemli bir özellik haline gelmektedir.[483]

İlk aşama siber güç yaklaşımlarında devletlerin stratejik çıkarlarıyla birlikte merkezde yer aldığı ve yukarıdan aşağı doğru yapılan teori yapılandırmalarında siber stratejiler ya da ulusal siber güvenlik stratejileri gibi ek kaynaklarla desteklendiği görülmektedir. Dolayısıyla bu bakış açısının tüm öğelerinde devlet dışı aktörler birer pasif entelektüel sermaye olarak kabul edilmekte ve devletler ise siber gücünü nasıl optimize edeceğini en verimli şekilde öğrenmesi gereken siyasi varlıklar olarak konumlandırılmaktadırlar. Buna karşın, siber uzay sahasının dinamik yapısında yer alan hem devlet hem de devlet dışı aktörlerin fazlalığı, bu alanın sunduğu fırsatlardan

---

[482] Charles M. Preston, "The Information Revolution: The Emergence of Cyber Power", Editör: Thomas A. Johnson, Power, *National Security, and Transformational Global Events: Challenges Confronting America, China, and Iran*, CRC Press, Florida 2012, s. 330.

[483] Jill Rowland, Mason Rice & Sujeet Shenoi, "The Anatomy of A Cyber Power", *International Journal of Critical Infrastructure Protection*, Cilt 7, Sayı 1, Mart 2014, ss. 7-10.

yararlanmak için anlık siber güç uygulamalarına sebep olmaktadır. Bu nedenle klasik yaklaşımlardaki siber alanın devlet merkezli tam kontrol edilebilirlik hedefleri gerçekçilikten oldukça uzak kalmaktadır. İşte bu durum, geleneksel devlet gücü anlayışına veya güvenlik açıkları ile bunların sömürülmesine yönelik yeni ve güçlü meydan okumayı daha açık bir şekilde vurgulamaktadır.[484]

Uluslararası İlişkiler ve güvenlik konularındaki genel güç tartışmalarına bağlı olarak siber güç kullanımının basit bir araç olmanın çok ötesinde yer aldığına dair daha fazla spesifik kategorizasyonlar ve modellemeler gereklidir. Bu bağlamda Joseph Nye'ın siber alandaki gücün ilişkisel üç yüzünü veya yönlerini sert ve yumuşak güç davranışlarına göre öne çıkardığı modellemesi son derece dikkat çekicidir.[485]

Tablo-25: Siber Alanda Gücün Üç Yüzü

Birinci Yüz: (B'nin başlangıçta yapmayacağı şeyi yapmasına A sebep olur.)
Sert Güç: Hizmet Engelleme Saldırıları, Kötü Amaçlı Yazılımın Eklenmesi, SCADA Saldırıları, Blogcuların Tutuklanması
Yumuşak Güç: Bilgisayar korsanlarının ilk tercihlerini değiştirmek için bilgilendirme kampanyası, Terör örgüt üyelerinin işe alınması
İkinci Yüz: (Gündem kontrolü: A, B'nin stratejilerini hariç tutarak B'yi seçiminden alıkoyar.)
Sert Güç: Güvenlik Duvarları, Filtreler, Şirketlere çeşitli fikirleri dışlama baskısı
Yumuşak Güç: İnternet servis sağlayıcılar ile arama motorlarının self gözlemi, Alan adlarına yönelik ICANN kuralları, Geniş çaplı kabul görmüş yazılım standartları
Üçüncü Yüz: (A, B'nin tercihlerini şekillendirir ve böylece bazı stratejiler asla dikkate alınmaz.)
Sert Güç: Sansürlü materyal yayınlayan blogcuları cezalandırma tehdidi
Yumuşak Güç: Tercihler oluşturmak için bilgilendirme yapılması (örn. Milliyetçiliğin "vatansever bilgisayar korsanlarınca" teşvik edilmesi), Tepki normları geliştirilmesi

Kaynak: Joseph S. Nye, Jr., *Cyber Power*, Harvard Kennedy School, Belfer Center for Science and International Affairs, Report, Massachusetts Mayıs 2010, s. 7.

[484] Myriam Dunn Cavelty, "Europe's Cyber-Power", *European Politics and Society*, Cilt 19, Sayı 3, 2018, ss. 307-308.
[485] Joseph S. Nye, Jr., *a.g.e.*, s. 7.

Tablo 25'te görüldüğü üzere; siber alandaki gücün ilk yüzü, bir aktörün diğer aktörlere, ilk tercihlerine veya stratejilerine aykırı şekilde davranabilmelerini sağlamaktadır. Hizmet engelleme (*Denial of Service, DoS*) ve Dağıtılmış Hizmet Engelleme (*Distributed Denial of Service, DDoS*) saldırıları[486] ya da muhalif blog yazarlarının tutuklanması veya mesaj göndermelerinin bir şekilde engellenmesi[487] sert güce ilişkin örnekleri oluşturmaktadır. Bir kişi ya da oluşumun, başkalarının davranışlarını değiştirmeye ikna etme çabaları ise yumuşak güce ilişkin örneklerdir.[488] Siber alandaki gücün ikinci yüzü, bir aktörün diğerinin stratejilerini hariç tutarak seçimlerini engellediği gündem belirleme veya çerçeveleme sağlamaktadır. Buradaki etki, tartışma kapsamının sınırlanması veya çatışmaların ön plana çıkmasının engellenmesi için kullanılmaktadır. Bu durum diğerlerinin iradesine aykırı ise sert gücün örneği, meşru kabul edilirse yumuşak gücün örneği kabul edilmektedir.[489] Siber alandaki gücün üçüncü yüzü ise bir aktörün diğerinin ilk tercihlerini şekillendirmesini içermektedir ki böylece bazı stratejiler dikkate bile alınmamaktadır. Bu bağlamda belirli fikirlerin yetkisiz hale getirilmesi ve İnternete yayılmasının kısıtlanmasına yönelik aksiyonlar[490] sert güç örneğini oluştururken,

---

[486] Örnek için bkz.: BBC News, "DDoS: Man Who Sold Website Defences Pleads Guilty to Attacks", 21 Ocak 2020, *https://www.bbc.com/news/technology-51189386*, (Erişim Tarihi: 20 Mart 2020).

[487] Örnek için bkz.: The Guardian, "Chinese Human Rights Activist Liu Hiaobo Sentenced to 11 Years in Jail", 25 Aralık 2009, *https://www.theguardian.com/world/2009/dec/25/china-jails-liu-xiaobo*, (Erişim Tarihi: 20 Mart 2020).

[488] Çin hükümet yetkililerince Çinli öğrencilerin Japonya karşıtı gösteri yapmaları için İnternetin kullanılmasına dair örnek için bkz.: Jeffrey N. Wasserstrom, "Chinese Students and Anti-Japanese Protests, Past and Present", *World Policy Journal*, Cilt 22, Sayı 2, Yaz 2005, ss. 59-65.; El Kaide terör örgütünün İnterneti kullanarak insanları etkilediklerine dair örnek için bkz.: The New York Times, "Focus on Internet Imams as Al Qaueda Recruiters", 31 Aralık 2009, *https://www.nytimes.com/2010/01/01/us/01imam.html*, (Erişim Tarihi: 20 Mart 2020).

[489] 2010 yılındaki İran Devrimi yıldönümünde hükümetin protestocuların film vb. paylaşımlarını engellemek adına İnterneti yavaşlattığı yumuşak siber güç örneğine dair bkz.: The New York Times, "Iran Disrupts Internet Service Ahead of Protests", 10 Şubat 2010, *https://www.nytimes.com/2010/02/11/world/middleeast/11tehran.html*, (Erişim Tarihi: 21 Mart 2020).; 2009 yılında Çin'e bağlı Sincan Uygur Özerk Bölgesi'nde meydana gelen olaylar sonrasında çok sayıda web sitesinin kapatılmasına dair örnek için bkz.: Reuters, "China Tightens Web Screws After Xinjiang Riot", 6 Temmuz 2009, *https://www.reuters.com/article/us-china-xinjiang-internet/china-tightens-web-screws-after-xinjiang-riot-idUSTRE5651K420090706*, (Erişim Tarihi: 21 Mart 2020).

[490] İngiltere'nin İnternette kumar oynanmasını engellemek için kredi kartı kullanımına yönelik aldığı önlemler için bkz.: BBC News, "Gambling on Credit Cards to be Banned", 14 Ocak 2020, *https://www.bbc.com/news/business-51103006*, (Erişim Tarihi: 21 Mart 2020).; The Independent, "Online Gamblers will no Longer be Allowed to Use Credit Cards for Betting", 14 Ocak 2020, *https://www.independent.co.uk/news/uk/home-news/gambling-credit-cards-betting-ban-regulation-commission-deposits-a9282751.html*, (Erişim Tarihi: 21 Mart 2020).

bazı fikirlerin ve görsellerin –çocuk pornografisi gibi– kaldırılması ya da kısıtlanması hususunun geniş bir kültürel fikir birliğine dayanması yumuşak güç örneğini teşkil etmektedir. Dolayısıyla siber kaynaklar, siber alan içerisinde siber sert güç ve siber yumuşak güç üretebilmektedirler.[491] Öyle ki, sunulan örneklerden de anlaşılacağı üzere, siber alandaki işlemlerin her zaman bilgi tabanlı olması, bu alan içerisindeki sert ve yumuşak güç kavram ayrımını gerçek dünyaya kıyasla daha zorlaştırmaktadır. Özellikle siber alandaki yumuşak gücün söylem olarak sert güçten ayrı görünmek yerine onun farklı yollarla devamı ya da fiziksel olmayan ama yine de zorlayıcı bir güç biçimi şeklinde tezahürü gözlenebilmektedir.[492]

Son olarak David J. Betz ile Tim Stevens'a ait olan siber gücün daha yaygın ve dolaylı güç biçimlerine odaklanan dört boyutlu modeline değinmekte fayda görülmektedir: Betz ve Stevens'a göre siber güç, yeni veya farklı bir güç biçiminden ziyade gücün siber uzayda belirmesidir. Yerel koşullar yeni olaylar ve özellikler üretebilir ancak aynı genel ilkeler geçerlidir. Buna göre işlemleri siber uzay sahasında dört farklı siber güç biçimi olarak görülebilen dört temel güç formu söz konusudur: Zorlayıcı siber güç, Kurumsal siber güç, Yapısal siber güç ve Üretken siber güç.[493] Zorlayıcı siber güç, bir siber aktörün diğerlerinin var oluş koşullarını ve davranışlarını değiştirmek için doğrudan baskı kullanmasıdır. Siber uzay alanına erişimi olan herhangi bir aktör –aktivistler, bilgisayar korsanları, teröristler, devletler, özel firmalar, kamu şirketleri, askeri ittifaklar vb.– gerekli bilgi ve beceriye sahipse, varsayımsal olarak bir başkasına karşı zorlayıcı siber güç uygulayabilir.[494] İkinci olarak tanımlanan kurumsal siber güç, esas olarak resmi ve gayri resmi kurumların arabuluculuğu yoluyla bir siber aktörün diğeri tarafından dolaylı olarak kontrol edilmesi anlamına gelmektedir. Burada önemli olan husus, aracı olan kurumun belirli bir devletin tam kontrolü altında olmamasıdır.[495] Yapısal siber güç ise siber uzay yapısının doğrudan bağlı olduğu aktörlerin eylemlerini dolaylı olarak bağlı olduğu

[491] Joseph S. Nye, Jr., *a.g.e.*, ss. 7-9.
[492] Janice Bially Mattern, "Why 'Soft Power' Isn't So Soft: Representational Force and the Sociolinguistic Construction of Attraction in World Politcs", *Millennium: Journal of International Studies*, Cilt 33, Sayı 3, 2005, s. 583.
[493] David J. Betz & Tim Stevens, *Cyberspace and The State: Towards A Strategy For Cyber-Power*, 1. Basım, Routledge, New York 2011, ss. 44-45.
[494] *A.g.e.*, s. 45.
[495] *A.g.e.*, s. 47.

diğer aktörlere kıyasla nasıl kolaylaştırabileceği veya kısıtlayabileceğiyle ilgilidir.[496] Son siber güç biçimi olan üretken siber güç ise siber ortamda yürürlüğe giren ve siber ortamın aracılık ettiği söylem yoluyla sosyal konuların oluşturulması anlamına gelmektedir. Böylelikle sosyal eylemleri sınırlayan ya da kolaylaştıran olasılık anları tanımlanır.[497] Netice olarak yukarıda sunulan tüm siber güç tanımlamaları, kategorizasyonları ve modellemeleri göstermektedir ki; siber alanın dinamik, değişken, belirsiz ve karmaşık doğası, gücün çok yönlü yapısının en üst düzeyde yaşandığı bir ortam oluşturmaktadır. Bu noktada Uluslararası İlişkiler ve Siber Uluslararası İlişkiler aktörlerinin sahip oldukları siber gücün ne kadarına gerçekten sahip olduklarına dair yapılan kesin açıklamalar yanıltıcı olabilmektedir. Güç ve strateji tartışmalarında siber ortamın farklı yönlerine ve siber güç çeşitliliğine dair farkındalığın, olası hatalı öngörülerin minimize edilmesi açısından yardımcı olabileceği düşünülmektedir.

4. Siber Uzayda Hukukun ve İşbirliğinin Uygulanabilirliği

Devletler, bireylerin birbirleriyle doğal, sosyal ve siber alanlarda etkileştikleri ve birbirleri üzerinde hak talebinde bulunabildikleri çeşitli örgütsel varlıkları kapsamaktadırlar. Aynı zamanda uluslararası hukukta egemen olarak tanımlanan ve uluslararası forumlarda vatandaşları adına konuşmak için yetkilendirilen tek tüzel kişilik olarak öne çıkmaktadırlar. Bu bağlamda prensip olarak devletlerin birincil amaçları; uluslararası olarak tanınan geçirimsiz resmi sınırlar içerisinde kendi güvenliklerini sağlamak ve varlıklarını sürdürebilmektir. Buna karşın pratikte devletler, her zaman sınırlarını tam anlamıyla kontrol altına alamaz, egemenliklerini garanti edemez, hedeflerine her daim eksiksiz şekilde ulaşamaz, güç araçları üzerinde kontrolü her zaman kusursuz olarak sağlayamaz ve vatandaşlarının gözünde her zaman etkili birer kurum olarak hizmet edemezler. Uluslararası ekosistemde devletler hala birincil aktör olmalarına rağmen sayısı artan devlet dışı aktörler giderek bu yapıyı doldurmaktadırlar.[498] Siber uzay sahasının karmaşık ve dinamik doğası, bilgisayarların, ağların ve diğer bilgi teknolojilerinin niteliği, maliyeti ve

[496] *A.g.e.*, s. 48.
[497] *A.g.e.*, s. 50.
[498] Nazli Choucri, *a.g.e.*, s. 31.

kullanılabilirliği, bu alanda ağırlığı giderek artan devlet dışı aktörlere tıpkı devletlerin potansiyel kullanımlarına benzer şekilde operasyonel yürütme kapasiteleri sağlamaktadır. Bunun farkına varan devletler, bir taraftan ulusal stratejik, operasyonel ve taktik doktrinler geliştirirlerken, diğer yandan da uluslararası normlar ve kurallar oluşturulması için sürekli olarak çabalamakta ve uluslararası işbirlikleri gerçekleştirmektedirler.[499] Fakat beşinci stratejik alan olarak siber uzay, diğerlerine – kara, hava, deniz ve dış uzay– kıyasla tamamen yapay ve teknolojik hareketliliği yüksek bir saha olduğundan, yapılan her türlü düzenleme ve alınan her türlü önlem sürekli bir yetersizlik içindedir. Öyle ki, söz konusu dinamizm, oluşturulan uluslararası norm, yasa ve düzenlemeleri devamlı olarak hareketli hedefleri takip etmeye mecbur kılmaktadır. Dolayısıyla siber uzayın bu kusurlu yönetişimi, hiyerarşik kurallar yoluyla düzenlemeler uygulayan entegre kurumlar ile tanımlanabilir özü ve mevcut bağlantıları bulunmayan kurumlar arasındaki gevşek normlar ve oldukça dağınık uygulamalardan oluşan karmaşık bir rejim olarak kategorize edilebilmektedir.[500] Öte yandan uluslararası kurumsal girişimlerin ve küresel gündem oluşturmaya yönelik yeni eğilimlerin giderek büyümesiyle birlikte devletler ve devlet dışı aktörler arasında artan kurumsal bağlantılar gerçekleşmektedir. Böylelikle çeşitli devlet dışı aktörlerin uluslararası forumlara gözlemci ve benzeri pozisyonlarda katılımları söz konusu olmaya başlamakta ve dolayısıyla etki alanları genişleyerek meşru bir statüye ulaşmaktadırlar; ancak siber alanların uluslararası kurumlar aracılığıyla küresel hedefler doğrultusunda kullanılması, beraberinde sorunların ve zorlukların daha da genişlemesine vesile olmaktadır.[501] Bu noktada devletlerin ulusal ve dış politikalarında siber alanın kontrol düzeyi, uluslararası işbirliğini kolaylaştırma mekanizmaları, teknoloji ve İnternetin geleceği, uluslararası hukukun siber alanda uygulanması ve yeni yasal araçlarla desteklenmesi gibi temalar üzerinden geliştirilebilecek politikalar sayesinde uluslararası bir siber uzlaşma zemini söz konusu olabilir.[502] Devletlerin ve devlet dışı aktörlerin bu karmaşık sahada hem güç mücadelesinde bulundukları hem de işbirliği

[499] Duncan B. Hollis, "Why States Need an International Law for Information Operations", *Lewis & Clark Law Review*, Cilt 11, Sayı 4, 2007, s. 1033.
[500] Joseph S. Nye, Jr., *a.g.e.*, s. 15.
[501] Nazli Choucri & David D. Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma*, The Massachusetts Institute of Technology Press, Massachusetts 2018, s. 85.
[502] Chelsey Slack, *a.g.m.*, s. 73.

yaptıkları göz önünde bulundurulduğunda; geliştirilecek ilke, norm, kural, prosedür ve programlarla etkin siber uzay yönetişimi sağlanarak aktörler arasındaki gevşek bağlar sağlamlaştırılabilir; çünkü mevcut sorunlar ve aktörler arasındaki söz konusu zayıf bağlantı, bir taraftan aktörler arası işbirliğine ortam sağlarken, diğer taraftan da çeşitli anlaşmazlıkların öngörülemez boyutlara ulaşmasına neden olabilmektedir.[503] Bundan dolayı siber uzay sahasının uluslarası hukuk ve uluslararası işbirliği boyutlarıyla detaylandırılması yerinde olacaktır.

4.1. Uluslararası Hukuk ve Siber Uzay

Uluslararası hukukun yapısına bakıldığında, Uluslararası İlişkiler alanında faaliyet gösteren, kendi kendini sürdürebilen, tutarlı bir dizi kural olduğu ve olması gerektiği kabulünden hareketle çok devletli bir ortama bağlılık ve bu ortamın barış ve istikrarı için tasarlanmış kurallar görülmektedir. Uluslararası hukuk kuralları, devletler arasındaki sürtüşmeleri en aza indirerek, anlaşmazlıkların barışçıl çözümünü sağlamayı ve istikrarı hedeflemektedir. Uluslararası hukuk kurallarına rağmen savaş patlak verirse, savaşın kontrol altına alınması, savaşın neden olduğu zararın en aza indirilmesi ve savaş sonrası güvenli bir barış ortamının tesisi, yine uluslararası hukukun birincil hedeflerindendir.[504] Diğer taraftan siber uzay sahasının giderek bireysel, toplumsal ve küresel ilişkilere eklemlenmesi, söz konusu alanın katastrofik etkiler yaratmasına, önemli sonuçlar doğurabilecek potansiyel ve dinamik yapıya haiz olmasına neden olmaktadır. Böyle yapıya sahip karmaşık bir alanın, uluslararası hukuktan yoksun görülmesi mümkün değildir. Aksine, kötü niyetli devletlerden siber teröristlere, zararlı oluşumlardan bilgisayar korsanlarına kadar, geniş aktör çeşitliliğini içerisinde barındıran, küresel kritik altyapılardan ulusal siber ağlara kadar sonuçları son derece sarsıcı olabilecek çok boyutlu hedef noktalarını kapsayan yepyeni bir savaş boyutu olarak nitelendirilmektedir. Bu alanda gerçekleştirilebilecek her türlü yıkıcı operasyon, hükümet işlevlerinin bozulmasından

---

[503] Joseph S. Nye, Jr., "The Regime Complex for Managing Global Cyber Activities", *Global Commission on Internet Governance Paper Series*, Sayı 1, Mayıs 2014, s. 9.
[504] Anthony D'Amato, "International Law, Cybernetics, and Cyberspace", *International Law Studies,* Cilt 76, Sayı 1, 2002, s. 60.

büyük ekonomik kayıplara, ciddi fiziksel yıkımlardan yaygın ölümlere kadar değişiklik gösterebilmektedir.[505]

Uluslararası hukukçuların siber alana yaklaşımı, söz konusu alanın uluslararası hukukta nasıl temsil edildiğine dair anlayışlardan etkilenmektedir. Bu nedenle, sadece fiziksel alanlarla olan benzeşimler incelenmemektedir. Aynı zamanda siber uzay sahasına devletlerin egemen eşitliği, uluslararası barış ve güvenliğin korunması, uluslararası sorunların çözümü için uluslararası işbirliği gibi temel uluslararası hukuk ilkelerinin nasıl uygulandığı ve durumun nasıl modellendiğine de bakılmaktadır.[506] Öyle ki, Uluslararası Adalet Divanı'nın (UAD) içtihadı, antlaşmaların yorumlanması, devletler arasındaki bölgesel uyuşmazlıklar veya Uluslararası İlişkilerde güç kullanımı gibi geleneksel başlıkların hâkimiyeti altındayken siber uzay gibi yeni ve oldukça dinamik bir fenomenin doğrudan uluslararası hukuk tarafından benimsenmesi kolay olmamaktadır.[507]

Devletlerin kendi ulusal sınırları içerisinde giderek daha fazla kontrol sahibi olmalarına ve hatta sınırları içerisindeki sunucular ve düğümler (*nodes*) üzerinde yetkileri bulunmalarına rağmen sunucular (*server*) ve bilgisayarlar arasındaki iletişim, çoğunlukla özel ağlar tarafından işletilen ve herhangi bir devlet kontrolünde olmayan uluslararası ağlar üzerinden yönlendirilmektedir. Örneğin; bir ülkeden gönderilen iş teklifleri, mesajlar, veriler vb. başka bir ülkedeki sunucuda depolanırken, üçüncü bir ülkedeki olayları etkileyebilmektedir. Böylelikle siber alandaki kamusal ve özel sektöre ait ulusal varlıklar, farklı siber aktörlerin çeşitli siber operasyonlarıyla araştırılabilmekte, etkilenebilmekte ve hatta kontrol edilebilmektedir. Öne çıkan bu özelliklerden dolayı siber alanın devletlerin klasik egemenlik alanlarının ötesinde ve insan faaliyetlerinin diğer alanlarıyla benzer düzenlemelere tabi olmayan yeni bir boyut olduğu iddiaları söz konusu olmaktadır.[508] Diğer yandan ise siber uzay alanını beşinci stratejik rekabet alanı

---

[505] Michael N. Schmitt, "Cyberspace and International Law: The Penumbral Mist of Uncertainity", *Harvard Law Review Forum*, Cilt 126, Sayı 176, 2013, s. 176.
[506] Nicholas Tsagourias, "The Legal Status of Cyberspace", Editörler: Nicholas Tsagouris & Russell Buchan, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, Cheltenham 2015, ss. 15-16.
[507] Paul Przemyslaw Polanski, "Cyberspace: A New Branch of International Customary Law?", *Computer Law & Security Review*, Cilt 33, Sayı 3, 2017, s. 372.
[508] Pål Wrange, "Intervention in National and Private Cyberspace and International Law", *Stockholm University Research Paper*, Sayı 23, 2017, ss. 2-3.

olarak kabul etmeyen ve dolayısıyla da uluslararası hukukun siber sahaya ve operasyonlarına uygulanabileceğini iddia eden görüşler de söz konusudur. Bu yaklaşımlara göre siber uzayın yapay özelliği ve diğer dört alanın aksine gidilemez olması, onu diğer alanlardan ayırmak yerine onları doğrudan etkilemektedir. Bilgisayar ve telekomünikasyon ağlarıyla birlikte İnternetten oluşan bu kavramsal ortam, uluslararası hukuk amacıyla yeni bir saha veya insan faaliyet alanı oluşturmayan kurgusal bir boyut şeklinde nitelendirilmektedir. Bu sebeple siber uzayın, sadece dış uzay ve hava sahasından ayrımının yapılması yeterlidir. Buna göre siber faaliyetler, mevcut dört stratejik alanda gerçekleştiğinden dolayı söz konusu alanlarla ilgili uluslararası hukuk normları tarafından düzenlenebilirler.[509] Yukarıda sunulan bu iki farklı görüş, uluslararası hukukun siber uzay sahasına ve siber operasyonlara uygulanabilirliği hususundaki tartışmalı boyutu gözler önüne sermektedir.

Öte yandan siber uzay sahası, herhangi bir aktörün kuralsız veya kısıtlama olmaksızın düşmanca faaliyetler gerçekleştirebileceği kanunsuz bir alan olarak düşünülmemelidir. Teknolojik gelişmelerle birlikte özellikle çatışma araçlarında yaşanan dönüşüm, mevcut kuralların bu yeni ortamda geçerli olacak şekilde düzenlenmesini gerekli kılmaktadır.[510] Uluslararası hukuk normlarının siber alana uygun şekilde düzenlenmesi, siber uzayın operasyonel doğasının kullanımına dair çeşitli yaklaşımların yarattığı belirsizlik ortamının minimize edilebilmesi, siber alandaki asimetrik çatışmaların yaratabileceği etki büyüklüğünün farkına varılabilmesi ve siber sahanın farklı koşullarda sağlayabileceği fonksiyonel faydaların maksimizasyonu açısından son derece önemlidir.[511] Siber uzay sahası her ne kadar yapay nitelikte olsa da reel dünyadaki etki boyutu ve kapsamı göz önünde bulundurulduğunda, tüm devletler ve uluslar tarafından eşit olarak paylaşılan doğal çevrenin evrensel koruma ve düzenleme ihtiyacının benzerine sahiptir. Siber ortam da doğal çevre gibi devlet sınırlarından bağımsız şekilde var olmakta ve yetki mücadelelerine sebebiyet vermektedir. Uluslararası siber güvenliğin devletler

[509] François Delerue, "Reinterpretation or Contestation of International Law in Cyberspace?", *Israel Law Review*, Cilt 52, Sayı 3, 2019, ss. 302-304.
[510] Harold Hongju Koh, "International Law in Cyberspace", *Harvard International Law Journal*, Cilt 54, Sayı 1, Aralık 2012, s. 3.
[511] Duncan B. Hollis, *a.g.m.*, s. 1039.

açısından önemli bir öncelik haline gelmesiyle birlikte ise insanların çevrimiçi faaliyetlerini düzenlemenin tek mantıklı yolu olarak uluslararası hukuk görülmüştür.[512]

Geleneksel uluslararası hukuk, devletlerin yasal zorunluluk inancıyla (*opinio juris*) izledikleri genel ve tutarlı pratikler üzerinden gelişmektedir. Devlet uygulamalarının *opinio juris* olarak siber faaliyetlerle ilgili boşluğu, uluslararası hukukun bu alana nasıl uygulanabileceğine dair görüşlerle doldurulmaktadır.[513] Buna karşın, uluslararası hukukun olağan kurallarının siber uzay alanında nasıl anlaşılması gerektiği tam olarak açık değildir ve devletler de bu konuların açıklığa kavuşturulması hususunda pek yardımcı olmamıştır. Özellikle siber alanın güçlenerek yayılmaya ve derinleşmeye başladığı süreçlerde devletlerin yeni uluslararası sözleşmelere veya farklı yasal enstrümanlar üzerinden müzakerelere mesafeli durması, *opinio juris* devlet uygulamalarının olması gerekenden daha az kalmasına neden olmuştur.[514] Siber faaliyetlerin büyük çoğunluğunun gizlilikle çevrelenmesi, siber aktörlerin anonimliği ve dolayısıyla siber aktör motivasyon analizlerinin zorluğu gibi temel siber ortam faktörleri de hesaba katıldığında devletler açısından uygulamalar daha da karmaşıklaşmaktadır.[515] Bilhassa günümüz Uluslararası İlişkilerindeki devletlerin siber güvenliğin ve siber gücün öneminin daha fazla bilincine vararak orduları kapsamında, büyük finansmanlar sağlayarak siber yeteneklerini geliştirme girişimleri ve diğer devletler ya da devlet destekli aktörler aleyhine faaliyetlerde bulunmaları, Uluslararası İlişkilerde kuvvet kullanımını düzenleyen kurallarca siber alan eylemlerinin irdelenmesini elzem kılmaktadır.[516]

Uluslararası hukuk, çatışmayı düzenleyen iki ayrı hukuk organından oluşmaktadır: Savaşa başvurmanın hukuku (*jus ad bellum*) ve Savaşta hukuk (*jus in bello*). *Jus ad bellum* normları, devletlerin ulusal politikalarının aracı olarak güce ne zaman başvurduklarını belirlerken, *jus in bello* normlar ise askeri ve diğer silahlı

---

[512] Joanna Kulesza, "International Internet Law", *Global Change, Peace & Security*, Cilt 24, Sayı 3, Ekim 2012, ss. 353-354.
[513] Brian J. Egan, J. D., "International Law and Stability in Cyberspace", *Berkeley Journal of International Law*, Cilt 35, Sayı 1, 2017, s. 171.
[514] Pål Wrange, *a.g.m.*, s. 19.
[515] Gary Brown & Keira Poellet, "The Customary International Law of Cyberspace", *Strategic Studies Quarterly*, Cilt 6, Sayı 3, Cyber Special Edition, Güz 2012, s. 129.
[516] Yasir Gökçe, "Güç Kullanımı Olarak Siber Faaliyetler: Uluslararası Hukukun Siber Uzaya Uygulanabilirliği", *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 1, Sayı 1, 2017, s. 25.

aktörlerin kimi ve neyi hedef alabileceği de dâhil olmak üzere nasıl güç kullanabileceğini ve uygulanan kuralları belirlemektedir.[517] Geleneksel uluslararası hukuku yansıtan BM Antlaşması'nın 2. Maddesi'nin 4. Fıkrası'ndaki "*Teşkilâtın Üyeleri, milletlerarası münasebetlerinde gerek herhangi bir başka Devletin toprak bütünlüğüne veya siyasî bağımsızlığına karşı, gerekse Birleşmiş Milletlerin amaçları ile telif edilemeyecek herhangi bir surette, tehdide veya kuvvet kullanılmasına başvurmaktan kaçınırlar.*"[518] hükmü gereği devletlerin birbirlerine güç kullanmaları, aynı Antlaşmanın 39., 42. ve 51. Maddeleri'nde BM Güvenlik Konseyi'nin izin verdiği durumlar ve meşru müdafaa hakkı istisnaları dışında yasaklanmıştır. Söz konusu maddeler devlet sorumluluğu kapsamında yalnızca devletler tarafından yürütülen eylemlere atfedilmiştir ve terörist gruplar gibi devlet dışı aktörlerin eylemleri üzerinde hiçbir etkisi bulunmamaktadır.[519] Dolayısıyla devlet dışı aktörlerin eylemleri devletlere atfedildiği takdirde yukarıda sunulan kuvvet kullanma yasağı hükmü ihlal edilmiş olmaktadır. Ek olarak; BM Antlaşması'nın 51. Maddesi'nde "silahlı saldırıya hedef olma" vurgusu ve Uluslararası Adalet Divanı'nın (UAD) 8 Temmuz 1996 tarihli "Nükleer Silahların Tehdit ve Kullanımının Hukuka Uygunluğuna Dair Danışma Görüşü"[520]ndeki kitlesel imha ve felaket doğurabilecek her türlü aracın –nükleer, kimyasal, biyolojik vb.– güç kullanımına elverişli silah olarak değerlendirilmesi, silahlı saldırı kapsamında saldırı araçlarının ve sonuçlarının etkili olduğunu göstermektedir.[521] Buna göre *jus ad bellum* uygulanırken, siber faaliyetleri kuvvet kullanım çerçevesinde geleneksel saldırılardan ayıran dört özellik öne çıkmaktadır: Çeşitli siber operasyon türlerinin ilk eylem sonrası ikinci bir aktör tarafından daha fazla eylem gerektirmesi anlamına gelen "dolaylılık"; Ne saldırı hedefinin ne de kullanılan silahın fiziksel düzeyde bulunmayacağı gerçeğini ifade eden "soyutluk"; Bazı durumlarda saldırının kökenini

---

[517] Michael N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context", Editörler: Christian Czosseck, Rain Ottis & Katharina Ziolkowski, *Proceedings of the 4th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn 2012, s. 284.

[518] T.C. Resmi Gazete, "Birleşmiş Milletler Aıdlaşması", Kanun No: 4801, Sayı: 6092, 24 Ağustos 1945, s. 9238, *https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf*, (Erişim Tarihi: 26 Mart 2020).

[519] Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?", *Stanford Law & Policy Review*, Cilt 25, Sayı 2, 2014, s. 279.

[520] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons: Advisory Opinion of 8 July 1996*, Reports of Judgements, Advisory Opinions and Orders, s. 248.

[521] Yasir Gökçe, *a.g.m.*, s. 27.

tespit etmenin çok zor olabileceği gerçeğini dikkate alan "konumsallık"; siber operasyonların sonuçlarının basit rahatsızlıklardan kapsamlı fiziksel yıkımlara kadar çeşitlilik gösterebileceğini ifade "sonuçsallık".[522] Siber operasyonlar ile kuvvet kullanım eşiği sorununa yönelik Duncan B. Hollis tarafından üç ana yaklaşım – araçsal yaklaşım, hedefe dayalı yaklaşım ve etkisel yaklaşım– geliştirilmiştir. Buna göre araçsal yaklaşımda belirleyici faktör kullanılan silahtır ve bir siber operasyonda kullanılan silah geleneksel olarak kullanılanlara yeterince benziyorsa kuvvet kullanımı olarak nitelendirilebilir. Hedefe dayalı yaklaşımda ise kritik altyapıları hedefleyen herhangi bir eylem silahlı saldırı olarak tanımlanır ve kuvvet kullanımı kapsamındadır. Etkisel yaklaşımda ise siber operasyonun genel etkileri belirleyici faktör olarak alınır ve kinetik kuvvet tarafından üretilen etkilere eşdeğer etkiler yaratıldığında kuvvet kullanımı gerçekleştirilmiş olmaktadır.[523] Bu bağlamda oluşturulan uluslararası hukuk anlaşma metinlerinde özellikle etkisel yaklaşımın öne çıktığı görülmektedir.

Siber suçlara yönelik başlıca bağlayıcı uluslararası hukuk anlaşmaları şu şekildedir: Avrupa Konseyi Siber Suç Sözleşmesi (*The Convention on Cybercrime of the Council of Europe*)[524]; Şangay İşbirliği Örgütü Uluslararası Bilgi Güvenliği Alanında İşbirliği Anlaşması (*Shanghai Cooperation Organization Agreement on Cooperation in the Field of Ensuring the International Information Security*)[525]; Avrupa Konseyi Çocukların Cinsel Suistimal ve Cinsel İstismara karşı Korunması Sözleşmesi (*The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*)[526]. Siber savaş ve siber terörizme yönelik bağlayıcı uluslararası anlaşma henüz olmamakla birlikte bağlayıcı olmayan uluslararası hukuk referans kaynağı metinler şunlardır: Siber Savaşa Uygulanacak Uluslararası Hukuk

---

[522] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, 1. Basım, Cambridge University Press, Cambridge 2012, ss. 65-74.
[523] Duncan B. Hollis, *a.g.m.*, ss. 1040-1041.
[524] Council of Europe, "Details of Treaty No. 185: Convention on Cybercrime", *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185*, (Erişim Tarihi: 28 Mart 2020).
[525] The Shanghai Cooperation Organisation (SCO), "Documents", *http://eng.sectsco.org/documents/*, (Erişim Tarihi: 28 Mart 2020).
[526] Council of Europe, "Details of Treaty No.201: Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse", *https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/201*, (Erişim Tarihi: 28 Mart 2020).

Hakkında Tallinn El Kitabı (*Tallinn Manual on the International Law Applicable to Cyber Warfare*); Siber Operasyonlara Uygulanacak Uluslararası Hukuk Hakkında Tallinn El Kitabı 2.0 (*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*).

4.1.1. Avrupa Konseyi Siber Suçlar Sözleşmesi (2001)

Siber faaliyetler, uluslararası hukukun davranışlar ve yükümlülüklerle ilgili olan birincil kuralına aykırı olmaları ve birincil kuralların yaratılmasını, değiştirilmesini, yorumlanmasını, geçerliliğini, sonra ermesini ve ihlallerinin sonuçlarını düzenleyen devlet sorumluluğundaki ikincil kurallar[527] altında bir devlete atfedilmeleri durumunda uluslararası olarak yasadışı eylem şeklinde yorumlanmaktadırlar. "Avrupa Konseyi Siber Suçlar Sözleşmesi" (*The Convention on Cybercrime of the Council of Europe*) birincil kurallar bağlamında siber faaliyetlerin açıkça ve spesifik olarak ele alındığı bilgi teknolojilerine yönelik ilk girişim olarak kabul edilmektedir.[528] "Budapeşte Sözleşmesi" (*The Budapest Convention*) olarak da bilinen bu metin, siber sahayla ilgili konularda tek bağlayıcı uluslararası araçtır ve siber suçlara karşı kapsamlı ulusal mevzuat geliştiren her ülke için bir rehber niteliği taşımaktadır. Ayrıca bu anlaşmaya taraf olan devletler arasında uluslararası işbirliği geliştirilmesi adına bir çerçeve görevi görmektedir.[529] 30 Mart 2020 tarihi itibariyle bu sözleşme 65 devlet tarafından onaylanmış, 3 ülke – İrlanda, İsveç ve Güney Afrika– ise sözleşmeyi imzalamış ancak henüz onaylamamıştır. Avrupa dışındaki taraf devletler şu şekildedir: ABD, Arjantin, Avustralya, Kanada, Şili, Kolombiya, Kosta Rika, Dominik Cumhuriyeti, Gana, İsrail, Japonya, Mauritius, Fas, Yeşil Burun Adaları, Panama, Paraguay, Peru, Filipinler, Senegal, Sri Lanka ve Tonga.[530] Sözleşmenin Birinci Bölümünde "Terimler" başlığı altında "bilgisayar sistemi", "bilgisayar verisi", "hizmet sağlayıcı"

---

[527] Hukukun birincil ve ikincil kuralları hakkında detaylı bilgi için bkz.: Herbert Lionel Adolphus Hart, *The Concept of Law*, 2. Basım, Oxford University Press, New York 1994, ss. 213-237.
[528] Marco Roscini, *a.g.e.*, s. 19.
[529] Council of Europe, "Details of Treaty No. 185: Convention on Cybercrime", Treaty Office, *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185*, (Erişim Tarihi: 30 Mart 2020).
[530] Council of Europe, "Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime", Treaty Office, *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=EyR6nySC*, (Erişim Tarihi: 30 Mart 2020).

ve "trafik bilgileri" kavramları tanımlanmıştır. İkinci Bölümde "Ulusal Düzeyde Alınacak Önlemler" başlığı altında "Maddi Ceza Hukuku", "Usul Hukuku" ve "Yargı Yetkisi" açıklanmıştır. Üçüncü Bölümde ise "Uluslararası İşbirliği" başlığı altında "Genel İlkeler", "Özel Hükümler" ve "Diğer Hükümler" sunulmuştur.[531]

23 Kasım 2001 tarihinde imzalanarak 1 Temmuz 2004 tarihinde yürürlüğe giren Budapeşte Sözleşmesi'nin üç ana hedefi söz konusudur: Buna göre ulusal hukuktaki yerel suç unsurlarıyla siber suçlar alanındaki ilgili hükümlerin uyumlu hale getirilmesi, siber suçların soruşturulması ve kovuşturulmasıyla ilgili elektronik kanıtların toplanması hususunda yerel ceza mahkemelerinin desteklenmesi ve siber alana dair bir uluslararası işbirliği rejiminin hızlı ve etkili şekilde oluşturulması amaçlanmıştır.[532] Bu Sözleşmeye göre artık bilgisayar verilerinin ve sistemlerinin gizliliği ile bütünlüğü ve kullanılabilirliğine yönelik siber uzay sahasından kaynaklanan eylemler doğrudan tehdit olarak yasal çerçevede ele alınmıştır. Hem özel mülkiyetin hem de kamu mallarının korunmasını hedefleyen bu Sözleşme, toplumun siber suçlara karşı korunmasına odaklanan taraf devlet yasalarının uyumlu hale getirilmesine zemin hazırlamıştır.[533]

Sözleşmeye verilen reaksiyonlara bakıldığında; özel sektörün hem destekleyen hem de çekimser kalan yönlerinin olduğu görülmektedir. Telif hakkı sahipleri Sözleşmeyi güçlü şekilde desteklerken, İnternet servis sağlayıcıları ve diğer ağ operatörleri ise Sözleşmenin üzerlerine depolanmış trafik verileri ve abone bilgileri şeklinde konulabilecek ek müdahale talepleri ve artabilecek yüklerden endişe duymuşlardır.[534] ABD'nin Sözleşmenin taslak sürecinde, müzakerelerinde ve hazırlanmasında doğrudan yer alması, Sözleşmenin merkezi hükümlerinin mevcut ABD yasaları ve prosedürlerinin çerçevesiyle tutarlılık sağlamasına neden

---

[531] Council of Europe, "Convention on Cybercrime", European Treaty Series, Sayı 185, Budapeşte, 23 Kasım 2001. Sözleşmenin hem İngilizce hem de Türkçe metnine şuradan ulaşılmıştır: *https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/8601684*, (Erişim Tarihi: 30 Mart 2020).

[532] Kriangsak Kittichaisaree, *Public International Law of Cyberspace*, Springer Nature, Law, Governance and Technology Series, Cilt 32, Cham 2017, s. 271.

[533] Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis & Theodoros Apostopoulos, "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare", *Information & Computer Security*, Cilt 24, Sayı 1, 2016, s. 41.

[534] Michael A. Vatis, "The Council of Europe Convention on Cybercrime", *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, The National Academic Press, Washington 2010, s. 218.

olduğundan ABD'nin Sözleşmeye taraf olması gayet kolay gerçekleşmiştir.[535] Diğer taraftan en dikkat çekici reaksiyon Rusya ve Çin'den gelmiştir. Rusya, bu Sözleşmeyi imzalamamış ve onaylamamıştır. Bu durum, Rusya'nın 1990'ların ortalarından beri BM'de ulus devletlerin siber silahlarla yapabileceklerini kısıtlayacak bir siber silah kontrol anlaşması önerisiyle alakalıdır.[536] Sözleşmeyle ilgili olarak ise Rusya, yasa uygulayıcı kurumların bilgisayar ağlarına veya verilere, ağ sorumluları ya da veri sahiplerinin onayıyla da olsa, tek taraflı sınır ötesi erişimine izin verilmesinin egemenlik ihlali olduğu ve Rus anayasasına aykırılık teşkil ettiği gerekçeleriyle reddetmiştir.[537] Buna karşın, Michael A. Vatis'e göre Rusya'nın Budapeşte Sözleşmesi'ni imzalamamasının asıl nedeni olarak çok sayıda siber saldırının arkasında Rusya'nın ve Rus devlet destekli devlet-dışı aktörlerin bulunması ve bundan dolayı siber suç soruşturmalarında diğer ülkelere yardım etme yükümlülüğünden kaçınma arzusu olduğu belirtilmektedir.[538] Çin'e bakıldığında, siber alandaki uluslararası anlaşmalara Rusya ile benzer şekilde devlet merkezli yaklaşım sergilediği görülmektedir. Buna göre Çin, Sözleşmenin siber suç soruşturmaları ve kovuşturmaları sırasında ulusötesi kanıtların toplanmasına ilişkin hükümlerinin devlet egemenliğini ihlal ettiğini belirtmiş ve BM Antlaşması'nın Budapeşte Sözleşmesi'ne kıyasla daha doğru bir metin olduğunu savunmuştur.[539]

Sonuç olarak; Budapeşte Sözleşmesi ile siber alana dair uluslararası düzeyde soruşturma prosedürlerinin standartlaştırılması, devletler arasında yasaların uyumlu ve tutarlı hale getirilmesi ve muhtemelen Sözleşmeye taraf devletlerdeki siber suçların büyüme hızının yavaşlaması gibi net faydalar sağlanmıştır. Diğer taraftan, Sözleşmeye taraf olmak, siber güvenlik konusunda tarafların artık daha fazla bilinçli olacağının işareti şeklinde yorumlanabilmektedir. Bununla birlikte, bilgi paylaşımını

---

[535] Amalie M. Weber, "The Council of Europe's Convention on Cybercrime", *Berkeley Technology Law Journal*, Cilt 18, Sayı 1, Annual Review of Law and Technology, 2003, s. 435.
[536] Tim Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-security", Harvard Kennedy School, Belfer Center for Science and International Affairs, *Explorations in Cyber International Relations Discussion Paper Series 2011-11*, Eylül 2011, s. 6.
[537] John Markoff & Andrew E. Karmer, "In Shift, U.S. Talks to Russia on Internet Security", The New York Times, 12 Aralık 2009, *https://www.nytimes.com/2009/12/13/science/13cyber.html*, (Erişim Tarihi: 30 Mart 2020).
[538] Michael A. Vatis, *a.g.m.*, s. 218.
[539] Kimberly Hsu & Craig Murray, "China and International Law in Cyberspace", *U.S.-China Economic and Security Review Commission Staff Report*, 6 Mayıs 2014, s. 3.

ve uyarmayı içeren normlar sayesinde kullanıcıların savunmasızlığının azalması ya da suç dürtülerinin sınırlandırılması söz konusu olabilir.[540] Dolayısıyla Budapeşte Sözleşmesi, Siber Uluslararası İlişkilerin düzenlenmesinde uluslararası hukuk rolündeki en önemli gelişmelerin başında gelmektedir.

4.1.2. Siber Savaşa Uygulanacak Uluslararası Hukuk Hakkında Tallinn El Kitabı (2013)

Estonya'nın Tallinn kentindeki NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (*The NATO Cooperative Cyber Defence Centre of Excellence,* NATO CCD-CoE), siber savaşı düzenleyen uluslararası hukukun ilk kapsamlı incelemesinin yürütülmesi adına "Uluslararası Uzmanlar Grubu"nu (*International Group of Experts*) oluşturmuştur. Uluslararası Kızılhaç Komitesi (*The International Committe of the Red Cross,* ICRC), NATO'nun Müttefik Dönüşüm Komutanlığı (*Allied Command Transformation,* ACT) ve ABD Siber Komutanlığı'nın (*The United States Cyber Command*, USCYBERCOM) gözlemciler sağladığı bu Grup, siber operasyonlarla ilgili yasal tavsiyeden sorumlu kıdemli askeri görevliler de dâhil olmak üzere toplamda yirmi uluslararası hukuk uzmanı ve uygulayıcıyı kapsamıştır. Üç yıllık bir sürecin ardından "Siber Savaşa Uygulanacak Uluslararası Hukuk Hakkında Tallinn El Kitabı" (*Tallinn Manual on the International Law Applicable to Cyber Warfare*) isimli çalışma 2013 yılında yayınlanmıştır.[541] Tallinn El Kitabı projesi, siber faaliyetleri çevreleyen karmaşık hukuki meselelere bir dereceye kadar açıklık getirilmesi umuduyla, siber savaşı düzenleyen uluslararası hukuku inceleyen, proje dâhilindeki uzmanların oybirliğiyle kabul edilen ve bağlayıcılığı bulunmayan bir kurallar dizisidir.[542]

Tallinn El Kitabı, uluslararası güvenlik alanında yasal uzmanlığın nasıl harekete geçirilebileceğine dair iyi bir örnek olarak yorumlanmaktadır. Uluslararası

---

[540] Roger Hurwitz, "A New Normal? The Cultivation of Global Norms As Part of A Cybersecurity Strategy", Editörler: Panayotis A. Yannakogeorgos & Adam B. Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, Taylor & Francis, Florida 2014, s. 253.

[541] Wolff Heintschel von Heinegg, "The Tallinn Manual and International Cyber Security Law", Editörler: Terry D. Gill, Robin Geiß, Tim McCormack, Christophe Paulussen & Jessica Dorsey, *Yearbook of International Humanitarian Law*, Cilt 15, 2012, ss. 3-4.

[542] Michael N. Schmitt, *Tallinn Manual On The International Law Applicable To Cyber Warfare*, 1. Basım, Cambridge University Press, Cambridge 2013, s. 18.

Uzmanlar Grubu, yasal kaynaklarla uzmanlıkları birleştirerek, uluslararası hukukun devlet merkezli temellerini zorlayan teknolojik gelişmeler karşısında mevcut uluslararası hukuk kurallarını uyumlu hale getirmeye çalışmıştır.[543] Bu arada projenin hazırlandığı yer olarak Tallinn'in seçilmesi tesadüfi değildir. 2007 yılında Estonya'da yaşanan bir dizi siber saldırı, siber alanın devletler arası doğasını gözler önüne sermiş ve uluslararası hukuka ilişkin bu devletler arası siber saldırıları yönetebilecek yasal tartışmaların geliştirilmesi için teşvik unsuru olmuştur. Yine Tallinn El Kitabı'nın metodolojisine bakıldığında, siber savaş ortamının düzenlenmesine yönelik yeni bir uluslararası yasa oluşturmak yerine mevcut uluslararası yasaların yaşanan devletler arası siber olaylara uygulandığı ve yorumlandığı görülmüştür.[544]

"Uluslararası Siber Güvenlik Hukuku" ve "Siber Silahlı Çatışma Hukuku" olmak üzere iki ana bölümden oluşan Tallinn El Kitabı, "Devletler ve Siber Uzay", "Kuvvet Kullanımı", "Genel Olarak Silahlı Çatışma Hukuku", "Düşmanca Davranışlar", "Belirli Kişiler, Nesneler ve Faaliyetler", "İşgal" ve "Tarafsızlık" olmak üzere yedi alt başlık ve toplamda 95 kural içermektedir. Bu başlıklar içerisinde egemenlik, yargılama yetkisi, siber altyapının kontrolü ve devletlerin yasal sorumluluğuna dair öne çıkan kurallar şu şekilde belirtilmiştir[545]:

> "*Kural 1–Egemenlik: Devlet, kendi egemenlik bölgesi dâhilinde, siber altyapı ve siber eylemler üzerinde kontrol yetkisini kullanabilir.*[546]
> *Kural 2–Yargılama Yetkisi: Bir devlet, uygulanabilir uluslararası yükümlülükleri ihlal etmeden:*
> *a) Kendi sınırlarındaki siber faaliyetlerle ilgili kişiler üzerinde,*
> *b) Kendi sınırlarındaki yerleşik siber altyapı üzerinde,*

[543] Oliver Kessler & Wouter Werner, "Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare", *Leiden Journal of International Law*, Cilt 26, Sayı 4, Aralık 2013, s. 796.
[544] Ido Kilovaty, "Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", *American University National Security Law Brief*, Cilt 5, Sayı 1, 2014, s. 97.
[545] Çalışmanın Türkçe hali "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı (Uluslararası Siber Güvenlik Hukuku)" başlıklı ve 15 sayfalık özet şeklinde T.C. Milli Güvenlik Kurulu Genel Sekreterliği çevrimiçi sayfasına yüklenmiştir. Ana bölüm ve alt bölüm başlıklarıyla, öne çıkan dört kuralın Türkçe versiyonu buradan kullanılmış olup ek olarak her kuralın orijinal metindeki yerleri dipnot olarak belirtilmiştir. T.C. Milli Güvenlik Kurulu Genel Sekreterliği, "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı (Uluslararası Siber Güvenlik Hukuku)", *https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku*, (Erişim Tarihi: 31 Mart 2020).
[546] Michael N. Schmitt, *Tallinn Manual On…,* s. 25.

> *c) Uluslararası hukukla uyumlu biçimde, kendi sınırı haricinde de, yargılama yetkisini kullanabilir.*[547]
>
> *Kural 5–Siber Altyapının Kontrolü: Bir Devlet, kendi sınırlarında veya kendi münhasır resmi kontrolünde olup, başka Devletleri ters veya hukuksuz olarak etkileyecek siber altyapıya bilerek izin vermez.*[548]
>
> *Kural 6–Devletlerin Yasal Sorumluluğu: Bir Devlet, kendisine atfedilebilen ve uluslararası yükümlülük ihlali oluşturan bir siber operasyon konusunda uluslararası yasal sorumluluğa katlanır.*[549]"

Diğer taraftan Tallinn El Kitabı'nda savaşa girmenin haklı nedenleri (*jus ad bellum*), savaş sırasında uyulması gereken kurallar (*jus in bello*) arasında her zaman belirgin olmamakla beraber şöyle bir ayrım tespit edilmiştir: "Öncesinde kinetik silahlı çatışma yapmış olan tarafların siber operasyonları" ve "Kendi başına silahlı bir çatışmayı tetikleyen siber operasyonlar". Bu bağlamda Uluslararası Uzmanlar Grubu, 23. Kuralın 10. Maddesinde "tahribatsız fakat şiddetli siber operasyonların, düşmanlıkları silahlı çatışma düzeyinde arttırıp arttırmayacağı" konusunda fikir birliği sağlamanın oldukça zor olduğunu belirtmektedir.[550] Dolayısıyla siber güç tarafından tetiklenen silahlı bir çatışmanın kinetik silahların kullanımına yol açabileceğinin hesabının da yapılması gereklidir.[551]

2013 yılında yayınlanan Tallinn El Kitabı, yıkıcı siber saldırılar ve bu durumda kalan devletlerin kendilerini savunma hakları üzerine kurgulanmıştır. Ulusal güvenlik perspektifinden bakıldığında ise siber operasyonlar, barış zamanında meydana gelenlere kıyasla daha endişe verici olsa da, devletlerin günlük olarak kuvvet kullanım eşiği altındaki siber sorunlarla ve risklerle –bilgi hırsızlığı, manipülasyon, devletin bilgisayar ağlarına sızılması vb.– de uğraşması gerekmektedir.[552] Bu bağlamda 2013-2016 yılları arasında NATO CCD-CoE tarafından Tallinn El Kitabı'nın barış zamanındaki siber operasyonları düzenleyen uluslararası kamu hukukunu da dâhil edecek şekilde genişletilmesi söz konusu

---

[547] *A.g.e.*, s. 27.
[548] *A.g.e.*, ss. 32-33.
[549] *A.g.e.*, s. 35.
[550] *A.g.e.*, s. 78.
[551] Dieter Fleck, "Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual", *Journal of Conflict and Security Law*, Cilt 18, Sayı 2, Temmuz 2013, s. 337.
[552] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights", *Georgetown Journal of International Law*, Cilt 48, Sayı 3, 2017, ss. 736-737.

olmuştur.[553] 2017 yılında da "Siber Operasyonlara Uygulanacak Uluslararası Hukuk Hakkında Tallinn El Kitabı 2.0" (*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*) başlığıyla güncellenerek yayınlanmıştır.

Netice olarak Tallinn El Kitapları (1.0 & 2.0), siber uzay alanına yönelik normların ve kuralların yasal uzmanlıklar çerçevesinde nasıl geliştirilebileceğini göstermektedir; ancak siber alanın dinamik, karmaşık ve belirsiz yapısının doğurduğu öngörülemez nitelikli sorunlar, bu kılavuzların sayesinde bazı konularda fikir birliği ile azaltılırken, bir taraftan da yeniden üretilmektedir. Kuralların ve ilkelerin uygun şekilde yorumlanması konusunda fikir birliği olmayan durumlar, uluslararası hukuki muhakemede ucu açık ilkeleri ve bağlamsal faktörleri yeniden sunarak mevcut belirsizliklerin yansıtılmasına ve sağlamlaştırılmasına neden olmaktadır.[554] Öte yandan Tallinn El Kitapları; kapsamlı yapısı, analiz çeşitliliği ve devlet yaklaşımları ile uzman görüşlerini biraraya getiren derin özelliği dikkate alındığında, siber operasyonlara yönelik uluslararası hukuk tartışmalarında en değerli referans kaynaklarından biri olarak kabul edilmektedirler.[555] Siber alanın diğer stratejik alanlardan çok farklı olan özelliklerinden kaynaklanan çeşitli belirsizlik ve hukuksal boşluk durumlarının, siber uzaydaki değişimin hızlanması ve geleneksel hukuk yaklaşımlarının devletlerin yeni pratikleriyle gelişerek ve uyumlu hale gelerek doldurulacağı öngörülmektedir.[556] Bu açıdan devletlerin siber alanda karşılabilecekleri sorunlu durumlar karşısında yasal zorunluluk duygusuyla uygulama geliştirebilmeleri hususunda Tallinn El Kitapları yönlendirici kaynak pozisyonundadır.

---

[553] Michael N. Schmitt, *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*, 1. Basım, Cambridge University Press, Cambridge 2017, s. 1.
[554] Oliver Kessler & Wouter Werner, *a.g.m.*, s. 810.
[555] Eric Talbot Jensen, *a.g.m.*, s. 778.
[556] Sandra Braman, "Cyber Security Ethics at the Boundaries: System Maintenance and the Tallinn Manual", Editörler: Ludovica Glorioso & Anna-Maria Osula, *Proceedings: 1st Workshop on Ethics of Cyber Conflict*, Tallinn 2014, s. 58.

4.2. Uluslararası İşbirliği ve Siber Uzay

Uluslararası işbirliği perspektifinden yaklaşıldığında siber uzay sahası, hiçbir aktörün çıkarılamadığı ve dışlanamadığı ortak bir mülkiyet kaynağı olarak yorumlanmaktadır. Dışlamanın bir seçenek olmadığı durumlarda aktörlerin mal ve hizmetlerin faydalarından bağlayıcı yükümlülükler olmaksızın yararlanma tercihleri ön plana çıkmakta ve aşırı sömürü sorunu oluşmaktadır. Siber alanla ilgili ortak bir anlaşmaya varabilmenin imkânsız olmasa bile oldukça zor olduğu varsayımının özünü teşkil eden aktör fazlalığı ve çeşitliliği göz önünde bulundurulduğunda, söz konusu aktörlerin güçlenmesiyle birlikte küresel müşterek değerlere olan bağımlılık giderek artmakta ve bu bağımlılıktan dolayı aktörlerin güvenliği müştereklerin güvenliğiyle sıkı sıkıya bağlı hale gelmektedir. Bu nedenle de aktörlerin var oluşlarını devam ettirebilmek ve çok daha güçlü poziyonlara gelebilmek adına maliyetleri paylaşarak işbirliği yapmaları kaçınılmaz olmaktadır.[557] Uluslararası İlişkiler alanının dayandığı devletler ararası sistemik veya küresel düzeyde faaliyet gösteren ve devlet kimliklerini ve davranışlarını etkileyen faktörler olduğu fikri, siber alanda çok daha komplike hale gelmektedir. Siber alan içi etkileşimlerin, tehditlerin, iç mücadelelerin ve niyet algılarının belirsizliği ve karmaşıklığı, devletleri siber alana yönelik küresel düzeyde işbirliklerine mecbur kılmaktadır.[558] Dahası, siber uzay sahasının çok kutuplu ve oligopolistik rekabet doğasının olası sert etkilerinin yumuşatılabilmesi adına özellikle büyük güçler arasındaki kaçınılmaz işbirliği ortamının siber alan için yeni kurallar, normlar ve standartlar oluşturması ve teşvikler yaratması da söz konusu olmaktadır.[559] Siber alan norm ve standartlarının uluslararası kabulü olmadığı takdirde elektronik ticari işlemlerin güvenliği ve kişisel iletişimin gizliliği gibi uluslararası olarak kabul edilmiş siber güvenlik hedefleri için paydaşlar arasındaki gerekli güven ortamı, devlet sponsorlu siber saldırıların tehdidine açık olmaktadır. Dolayısıyla uluslararası işbirliklerinin artması ve

---

[557] James Wood Forsyth Jr., "What Great Powers Make It: International Order and The Logic of Cooperation in Cyberspace", *Strategic Studies Quarterly*, Cilt 7, Sayı 1, Bahar 2013, ss. 95-98.
[558] Ronald J. Deibert & Masashi Crete-Nishihata, "Global Governance and The Spread of Cyberspace Controls", *Global Governance*, Cilt 18, Sayı 3, 2012, s. 345.
[559] Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable", *Strategic Studies Quarterly*, Cilt 9, Sayı 2, Yaz 2015, s. 79.

ilerletilmesiyle birlikte kurallar ve standartlar üzerinde mutabık kalınmakta ve sanal alanda uluslararası siber güvenin tesis edilmesi söz konusu olmaktadır.[560]

Diğer taraftan siber alandaki kritik altyapı güvenliği ile ilgili tartışmaların merkezinde etkili yönetişim konuları yer almaktadır. Bu bağlamda hem hükümetlerin hem de özel sektör kuruluşlarının sahip oldukları siber güvenlik yeteneklerini geliştirmesi gerekmektedir. Dolayısıyla özel sektörün güvenlik endüstrisiyle birlikte hükümet düzenlemelerinin ve işbirliklerinin dünya genelindeki kritik altyapıların savunulmasında hayati önemi bulunmaktadır. Dahası, küresel bir siber savunma yeteneğinin gerçekleştirilebilmesi ancak devletler arasında uluslararası işbirliği yoluyla elde edilebilir.[561] Öte yandan uluslararası hukukun siber alana uygun şekilde tasarlanma girişimlerinin iç politikalarla uyumlu hale getirilmesi, açık ve somut uluslararası kurumsal işbirlikleriyle desteklendiğinde başarılı olabilir. Teknolojinin karmaşıklığı, değişim hızı ve sosyal konuların önemi göz önüne alındığında, özel sektörün ve kamu yetkililerinin kendi başlarına yaptığı düzenlemelerin yetersizliği, kamu-özel işbirliklerinin uluslararası bağlamdaki etkili düzenleyici programları sayesinde ortadan kaldırılabilir.[562] Bu açıdan kurallar, yasalar, normlar ve kurumlar, merkezi otorite olmasa bile aktörlerin iradelerinin bastırılması ve işbirliğinin kolaylaştırılması adına son derece değerli prosedürel davranış biçimleridir. Siber alan içerisinde çatışmaların önlenebilmesi ya da minimize edilebilmesi ve düzenin inşa edilerek korunabilmesi için uluslararası kuruluşlar, işbirlikleri, normatif sözleşmeler gibi Siber Uluslararası İlişkilerin söz konusu prosedürel unsurları büyük önem arz etmektedir. Böyle kurumsal mekanizmalar, bir taraftan büyük güçlerin işbirliğinin dağılımsal avantajlarını yakalamak için kullandıkları araçlar olarak tanımlanırken, diğer taraftan işbirliklerinin gerçekleşebilmesi için gerekli koşullar olarak tasvir edilebilmektedir.[563] Dolayısıyla siber uzay sahasının en temel özelliğinin bir kez

---

[560] Richard Hill, "Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT", *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn 2015, s. 121.

[561] Murat Doğrul, Adil Aslan & Eyyüp Çelik, "Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism", *2011 3rd International Conference on Cyber Conflict*, Tallinn 2011, s. 35.

[562] Stephen J. Kobrin, "Territoriality and The Governance of Cyberspace", *Journal of International Business Studies*, Cilt 32, Sayı 4, 2001, s. 697.

[563] Lucas Kello, *The Virtual Weapon and International Order*, Yale University Press, New Haven & Londra 2017, ss. 84-85.

daha vurgulanmasında fayda bulunmaktadır: Siber alan, devletlerin önceden var olan rekabetçi veya çatışan çıkarlarını takip edebileceği pasif bir alan değil, aksine hızla değişen teknolojiler ve uygulamalarla hem çatışmalar hem de işbirlikleri için fırsatlar yaratan dinamik bir alandır.[564] Söz konusu dinamizm içerisinde prosedürel standart mekanizmasının oluşturabilmesi oldukça zor olmakla birlikte siber aktörlerin uzmanlarla bir araya gelebildikleri uluslararası forum ortamlarında geliştirdikleri ortak çalışmalar ve işbirlikleriyle gerçekleşebilmektedir. Bu bağlamda bölgesel ve küresel nitelikte öne çıkan başlıca işbirliği girişimleri şu şekildedir: Uluslararası Telekomünikasyon Birliği (*International Telecommunication Union*, ITU)[565]; İnternet Tahsisli Sayılar ve İsimler Kurumu (*Internet Corporation for Assigned Names and Numbers*, ICANN)[566]; İnternet Yönetişim Forumu (*The Internet Governance Forum*, IGF)[567]; Avrupa Ağ ve Bilgi Güvenliği Ajansı (*The European Union Agency for Cybersecurity*, ENISA)[568]; NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (*The NATO Cooperative Cyber Defence Centre of Excellence*, NATO CCD-CoE)[569]; İnternet Topluluğu (*Internet Society*, IS)[570]; Asya Pasifik Bilgisayar Olaylarına Müdahale Ekibi (*Asia Pacific Computer Emergency Response Team*, APCERT)[571].

---

[564] Roger Hurwitz, "Depleted Trust in the Cyber Commons", *Strategic Studies Quarterly*, Cilt 6, Sayı 3, Cyber Special Edition, Güz 2012, s. 21.

[565] International Telecommunication Union (ITU), "About International Telecommunication Union (ITU)", *https://www.itu.int/en/Pages/default.aspx*, (Erişim Tarihi: 1 Nisan 2020).

[566] Internet Corporation for Assigned Names and Numbers (ICANN), "About ICANN", *https://www.icann.org/resources/pages/welcome-2012-02-25-en*, (Erişim Tarihi: 1 Nisan 2020).

[567] The Internet Governance Forum (IGF), "About the IGF", *https://www.intgovforum.org/multilingual/tags/about*, (Erişim Tarihi: 1 Nisan 2020).

[568] European Union Agency for Cybersecurity (ENISA), "About ENISA", *https://www.enisa.europa.eu/about-eni*sa, (Erişim Tarihi: 1 Nisan 2020).

[569] The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD-CoE), "About Us", *https://ccdcoe.org/about-us/*, (Erişim Tarihi: 1 Nisan 2020).

[570] Internet Society (IS), "About Internet Society", *https://www.internetsociety.org/about-internet-society/*, (Erişim Tarihi: 1 Nisan 2020).

[571] Asia Pacific Computer Emergency Response Team (APCERT), "About APCERT", *https://www.apcert.org/about/index.html*, (Erişim Tarihi: 1 Nisan 2020).

4.2.1. Uluslararası Telekomünikasyon Birliği (*The International Telecommunication Union*, ITU)

Uluslararası Telekomünikasyon Birliği (ITU), ilk uluslararası telgraf ağlarının yönetilebilmesi için 17 Mayıs 1865 tarihinde Paris'te imzalanan "Uluslararası Telgraf Sözleşmesi"ndeki (*International Telegraph Convention*) yapılacak değişiklikleri denetlemek ve birlikte çalışabilirliği sağlamak amacıyla "Uluslararası Telgraf Birliği" (*International Telegraph Union*) adıyla kurulmuştur.[572] ITU'nun tarihsel evrimi dört ana süreçte gerçekleşmiştir: 1) 1865-1934 tarihleri arasında telgraf alanında başlayıp radyo alanında devam eden uluslararası işbirliği çabalarının olduğu dönem; 2) 1934'ten başlayıp II. Dünya Savaşı sonuna kadar geçen, radyo teknolojisinde ve kullanımında hızlı değişimlerin yaşandığı ancak ITU aktivitelerinin yetersiz kaldığı dönem; 3) ITU'nun radyo ve radyo frekans spektrumu çalışmalarına hâkim olduğu, 1947 Atlantic City Konferansları ile başlayıp 1965 Montreux Tam Salahiyetli Murahhaslar Konferansına kadar yeniden düzenlendiği dönem; 4) 1965'ten günümüze kadarki telekomünikasyon ve bilgisayar teknolojilerinin birleşmesini ve uydu iletişiminin ortaya çıkmasını kapsayan dönem.[573] Bu dönemler içerisinde ITU'nun yapısının ve faaliyetlerinin, değişen koşul ve yetkilerin ihtiyaçlarını karşılayabilecek şekilde dönüşüm yaşadığı tarih 15 Ekim 1947 olmuş ve BM'ye bağlı faaliyet yetkisi olan, devletlerarası hukuk tüzel kişiliğine sahip bir uzmanlık kuruluşuna evrilmiştir.[574]

İletişim ağlarında uluslararası bağlantının daha kolay ve pratik hale gelmesini hedefleyen ITU, küresel radyo spektrumu ve uydu yörüngeleri tahsis etmekte, ağların ve teknolojik sistemlerin sorunsuz şekilde birbirine bağlanabilmesini sağlayan teknik standartlar geliştirmekte ve dünya çapında yetersiz hizmet alan –dijital uçurum[575]–

---

572 International Telecommunication Union (ITU), "Discover ITU's History", *https://www.itu.int/en/history/Pages/DiscoverITUsHistory.aspx*, (Erişim Tarihi: 2 Nisan 2020).

573 George A. Codding, Jr., "Evolution of the ITU", *Telecommunications Policy*, Cilt 15, Sayı 4, Ağustos 1991, s. 271.

574 Bilgi ve İletişim Teknolojileri Kurumu, "Uluslararası Telekomünikasyon Birliği-ITU", *https://www.btk.gov.tr/itu*, (Erişim Tarihi: 2 Nisan 2020).

575 Dijital Uçurum/Dijital Boşluk (*Digital Divide*): Bireyler ve toplumlar arasında "Bilgi Çağı"na katılabilecek bilgi ve iletişim teknolojileri kaynaklarına sahip olanlar ile olmayanlar arasındaki farkı içermektedir. Aynı zamanda da gelişmekte olan ve gelişmiş ülkeler arasındaki standartlaşma boşluğunu vurgulamaktadır. Dünyanın çevrimiçi nüfusunun büyüklüğü hakkında güvenilir veri olmamasına rağmen yapılan çalışmalara ve geliştirilen tahminlere göre dünya nüfusunun yaklaşık %58,7'sinin İnternete erişimi varken, %40'ından fazlasının henüz İnternete erişimi bulunmamaktadır.

toplulukların BİT'lere erişebilmesi ve iletişim haklarının korunması için çalışmaktadır. Küresel kamu-özel sektör ortaklıkları için eşsiz bir platform olan ITU'nun üyeliği kapsamında 193 devletin yanı sıra yaklaşık 900 şirket ve çok sayıda üniversite, uluslararası ve bölgesel kuruluş bulunmaktadır. ITU, bilgi ve iletişim teknolojileri ekosisteminde en geniş ağa sahip oluşum olarak dikkat çekmektedir.[576] Birliğin yapısına bakıldığında esaslı çalışmaların üç sektör biriminin gözetimi altında gerçekleştiği görülmektedir: Frekans spektrumunun yanı sıra yerdurağan uyduların konumlarını yönetme sorumluluğuyla görevli "Radyokomünikasyon Sektörü" (*The Radiocommunication Sector,* ITU-R); İletişim teknolojilerinin, operasyonlarının ve tarifelerinin belirli standartlara oturtulmasından sorumlu "Telekomünikasyon Standardizasyon Sektörü" (*The Telecommunication Standardization Sector,* ITU-T); BM'nin uzman bir birimi olarak ITU'nun sorumluluklarını koordine etmekten sorumlu "Telekomünikasyon Geliştirme Sektörü" (*The Telecommunication Development Sector,* ITU-D).[577]

ITU'nun en dikkat çekici girişimlerinin başında, bilgi toplumunda güven ve güvenliğin arttırılmasını amaçlayan uluslararası işbirliği için 2007 yılında geliştirilen "ITU Küresel Siber Güvenlik Gündemi" (*The ITU Global Cybersecurity Agenda*, ITU GCA) çerçevesi gelmektedir. İşbirliği ve verimlilik için tasarlanan bu çerçeve; yasal önlemler, teknik ve prosedürel önlemler, organizasyon yapıları, kapasite geliştirme ve uluslararası işbirliği olmak üzere beş ana alandan oluşmaktadır.[578] Bu bağlamda görevi kolektif siber güvenliğin ilerletilmesine yönelik yaklaşımlar tanımlamak olan bir Üst Düzey Uzmanlar Grubu (*High Level Experts Group*) oluşturulmuş ve siber suçlarla ilgili raporlar hazırlanarak, Avrupa Konseyi Siber

---

Detaylı bilgi için bkz.: Internet World Stats, "Internet Usage Statistics: World Internet Users and 2020 Population Statas", *https://www.internetworldstats.com/stats.htm*, (Erişim Tarihi: 2 Nisan 2020).; Wenhong Chen & Barry Wellman, "The Global Digital Divide – Within and Between Countries", *IT & Society*, Cilt 1, Sayı 7, Yaz 2004, s. 19.

[576] International Telecommunication Union (ITU), "About International Telecommunication Union (ITU)", *https://www.itu.int/en/Pages/default.aspx*, (Erişim Tarihi: 2 Nisan 2020).

[577] Lawrence D. Roberts, "A Lost Connection: Geostationary Satellite Networks and The International Telecommunication Union", *Berkeley Technology Law Journal*, Cilt 15, Sayı 3, Güz 2000, s. 1109.

[578] International Telecommunication Union (ITU), "About GCA", *https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx*, (Erişim Tarihi: 2 Nisan 2020).; Hamadoun I. Touré, *Report of the Chairman of High-Level Experts Group (HLEG)*, ITU Global Cybersecurity Agenda (GCA), Mossi Norveç 2008, s. 2.

Suçlar Sözleşmesi'ne katılımın genişlemesi hedeflenmiştir.[579] ITU'nun bu tarz girişimleri ve çalışmaları, tarihi doğrultusundaki küresel politika ilkeleri bağlamında sürmektedir. Bilgi ve tecrübelerin paylaşılarak, toplu eylem, uluslararası işbirliği koordinasyonu, düzenlemelere yönelik ulusal ve bölgesel yaklaşımlarla büyümeye devam etmektedir.[580] Bilgi ve iletişim teknolojileri ortamında en fazla saygı duyulan hükümetlerarası organizasyonların başında gelmektedir ve belirleyiciliğini sürdürmektedir.

4.2.2. İnternet Tahsisli Sayılar ve İsimler Kurumu (*The International Corporation for Assigned Names and Numbers*, ICANN)

İnternetin giderek yayılması ve özellikle ticarileşmesi, alan adlarının (*domain names*) İnternette tanınabilir varlık sağlaması nedeniyle küresel ekonomik kaynaklar olarak değerinin ve öneminin artmasına vesile olmuştur. 1990'ların ortalarından itibaren ise alan adlarının tahsisi ve yönetim sistemi üzerindeki kontrol, küresel ekonomi-politik önemi olan bir konu haline gelmiştir.[581] Bunun sonucunda da 1998 yılında kar amacı gütmeyen çok paydaşlı bir özel sektör kurumu olarak "İnternet Tahsisli Sayılar ve İsimler Kurumu" (*The International Corporation for Assigned Names and Numbers*, ICANN) kurulmuştur.[582] ICANN, İnternetin alan adı ve adres atamalarının merkezi koordinasyonunu ilk olarak ABD Hükümeti ile yapılan sözleşme gereği iki yüklenici firma üzerinden gerçekleştirmiştir: Kaliforniya Üniversitesi'nde bilgisayar bilimcisi ve aynı zamanda İnternetin öncülerinden olan Jon Postel yönetimindeki "İnternet Tahsisli Sayılar Otoritesi" (*Internet Assigned Numbers Authority*, IANA) ve "Network Solutions".[583] Günümüzde IANA'nın

---

[579] Stephen D. McDowell, Zoheb Nensey & Philip E. Steinberg, "Cooperative International Approaches to Network Security: Understanding and Assessing OECD and ITU Efforts to Promote Shared Cybersecurity", Editörler: Jan-Frederik Kremer & Benedikt Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer-Verlag, Berlin Heidelberg 2014, s. 246.

[580] Jamal Shahin, "The European Union's Performance in the International Telecommunication Union", *European Integration*, Cilt 33, Sayı 6, Kasım 2011, s. 688.

[581] George Christou & Seamus Simpson, "Gaining a Stake in Global Internet Governance: The EU, ICANN and Strategic Norm Manipulation", *European Journal of Communication*, Cilt 22, Sayı 2, 2007, ss. 148-149.

[582] Marion G. Ben-Jacob, "Global Perspectives on Internet Regulation", *GSTF Journal of Computing (JoC)*, Cilt 6, Sayı 1, 2018, s. 2.

[583] Milton Mueller, John Mathiason & Hans Klein, "The Internet and Global Governance: Principles and Norms for a New Regime", *Global Governance*, Cilt 13, Sayı 2, 2007, s. 238.

işlevini de gerçekleştiren ICANN, İnternetin temel adres defteri olan "Alan Adı Sistemi"nin (*Domain Name System*, DNS) devam eden işlemleri için kritik öneme sahip teknik hizmetleri –İnternet Protokolü (*Internet Protocol*, IP) adresleri tahsisi, kapsamlı üst düzey alan adı (gTLD) tescil şirketleri akreditasyonu, dünya çapında İnternetin güvenli, istikrarlı ve birlikte çalışabilir olmasını kolaylaştırıcı faktörlerin sağlanması vb.– koordine etmekte ve alan adı rekabetini teşvik edici İnternet politikalarının geliştirilmesine yardımcı olmaktadır.[584]

ICANN'ın çok paydaşlı yapısal modeli; bireylerin, ticari olmayan paydaş gruplarının, endüstrinin ve hükümetlerin toplum temelli, uzlaşmaya dayalı ve politika belirleyici yaklaşımlarında önemli roller oynamaktadır.[585] ICANN'e sınırlı katılımı olan ana paydaş "hükümetler" olmuştur. Kurumun kurulması için asıl motivasyonu kritik İnternet kaynaklarından hükümet kontrolünün kaldırılması oluşturmuştur. İlgilenen herhangi bir hükümete veya uluslararası kuruluşa üyelik açıktır ancak ICANN, esasen özel sektörü temsilen kurulmuştur. Adres kayıtlarının, ICANN ve İnternet servis sağlayıcıları arasındaki en önemli bağlantılar haline gelmesi, özel şirketlerin daha fazla destek vermesini sağlamıştır. Ayrıca fikri mülkiyet oluşturulmasıyla beraber genişleyen İnternet ekonomisinde alan adlarının kritik birer mülkiyet haline geldiği daha iyi temsil edilmiştir.[586]

ICANN, bünyesinde uluslararası ve çok paydaşlı koordinasyon ve katılım barındıran uluslararası kurumsal bir biçimdir. Fakat uluslararasılaşmanın tartışmalı doğası ve çeşitli hükümet aktörleriyle özel sektör kurumları arasındaki çekişmeli ilişki göz önünde bulundurulduğunda, İnternet yönetişim düzenlemelerini değiştirme çabalarının çoğunun altında küresel güç mücadelesi gerçeğinin olduğu ve bu nedenle ICANN yönetiminde özel sektör ve uluslararası paydaş çokluğuna rağmen ABD yönetiminin dominantlığının devam ettiği ortadadır.[587] Gelişmiş ülkeler, ABD kontrolünün aşırı olduğunu algıladıkça ve gelişmekte olan ülkeler hâlihazırda mevcut

---

[584] Internet Corporation for Assigned Names and Numbers (ICANN), "Beginner's Guide to Participating In ICANN", *https://www.icann.org/resources/pages/beginners-guides-2012-03-06-en*, (Erişim Tarihi: 2 Nisan 2020).

[585] Internet Corporation for Assigned Names and Numbers (ICANN), "ICANN's Multistakeholder Model", *https://www.icann.org/community#groups*, (Erişim Tarihi: 2 Nisan 2020).

[586] John Mathiason, *Internet Governance: The New Frontier of Global Institutions*, 1. Basım, Routledge, Oxon 2009, ss. 88-90.

[587] Laura Denardis, *The Global War for Internet Governance*, Yale University Press, New Haven & London 2014, s. 49.

olan yönetim yapılarına erişim aradıkça bu tarz kurumların üyeliği, yetkileri ve yönetimiyle ilgili uluslararası çekişmeler giderek artacaktır.[588] Yine de ICANN'ın günümüz İnternet yönetişiminde birincil yeri olan alan adı sistemindeki belirleyiciliği ve geniş katılım temsiliyle rekabeti sağlaması, uluslararası işbirliği açısından son derece değerli görünmektedir.

4.2.3. İnternet Yönetişim Forumu (*The Internet Governance Forum,* IGF)

ICANN'ın özel sektörde çok paydaşlı bir kurum olarak kurulmasına rağmen ABD Hükümeti ile sözleşme ilişkilerini sürdürmesi, ABD'nin ICANN yönetimindeki baskınlığını ve tek taraflı gözetimini sağlamıştır. Özellikle DNS kök sunucuları[589] üzerindeki ağırlığı dikkate alındığında, birçok ülke ve siber aktör tarafından bu durum rahatsız edici bulunmuştur. Buna göre de İnternet yönetişimi, sadece teknik yönetim konusu olmayıp, birçok farklı boyutu benimseyen kamu politikalarından biri haline gelmiştir.[590] 2003-2005 yılları arasında BM tarafından gerçekleştirilen devlet merkezli bir dizi diplomatik konferans serisi olan "Dünya Bilgi Toplumu Zirvesi" (*The World Summit on the Information Society*, WSIS)[591], AB ile gelişmekte olan

---

[588] Nazli Choucri, *a.g.e.*, s. 224.

[589] Alan Adı Sisteminin (DNS) en üstünde yer alan "kök sunucular" (DNS *Root Servers*), sunucu adı ve İnternet Protokolü (IP) dönüşümünün başladığı yerdir. İnternet trafiğini yönlendiren bu kök sunuculara müdahale edilmesi durumunda İnternet trafiğinin tamamen durması söz konusu olabilmektedir. Dünya üzerinde toplamda 13 adet kök sunucu bulunmaktadır ve bunların 10 tanesi ABD sınırıları içerisinde, üç tanesi ise İngiltere (Londra), İsveç (Stockholm) ve Japonya'da (Tokyo) yer almaktadır. Detaylı bilgi için bkz.: Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace*, 1. Basım, Massachusetts Institute of Technology Press, Massachusetts 2004, ss. 47-55.; İTÜ Bilgi İşlem Daire Başkanlığı (İTÜBİDB), "DNS (Domain Name System - Etki Alanı Ad Sunucusu)", *https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/dns-(domain-name-system---etki-alan%C4%B1-ad-sunucusu)*, (Erişim Tarihi: 3 Nisan 2020).; Deutsche Welle Türkçe (DW), "İnternetin Kontrolü ABD'de", *https://www.dw.com/tr/internetin-kontrol%C3%BC-abdde/a-2523743*, (Erişim Tarihi: 3 Nisan 2020).

[590] Li Yan, "Reforming Internet Governance and the Role of China", *Focus Asia: Perspectives & Analysis*, Institute for Security and Development Policy, Sayı 12, Şubat 2015, s. 2.

[591] Dünya Bilgi Toplumu Zirvesi, 2003 yılında İsviçre'de (Cenevre) ve 2005 yılında Tunus'ta (Tunus) iki aşamalı olarak gerçekleşmiştir. İlk aşamanın amacı; açık bir siyasi irade beyanı geliştirilmesi, teşvik edilmesi ve herkesin çıkarlarının yansıtıldığı Bilgi Toplumu için temellerin oluşturulması adına somut adımlar atılmasıdır. İkinci aşamanın amacı ise Cenevre'de oluşturulan Eylem Planı'nın hayata geçirilmesi, Cenevre ve Tunus belgelerinin uygulanması ve takibi, İnternet yönetişimi alanlarında anlaşmalar yapılması, sorunlara çözümler bulunması ve finansman mekanizmaları oluşturulmasıdır. Detaylı bilgi için bkz.: International Telecommunication Union (ITU), "World Summit on the Information Society: Geneva 2003-Tunis 2005", *https://www.itu.int/net/wsis/index.html*, (Erişim Tarihi: 3 Nisan 2020).; Türkiye Cumhuriyeti Cumhurbaşkanlığı, Strateji ve Bütçe Başkanlığı, Bilgi ve İletişim Teknolojileri Dairesi, "Dünya Bilgi Toplumu Zirvesi",

ülke hükümetlerinin, ABD'nin İnternet yönetişimi ve siber uzaydaki üstünlüğüne meydan okumak için bir platform sağlamış ve iletişim bilgi politikası konuları etrafında pek çok uzmanı ve akademisyeni geniş bir yelpazede seferber etmiştir.[592] WSIS, DNS kök sunucularında sadece ABD'nin değil, tüm devletlerin eşit rol ve sorumluluğa sahip olması gerektiğini belirtmiş ve "kritik internet kaynaklarının koordinasyonu ve yönetimi ile ilgili kamu politikası konularında küresel olarak uygulanabilir ilkelerin geliştirilmesi" çağrısında bulunmuştur.[593] Öyle ki, bu ilkeleri geliştirmek için önerilen mekanizmaların belirsiz olması, uluslararası düzeyde çok paydaşlı yönetişim konusunda "İnternet Yönetişim Forumu"nun (*The Internet Governance Forum*, IGF) oluşturulmasını sağlamıştır.[594] IGF, İnterneti denetlemek için güçlü, yetkili ve hükümetlerarası bir kurum isteyenler ile gözetim istemeyenler arasında bir uzlaşma yolu olarak yorumlanmıştır. Söz konusu uzlaşma, politika sorunlarının açık ve çok paydaşlı bir ortamda tartışılması halinde hükümetler, özel sektör ve sivil toplum arasında oluşturulabilecek ortaklığın başarabileceği bir düzene yol açabileceği ilkesine dayandırılmıştır.[595] Bu bağlamda Tunus Zirvesi Nihai Dokümanı'nın 77. Maddesinde IGF'nin yapısı; "gözetim işlevi olmayan, mevcut düzenlemelerin, mekanizmaların, kurumların veya organizasyonların yerini almayan ancak bunları süreçlere dâhil eden ve uzmanlıklarından yararlanan, tarafsız, tekrarlayıcı olmayan ve bağlayıcılığı bulunmayan"[596] şeklinde tanımlanmıştır.

2006 yılında ilk IGF organize edilmiş ve o zamandan beri yıllık olarak toplanmaya devam etmiştir. Paydaşları tarafından gerekli ve önemli bir diyalog alanı olarak tanımlanan IGF'nin küresel yıllık toplantılarının başarılı olmasıyla birlikte

---

http://www.bilgitoplumu.gov.tr/uluslararasi-calismalar/dunya-bilgi-toplumu-zirvesi/, (Erişim Tarihi: 3 Nisan 2020).

[592] Michel JG van Eeten & Milton Muller, "Where is the Governance in Internet Governance?", *New Media & Society*, Cilt 15, Sayı 5, 2012, s. 724.

[593] World Summit on the Information Society, "Tunis Agenda For The Information Society", Madde 68-69-70, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 Kasım 2005, *https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html*, (Erişim Tarihi: 3 Nisan 2020).

[594] Milton Mueller, John Mathiason & Hans Klein, *a.g.m.*, s. 242.

[595] John Mathiason, *a.g.e.*, s. 126.

[596] World Summit on the Information Society, "Tunis Agenda For The Information Society", Madde 77, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 Kasım 2005, *https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html*, (Erişim Tarihi: 3 Nisan 2020).

ulusal ve bölgesel IGF'lerin oluşturulması da teşvik edilmiştir.[597] Böylelikle uluslararası toplum tarafından İnternet ve teknolojilerle ilgili kilit konular tanımlanmış ve ilgili politika kararları şekillendirilmiştir. IGF'nin esas önemi; hükümetler, hükümetlerarası kuruluşlar, özel sektör, teknik topluluklar ve STK'lar arasındaki İnternet yönetişimi ile ilgili kamu politikası sorunlarıyla ilgilenen söylemi kolaylaştırma yeteneğinde yatmaktadır. Üyelik merkezli bir oluşum yerine açık bir forum olan IGF, gerçekleştirdiği etkinliklerle siber alana dair düzenleyici çerçeveler, potansiyel riskler ve küresel eğilimler konularında paydaşları arasında bilinçli bir tartışma ortamı yaratmakta ve işbirlikleri oluşturmaktadır. Görev süresi beşer yıllık periyotlar –2006-2010, 2011-2015– halinde BM tarafından belirlenen IGF, 2015 yılındaki WSIS+10 incelemesiyle birlikte 10 yıllık –2016-2025– uzatılmıştır.[598]

Netice olarak IGF, kuruluşundan bugüne dek, siber uzay ortamında ve hükümetlerarası aygıtlarda yaşanan farklı karar alma süreçleri ve otorite kültürleri arasındaki çözülememiş sorunların aracısı olmuştur. Aynı zamanda, paydaşların ideolojileri ve ekonomik felsefelerinin yanı sıra çok sayıda farklı dünya görüşünü, kültürel, ulusal ve kurumsal kimliği bir araya getirmiştir.[599] Siber uzayın karmaşık ve dinamik yapısının yönetişim ilkelerinin ve çalışma fonksiyonlarının anlaşılabilmesi açısından IGF, son derece önemli bir platformdur. Devletler ve diğer kurumlar ile geliştirmeye devam ettiği etkileşimler sayesinde İnternet yönetişiminin verimli hale getirilerek, bu alanda güvenlik ve istikrarın sağlanması hususlarında ciddi katkılar sağlamaktadır. Böylece küresel müşterek olarak siber uzay sahasında uluslararası düzen inşa edilebilmesi için siber aktörlerin ilkeler üzerinde mutabakata varma gerekliliğinin ne şekillerde yapılabileceğinin görülebilmesi ve idrak edilebilmesi adına değerli fırsatlar yaratılmaktadır.

---

[597] Jean-Marie Chenou & Roxana Radu, "Global Internet Policy: A Fifteen-Year Long Debate", Editörler: Roxana Radu, Jean-Marie Chenou & Rolf H. Weber, *The Evolution of Global Internet Governance: Principles and Policies in the Making*, Springer-Verlag, Berlin Heidelberg 2014, s. 10.

[598] Internet Governance Forum (IGF), "About IGF FAQs", *https://www.intgovforum.org/multilingual/content/about-igf-faqs*, (Erişim Tarihi: 3 Nisan 2020).

[599] Dmitry Epstein, "The Making of Institutions of Information Governance: The Case of the Internet Governance Forum", *Journal of Infromation Technology*, Cilt 28, Sayı 2, 2013, s. 140.

ÜÇÜNCÜ BÖLÜM

SİBER ULUSLARARASI İLİŞKİLER ÖRNEK OLAYLARI

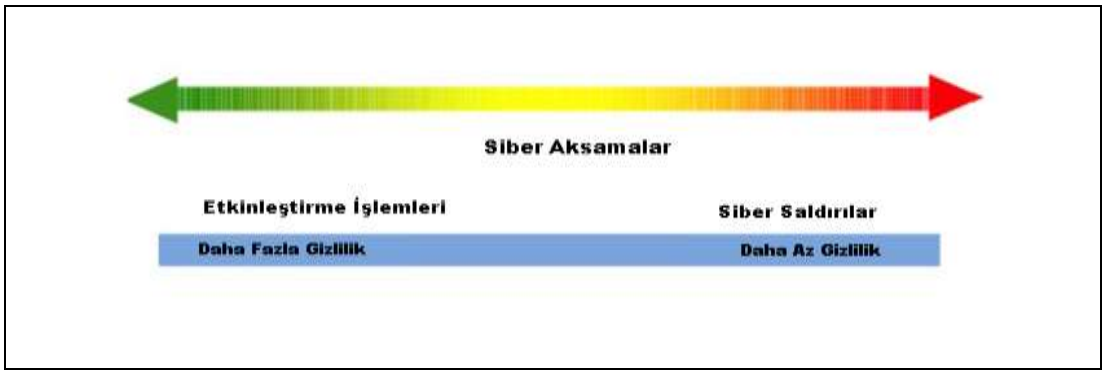
21. yüzyıl, Uluslararası İlişkilerde siber operasyonların konumunun ve belirleyiciliğinin giderek arttığı bir süreç olmaktadır. Siber operasyonlar devam ettikçe, küresel değişimler ve dönüşümler hızlanmakta, etki boyutları genişlemekte, güvenlik algısı ve çatışmanın doğası, yaşanan gelişmelerden doğrudan etkilenebilir hale gelmektedir. Siber uzay sahasının belirsiz ve karmaşık yapısı, saliseler içerisinde birçok kaynaktan çoklu eylemlerin gerçekleşebilmesine imkân sağlayabilmektedir. Beşinci stratejik alan olarak kabul edilen siber uzayın içerdiği aktör çeşitliliği de bu karmaşık yapıya eklendiğinde, söz konusu saha içerisindeki operasyonların karakterize edilebilmesinin giderek zorlaştığı görülmektedir; çünkü bir siber eylemin etkileri onu saldırı gibi gösteriyorsa, o eylemi gerçekleştiren aktörün amacı sadece casusluk yapmak olsa bile, kurban tarafından doğrudan saldırı olarak tanımlanabilmekte ve karşı önlem ya da karşı saldırılar gerçekleşebilmektedir. Öte yandan Uluslararası İlişkilerin tüm yönleriyle dinamik olarak siber alana eklemlenmesiyle birlikte mevcut baskın aktör olan devletlerin, ortaya çıkan bu yeni Siber Uluslararası İlişkiler sahasını uluslararasılaştırma ve egemenliklerini güçlendirme çabaları söz konusu olmuştur; ancak genişletilmiş ve çoğunlukla öngörülemeyen bu eylem alanının yaratacağı zorlukların devletlerce ne ölçüde karşılanacağı, sahip oldukları siber yeteneklere göre değişim göstermektedir.[600] Dolayısıyla bir devletin düşmanca bir siber olaya tepki göstermesi; olayın suç davranışı niteliği, devlet-dışı aktör boyutu, hükümet yaptırım faaliyeti vb. sonuçları olup olmadığına bağlı olarak değişebilmektedir.

Diğer taraftan Tablo-26'daki Siber Uzay Operasyonları Spektrumu'na bakıldığında; gizlilik ve saldırganlık seviyelerine bağlı olarak siber operasyonların tespit ve tanımlama kategorizasyonu söz konusu olmaktadır. Buna göre potansiyel siber operasyonlar neredeyse tespit edilemez seviyelerde olabilir. Üstelik gelecekte planlanan suç, casusluk ya da askeri faaliyetleri kolaylaştırabilecek çeşitli

[600] Andreas Wenger, "The Internet and the Changing Face of International Relations and Security", *Information & Security: An International Journal*, Cilt 7, 2001, s. 7.

motivasyonlar adına bir sisteme erişmek için tasarlanabilirler. Bu erişim işlemlerinin bir süreliğine veya asla fark edilmemesi sağlanabilir. Ek olarak; bilgisayar sistemlerinin ve ağlarının işlevselliği olumsuz yönde etkilenebilir ve hatta sistem ya da bileşenleri yok edilebilir. Dolayısıyla siber operasyonların saldırganlığı ve yıkıcılığı, onu fark edilebilir kılmaktadır ancak ortaya çıkan sorunların kaynağı her zaman belirgin olmayabilir. Bu nedenle siber operasyonların "erişim", "aksama" ve "saldırı" şeklinde üç geniş kategorizasyonu söz konusu olmaktadır.[601]

Tablo-26: Siber Uzay Operasyonları Spektrumu



Kaynak: Gary D. Brown & Owen W. Tullos, "On The Spectrum of Cyberspace Operations", Small Wars Journal, 11 Aralık 2012, *https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations*, (Erişim Tarihi: 10 Nisan 2020).

Siber eylemlerin ve olayların etkileri, onların nasıl karakterize edildiklerini ve yukarıdaki spektrum üzerinde nereye düştüklerini belirlemektedir. Yaygınlaşan İnternet kullanımı ve genişleyen siber uzay sahası, bu spektrum üzerinde yer alan operasyon sayısının muazzam boyutlara ulaşmasına vesile olmuştur. Öyle ki devletler, siber güvenlik açıklarının sadece ulusal ağların değil, vatandaşların günlük rutin faaliyetlerinin güvenliğini de doğrudan etkileyebileceğinin farkına varmaktadır.[602] Dolayısıyla artan ve çeşitlenen Siber Uluslararası İlişkiler güvensizlikleri, hükümetlerin kaynaklarını siber eylemlere karşı kendilerini savunma

[601] Gary D. Brown & Owen W. Tullos, "On The Spectrum of Cyberspace Operations", Small Wars Journal, 11 Aralık 2012, *https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations*, (Erişim Tarihi: 10 Nisan 2020).
[602] Nazli Choucri, *a.g.e.*, ss. 159-160.

ve saldırgan operasyonlar başlatma yeteneklerine kanalize etmeye giderek artan bir şekilde yönlendirmektedir.[603]

Bu bölümde; Siber Uluslararası İlişkiler örnek olaylarının daha iyi idrak edilebilmesi adına öncelikle kötü amaçlı yazılımlar (*malwares*) ve türleri –virüsler (*viruses*), solucanlar (*worms*), truva atları (*trojan horses/trojans*), botlar ve botnetler (*bots & botnets*), casus yazılımlar (*spywares*)– tanımlanacak, ardından siber olayların sınıflandırılması kapsamında popüler siber saldırı teknikleri –Keşif Saldırıları (*Reconnaissance Attacks*), Erişim Saldırıları (*Access Attacks*), Hizmet Engelleme Engelleme Saldırıları (*Denial of Service Attacks*, DoS) ve Dağıtılmış Hizmet Engelleme Saldırıları (*Distributed Denial of Service Attacks*, DDoS)– açıklanacak, sonrasında siber olaylar tarihinin safhaları belirtilecek ve nihayetinde de 21. yüzyılın öne çıkan en önemli Siber Uluslararası İlişkiler örnek olayları detaylı olarak analiz edilecektir.

1. Kötü Amaçlı Yazılımlar (*Malwares*)

Kötü Amaçlı Yazılımlar (*Malwares*), bilgisayarlara ve bilgisayar sistemlerine zarar vermek veya yok etmek için tasarlanmış tüm müdahaleci yazılımların genel adı olarak tanımlanmaktadır. "*Malware*", İngilizce'de "Kötü Amaçlı Yazılım" anlamına gelen "***Mal****icious Soft****ware***" kelimelerinin kısaltılarak birleştirilmiş halidir.[604] Kötü amaçlı yazılımlar, bilgisayarların normal işlemlerinin bozulması, hassas bilgilerin ele geçirilmesi ya da özel bilgisayar ağlarına erişilmesi için kullanılmakta ve yürütülebilir kod, komut dosyaları veya çeşitli yazılımlar şeklinde görülebilmektedir.[605] Bir aygıta kötü amaçlı yazılım programı bulaştığında, kullanıcılar tarafından fark edilebilir istenmeyen davranışlar ve sistem performans düşüklüğü söz konusu olabilmektedir; çünkü kötü amaçlı yazılımlar, bilgisayar sistemlerinde ve ağlarında istenmeyen işlemci etkinliği, bellek kullanımı ve ağ trafiği oluşturabilmektedirler. Bu tarz durumlar, uygulamalarda ya da sistem genelinde

---

[603] Anthony Craig & Brandon Valeriano, "Conceptualising Cyber Arms Races", *2016 8th International Conference on Cyber Conflict (CyCon)*, 31 Mayıs-3 Haziran 2016, Tallinn, s. 142.
[604] Cisco, "What Is Malware?", *https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html*, (Erişim Tarihi: 11 Nisan 2020).
[605] University of Central Arkansas, Information Technology, "What Is Malware?", *https://uca.edu/it/knowledgebase-legacy/what-is-malware/*, (Erişim Tarihi: 11 Nisan 2020).

çökme tarzı işlevsel süreklilik sorunları yaratabilmektedir. Diğer taraftan, kötü amaçlı yazılımların kullanıcılar tarafından fark edilememesi durumlarında söz konusu işlevsel sorunların kaynağı olarak yazılım kusurları veya donanım sorunları gibi hatalı varsayımlar üretilebilmektedir. Dahası, işlevsel olarak aygıt performansında algılanabilir değişikliklere neden olmaksızın kötü amaçlı yazılımların bulaşma durumu da bulunmaktadır ve çoğunlukla gayri meşru amaçlar – potansiyel olarak değerli ticari, kişisel, finansal verilerin gözlenmesi ya da çalınması vb.– için bu yol tercih edilmektedir.[606]

Yazılımlar, gerçek özelliklerinden ziyade içerik oluşturucularının amaçlarına göre kötü amaçlı yazılım olarak tanımlanmakta ve kabul edilmektedirler. Özellikle organize İnternet suçları üzerinden maddi kazançlar elde edilebilmesi, kötü amaçlı yazılımların her geçen gün artmasına neden olmaktadır. Öyle ki, başlangıçta şaka amaçlı ya da deneysel olarak yaratılan bu yazılımlar, günümüzde hedeflenen cihazların ve sistemlerin zarar görmesi, imha edilmesi gibi vandalist amaçlara hizmet etmektedir.[607] Kötü amaçlı yazılım bulaşmalarının çoğu dikkatsizlikle veya yanlışlıkla bu yazılımların indirilmesine neden olan eylemler üzerinden gerçekleşmektedir. E-posta bağlantılarına tıklanması, kötü amaçlı çevrimiçi sitelerin ziyaret edilmesi, geniş tabanlı sitelerden paylaşım dosyaları indirilmesi, mobil cihazlara gönderilen kısa mesajların okunması, taşınabilir belleklerin kontrolsüz kullanımı, reklam tıklamaları, sahte yazılım yüklemeleri gibi çok çeşitli ve kapsamlı şekillerde kötü amaçlı yazılımların bilgisayarlara ve ağlara bulaşması söz konusu olmaktadır.[608]

Kötü amaçlı yazılımlar, siber uzay sahasının en tehlikeli silahlarıdır ve siber aktörlerin büyük kayıplar yaşamalarına neden olmaktadır. 21. yüzyıl itibariyle kötü amaçlı yazılım endüstrisi, büyük ve iyi organize olmuş bir pazar haline gelmiştir. Bilhassa iyi finanse edilen çok uluslu kuruluşlar, geleneksel koruma anlayışının aksine yüksek teknolojilere ve yeteneklere büyük yatırımlar yaparak kötü amaçlı yazılımlardan koruma mekanizmaları geliştirmektedirler; ancak potansiyel kötü

---

[606] Jarno Niemelä, Mikko Hyppönen & Santeri Kangas, "Malware Protection", *U.S. Patent No. 9,501,644*, 22 Kasım 2016, s. 6.
[607] Norton, "What Is Malware and How Can We Prevent It?", *https://us.norton.com/internetsecurity-malware.html*, (Erişim Tarihi: 11 Nisan 2020).
[608] Avast, "How Does Malware Work?", *https://www.avast.com/c-malware*, (Erişim Tarihi: 11 Nisan 2020).

niyetli amaçlar için değerlendirilebilecek veri miktarının çok fazla olması ve kötü amaçlı yazılımların sürekli olarak geliştirilmesi ve değiştirilmesi, siber alanda güvenliğin her zaman büyük bir açık olarak görülmesini sağlamaktadır.[609]

Kötü amaçlı yazılımların davranış biçimleri, nasıl tetiklendikleri ve nasıl yayıldıklarıyla karakterize edilen çeşitli formları bulunmaktadır: Virüsler (*Viruses*), Solucanlar (*Worms*), Truva Atları (*Trojan Horses/Trojans*), Botlar & Botnetler (*Bots & Botnets*), Casus Yazılımlar (*Spywares*), Reklam Destekli Yazılımlar (*Adwares*), Şantaj Yazılımları (*Ransomwares*), Rootkit Yazılımlar (*Rootkits*).[610]

1.1. Virüsler (*Viruses*)

"Bilgisayar Virüsü" (*Computer Virus*) terimi, biyolojik anlamdaki virüsten türetilmiş ve fonksiyonellik açısından benzerlikler taşıyan bir kavramdır. Latincede "zehir" anlamına gelen "virüs" (*vīrus*) kavramı, içeriklerini çok daha büyük bir organizmanın hücresine enjekte ederek biyolojik viral enfeksiyonların yayılmasını sağlamakta ve hücrelerin virüs kopyaları üreten biyolojik bir fabrikaya dönüşmesine vesile olmaktadır.[611] Bilgisayar virüsleri de tıpkı biyolojik virüslerde olduğu gibi kendisinin bir kopyasını ekleyerek ve başka programların parçası haline gelerek yayılan ve enfeksiyonlar bırakan kötü amaçlı yazılım türlerindendir. Virüsler, verilere ya da yazılımlara ve hizmet engelleme (DoS) koşullarına neden olma şiddeti bakımlarından çeşitlilik gösterebilmektedirler. Hemen hemen tüm virüsler yürütülebilir bir dosyaya eklenmektedirler. Dolayısıyla kullanıcı tarafından ana bilgisayardaki kötü amaçlı yazılım veya program çalıştırılana kadar virüsler aktif olmamakta ve yayılmamaktadır. Buna karşın, ne zaman ana bilgisayar kodu yürütülürse, virüs kodu da yürütülmüş olur ve böylelikle çeşitli programların üzerine kendi kopyalarını ekleyebilirler. Bağlı oldukları yazılım ya da belgelerin diğer bilgisayarlara ağ, disk, dosya paylaşımı veya e-posta eki şeklinde aktarılmasıyla

---

[609] Royi Ronen, Marian Radu, Corina Feuerstein, Elad Yom-Tov & Mansour Ahmadi, "Microsoft Malware Classification Challenge", *CoRR*, abs/1802.10135, 2018, s. 1.

[610] Kaspersky, "Types of Malwares", *https://www.kaspersky.com/resource-center/threats/malware-protection*, (Erişim Tarihi: 11 Nisan 2020).

[611] Eugene H. Spafford, "Computer Viruses as Artificial Life", *Artificial Life*, Cilt 1, Sayı 3, 1994, s. 250.

virüslerin yayılması sağlanır.[612] Grip virüsleri konak hücreler olmaksızın nasıl ki çoğalamazlar, bilgisayar virüsleri de dosya veya belge gibi programlamalar olmadan asla çoğalamaz ve yayılamazlar. Virüsler, kendi kodlarını yürütmek için makro unsurları destekleyen meşru programlara ya da belgelere eklenerek çalışırlar ve bu süreçte verilerin bozulması, yok edilmesi, zarar görmesi gibi etkilere neden olabilecek potansiyele sahiptirler.[613] Bu bağlamda virüslerin en fazla öne çıkan özelliği; tamamen kendi iradeleriyle çalışamıyor olmalarıdır. Genellikle hedeflenen bilgisayar sisteminin operatörlerinin bilgisi olmaksızın kendisini çoğaltmak ve yaymak için tasarlanmışlardır. Çalıştırılan bilgisayarların operatörlerince işlem yapma zorunluluğu, virüslerin en büyük gücü olarak tanımlanmaktadır; çünkü virüslerin kötü amaçlarının gerçekleşebilmesi, bilgisayarların normal işlemlerini sürdürmelerine bağlıdır ve bu nedenle de daha önce bilinmeyen bir viral programı tanımlamak için kullanılabilecek tek bir benzersiz özellik bulunmamaktadır.[614]

1986 yılında Pakistan'da bir bilgisayar mağazası çalıştıran iki kardeşin, korsan yazılımları engellemek adına geliştirdiği "*Brain*" isimli ilk bilgisayar virüsü, yazılım hırsızlarının disketlerinin önyükleme sektörüne bulaşacak şekilde tasarlanmış ve korsan yazılım kopyalarına enfekte olarak bilgisayarların sabit diskine yayılmıştır.[615] Bu ilk virüsten günümüze kadar yazılan tüm virüsler, "beş nesil" (*five generations*) şeklinde sınıflandırılmaktadır: Buna göre birinci nesil (basit) virüsler, basit virüslerden oluşmakta, kendilerini kopyalamaktan başka fonksiyonu bulunmamakta ve sistemdeki varlıklarını gizlememektedirler. Bu virüsler ana bilgisayarı tekrar tekrar enfekte ederek belleğin tükenmesine ve erken tespit edilmeye yol açarlar. İkinci nesil (kendini tanıyan) virüsler ise virüs bulaşmış dosyaların bu gereksiz büyümesini önlemek için dosyaya ya da sisteme bulaştığını gösteren benzersiz bir imza yerleştirirler ve bu imzayı kontrol ederek ilerlerler. Üçüncü nesil (gizli) virüsler, kendilerini gizleme yeteneğiyle önceki nesillerden

---

[612] Cisco, "What Is The Difference: Viruses, Worms, Trojans, and Bots?", *https://tools.cisco.com/security/center/resources/virus_differences*, (Erişim Tarihi: 12 Nisan 2020).
[613] Norton, "What Is A Computer Virus?", *https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html*, (Erişim Tarihi: 12 Nisan 2020).
[614] David Harley, Robert Slade & Urs Gattiker, *Viruses Revealed*, McGraw-Hill/Osborne, New York 2001, s. 59.
[615] Kaspersky, "Malware & Computer Virus Facts & FAQs", *https://www.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs*, (Erişim Tarihi: 12 Nisan 2020).

farklılık göstermektedirler. Buna göre ikincil depolamanın taranması ve her bir virüse özgü veri deseni araması, önceki nesil virüslerin tanımlanabilmesini sağlamaktadır. Üçüncü nesil virüsler etkin olduklarında, seçilen sistem hizmeti çağrısı kesintilerini bozmakta ve bu işlemleri gerçekleştirme isteklerini durdurmaktadır. Dördüncü nesil (zırhlı) virüsler, virüs kodunun analiz edilmesini zorlaştıran gereksiz kod eklemeleri içermektedir ve bu virüsler etkilenen sistemde mevcutsa, anti-virüs yazılımına yönelik yönlendirilmiş saldırılar yapabilmektedir. Son olarak beşinci nesil (çok biçimli/polimorfik) virüsler, hedeflerini değiştirilmiş veya şifrelenmiş versiyonlarıyla enfekte etmektedirler. Bu virüslerin varlığının tespit edilebilmesi için şifrelemeyi tersine çeviren daha karmaşık algoritmaların kullanılması gerekmektedir.[616] Farklı nesil ve şekillerde tanımlanan virüslerin varlığı ve etki alanı, teknolojik cihaz ve kullanıcı sayısının artmasına bağlı olarak bilgisayar korsanları tarafından daha yaratıcı ve aktif hale getirilmeye devam etmektedir.

1.2. Solucanlar (*Worms*)

"Bilgisayar Solucanları" (*Computer Worms*), tek bir bilgisayardan kaynaklanan ve yerel ağ (LAN) ya da İnternet bağlantısı üzerinden diğer bilgisayarları arayan kötü amaçlı bir diğer yazılım türüdür. Bir solucan başka bir bilgisayar bulduğunda, kendisini bu bilgisayarda çoğaltır ve sonrasında kendisini çoğaltmaya devam edeceği yeni bilgisayarlar arar. Bu süreç, süresiz olarak veya bir zamanlama mekanizması söz konusu süreci durdurana kadar devam edebilir.[617] Bilgisayar solucanları, virüslere benzemektedirler çünkü kendilerinin işlevsel kopyalarını çoğaltırlar ve benzer hasarlara neden olabilirler. Öyle ki solucanlar, virüslerin aksine bağımsız yazılımlardır ve yayılmak için sunucu programı ya da insan yardımı gerektirmezler. Hedef sistemlerdeki güvenlik açıklarından yararlanarak bulaşan solucanlar, yine sistem dâhilindeki dosya aktarımı veya bilgi aktarımı özelliklerini kullanarak insan yardımı olmaksızın diğer bilgisayarlara

[616] S. Ravi Subramanya & Natraj Lakshminarasimhan, "Computer Viruses", *IEEE Potentials*, Cilt 20, Sayı 4, 2001, ss. 18-19.
[617] Michael Erbschloe, *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*, Elsevier Butterworth–Heinemann, Massachusetts 2005, s. 23.

yayılabilirler.[618] Daha spesifik olarak belirtilmesi gerekirse; bir solucanın bir cihaza bulaşabilmesi için öncelikle o cihazın var olduğunu keşfetmesi gerekmektedir. Solucanlar açısından sömürülecek yeni cihaz keşifleri için çeşitli teknikler bulunmaktadır. Tarama, harici hedef listeleri, önceden oluşturulmuş hedef listeleri, dâhili hedef listeleri ve pasif izleme, bu tekniklerin başlıcalarıdır. Ek olarak, solucanlar tarafından bu stratejilerin kombinasyonu da kullanılabilmektedir.[619] Diğer taraftan solucanlar genellikle sosyal mühendislik tekniklerini kullanırlar. Bunu yapmak için de bilgisayar korsanları tarafından kötü amaçlı dosyaları kamufle etmek amacıyla çoğunlukla ünlü insanlar, korsan yazılımlar veya cinsellikle ilgili dikkat çekici isimler tercih edilmektedir.[620] Bu tekniklere ek olarak; e-posta eki olarak gönderilen dosyalar, web kaynağı bağlantıları, anlık mesajlar, P2P dosya paylaşım ağları gibi çeşitli yollarla bilgisayar belleğine nüfuz edilebilmekte ve solucan kodu etkinleştirilebilmektedir. Ayrıca bilgisayar solucanları, ağ yapılandırma hatalarından ve işletim sistemindeki ya da uygulama güvenliğindeki boşluklardan da yararlanabilmektedirler. Birden fazla tekniği ve yöntemi aynı anda kullanabilmektedirler.[621]

Solucanların saldırıları, ağ uzmanları tarafından bilgisayar ağlarındaki en yüksek güvenlik riski olarak kabul edilmektedir. Uyarı veya kullanıcı etkileşimi olmaksızın yayılmak üzere yazılan bilgisayar solucanları, siber saldırılara yol açacak trafik hizmeti isteklerinde artışa neden olmaktadır. Saldırganlar, yazılım açıklarını hedeflemek için birincil araç olarak kötü amaçlı bir solucan kullanmayı tercih edebilmektedirler.[622] Ağ kaynaklarını hedef alan solucanlar; ağ kitlenmelerine, web kaynağı erişim hızının düşmesine ya da e-posta sunucularında aşırı yüklenmelere

---

[618] Cisco, "What Is The Difference: Viruses, Worms, Trojans, and Bots?", https://tools.cisco.com/security/center/resources/virus_differences, (Erişim Tarihi: 13 Nisan 2020).
[619] Nicholas Weaver, Vern Paxson, Stuart Staniford & Robert Cunningham, "A Taxonomy of Computer Worms", *WORM '03: Proceedings of the 2003 ACM Workshop on Rapid Malcode*, CCS03: 10th ACM Conference on Computer and Communications Security, Washington, D.C., Ekim 2003, s. 12.
[620] Panda, "What Do Computer Worms Do?", *https://www.pandasecurity.com/en/security-info/worm/*, (Erişim Tarihi: 13 Nisan 2020).
[621] Kaspersky, "What Is A Computer Virus or A Computer Worm?", *https://www.kaspersky.com/resource-center/threats/viruses-worms*, (Erişim Tarihi: 13 Nisan 2020).
[622] Bimal Kumar Mishra & Apeksha Prajapati, "Cyber Warfare: Worms' Transmission Model", *International Journal of Advanced Science and Technology*, Cilt 63, 2014, s. 83.

neden olabilmektedir.[623] Bununla birlikte, güvenlik uzmanları tarafından "Süper Solucanlar" (*Super Worms*) olarak adlandırılan ve giriş noktası belirsizliğini kullanabilecek karmaşık, çok biçimli ve başkalaşan davranış rutinlerini içerebilecek yeni solucanların ilerleyen zamanlarda yaratılabileceği ve etki boyutlarının çok daha fazla olabileceği öngörülmektedir.[624]

1.3. Truva Atları (*Trojan Horses/Trojans*)

"Truva Atları" (*Trojan Horses/Trojans*), yasal açıdan sorunlu görünmeyen ancak bilgisayarların kontrolünü ele geçirebilen kötü amaçlı yazılımlardır. Verilere veya ağlara zarar vermek, bozmak, çalmak gibi çeşitli zararlı eylemleri gerçekleştirmek üzere tasarlanmışlardır.[625] Truva atları, virüslerden ve solucanlardan farklı olarak programlanmış enfeksiyon rutini içermezler. Bu nedenle de sistemden sisteme ancak operatör kasıtlı olarak hareket etmeye ikna edilirse geçebilirler. Yani kullanıcılar açısından faydalı ve yasal açıdan sorunsuz görünen programlar, aynı zamanda kullanıcıların beklemeyeceği veya istemeyeceği eylemleri gerçekleştirebilirler.[626] Bilgisayar virüsleri ve solucanların aksine kendi kendilerini çoğaltamayan truva atları, kullanıcıları bir şekilde ikna ederek sisteme yüklenip etkinleştirildiğinde, siber suçlular tarafından gözetleme, hassas verilere ulaşma ve sistemlere arka kapı erişimleri elde etme gibi durumlar söz konusu olabilmektedir. Bu bağlamda veriler silinebilir, engellenebilir, değiştirilebilir, kopyalanabilir ya da bilgisayarların ve bilgisayar ağlarının performaslarında bozulmalar yaşanabilir.[627] Truva atları, siber-fiziksel sistemler içerisindeki entegre devrelerin (*integrated circuits*, IC) orijinal amaçlarıyla ilgisi olmayan görevleri yerine getirmek için entegre devrelere yerleşirler ve sonrasında truva atlarının entegre devre içerisindeki ekstra

---

[623] İTÜ Bilgi İşlem Daire Başkanlığı (İTÜBİDB), "Virüs, Solucan ve Truva Atı", *https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1*, (Erişim Tarihi: 13 Nisan 2020).

[624] Craig Fosnock, *Computer Worms: Past, Present, and Future CISSP*, Technical Report 8, East Carolina University, 2005, s. 6.

[625] Norton, "What Is A Trojan? Is It A Virus or Is It Malware?", *https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html*, (Erişim Tarihi: 14 Nisan 2020).

[626] David Harley, Robert Slade & Urs Gattiker, *a.g.e.*, ss. 12-13.

[627] Kaspersky, "What Is A Trojan Virus?", *https://www.kaspersky.com/resource-center/threats/trojans*, (Erişim Tarihi: 14 Nisan 2020).

kodları, belirlenen tetikleyicilere veya durumlara tepki vererek truva atlarının zararlı doğasını aktive etmektedir. Ek olarak, truva atları çok zor tanımlanabilmektedir çünkü mevcut devreler, truva atlarının varlığı ya da etkileri açısından kolayca test edilemezler.[628] Truva atları genellikle virüslü e-posta ekleri, ücretsiz oyunlar, uygulamalar, filmler veya tebrik kartları gibi ilgi çekici programlarda gizlenmektedirler.[629] Örneğin; kayıtlara geçen ilk gerçek truva atı olan "*ANIMAL-PERVADE*" isimli program, 1975 yılında basit bir hayvan temalı tahmin oyunu içerisine gizlenmiş ve oyunun indirilmesiyle birlikte mevcut kullanıcıların erişebileceği her sürücüde yedeklemeler oluşturmuş; fakat süreçlere herhangi bir zarar vermemiştir. Teknolojinin ilerlemesi ve İnternetin giderek yayılmasıyla birlikte truva atları, kısa sürede en popüler kötü amaçlı yazılım saldırılarından biri haline gelmiştir.[630] Günümüzde ise truva atlarının cihazlara yayılma hızındaki artışta özellikle sosyal kanalların manipüle edilmesinin birincil yöntem olarak kullanıldığı görülmektedir.

1.4. Botlar ve Botnetler (*Bots & Botnets*)

"Botlar" (*Bots*) veya "İnternet Robotları" (*Internet Robots*), bir arama motorunu dizine ekleme gibi tekrarlayan işleri veya bilgisayar üzerinde tam kontrol sağlanması gibi belirli görevleri insandan daha hızlı gerçekleştirebilen uygulamalardır ve "örümcekler" (*spiders*), "web botları" (*web bots*) gibi isimlerle de görülebilmektedirler.[631] Botlar bilgisayarda çalıştırıldığında, bilgisayarın kaynaklarına erişimi tıpkı bilgisayar kullanıcısı gibi olmaktadır. Örneğin; dosyalar okunabilir ve yazılabilir, programlar yürütülebilir, kameraya erişilebilir, e-posta gönderilebilir, bilgisayar kullanılamaz hale getirilerek sistem dosyaları silinebilir, dijital sertifikalar çalınabilir, bilgisayar açılıp kapatılabilir, dosyalar indirilebilir

---

[628] Hannah Vincent, Lee Wells, Pablo Tarazaga & Jaime Camelio, "Trojan Detection and Side-Channel Analyses for Cyber-Security in Cyber-Physical Manufacturing Systems", *Procedia Manufacturing*, 43rd Proceedings of the North American Manufacturing Research Institution of SME, Cilt 1, 2015, s. 80.

[629] Avast, "What Is A Trojan Horse?", *https://www.avast.com/c-trojan*, (Erişim Tarihi: 14 Nisan 2020).

[630] Joseph Regan, "What Is A Trojan Horse? Is It Malware or Virus?", AVG, 10 Aralik 2019, *https://www.avg.com/en/signal/what-is-a-trojan*, (Erişim Tarihi: 14 Nisan 2020).

[631] Norton, "What Are Bots?", *https://us.norton.com/internetsecurity-malware-what-are-bots.html*, (Erişim Tarihi: 15 Nisan 2020).

vb.[632] Çok sayıda botun birden fazla bilgisayara yayılması ve İnternet üzerinden birbirlerine bağlanmalarıyla ise "botnet" (*botnet*) adı verilen bir bot ağı oluşturulur. Botnetin üç temel unsuru vardır: Hedefleri enfekte eden ve hedef operatörlerinin bilgisi olmaksızın onları botnet parçası haline getiren "botlar"; hedeflerdeki botlara komut gönderen "botmaster"lar; ve tüm botnetin botmaster tarafından kontrolünün sağlandığı "komut ve kontrol sunucuları" (*the command and control servers*, C&C).[633] Öte taraftan botların nasıl kullanıldığına bağlı olarak iyi ve kötü olarak tanımlanmaları mümkündür. Buna göre; bilgi toplanması, anlık mesajlaşma, anlık geçiş sohbeti veya çeşitli web arayüzleriyle otomatik etkileşimler, yani web siteleriyle dinamik iletişim sağlanması, iyi bot fonksiyonlarına örnek verilmektedir.[634] Kötü amaçlı botlar ise genellikle truva atları ile solucanların uzaktan erişim kombinasyonu olarak düşünülmekte ve saldırganlara hedeflere uzaktan erişim imkânıyla birlikte solucanlar gibi yayılabilme fırsatları sunmaktadır.[635] Diğer taraftan botnet ağlarının algılanması oldukça zordur. Bunun nedeni, normal cihaz işlevlerinin bozulmaması ve operatörün uyarılmaması adına oldukça düşük hesaplama gücü kullanılmasıdır. Daha gelişmiş botnetlerde ise siber güvenlik yazılımları tarafından algılanmayı önleyebilmek için davranış güncelleme tasarlamaları bulunmaktadır.[636] Botnetler, günümüz siber uzay ortamında baskın zararlı ağlar haline gelmektedir. İnternet üzerindeki bu tarz kötü amaçlı ağların yapıları, boyutları, yayılma davranışları gibi hususların tespit edilebilmesi giderek karmaşıklaşmakta ve zorlaşmaktadır. Kötü amaçlı bot ağları, aynı anda birçok ticaret, üretim ve kontrol ağında yaygın olarak bulunabilmekte ve çok büyük boyutlarda olabilmektedir. Bot sayılarının muazzam boyutlarda olması sebebiyle güç şebekeleri, hava trafik kontrol ağları veya iletişim ağları gibi son derece önemli altyapı unsurları

---

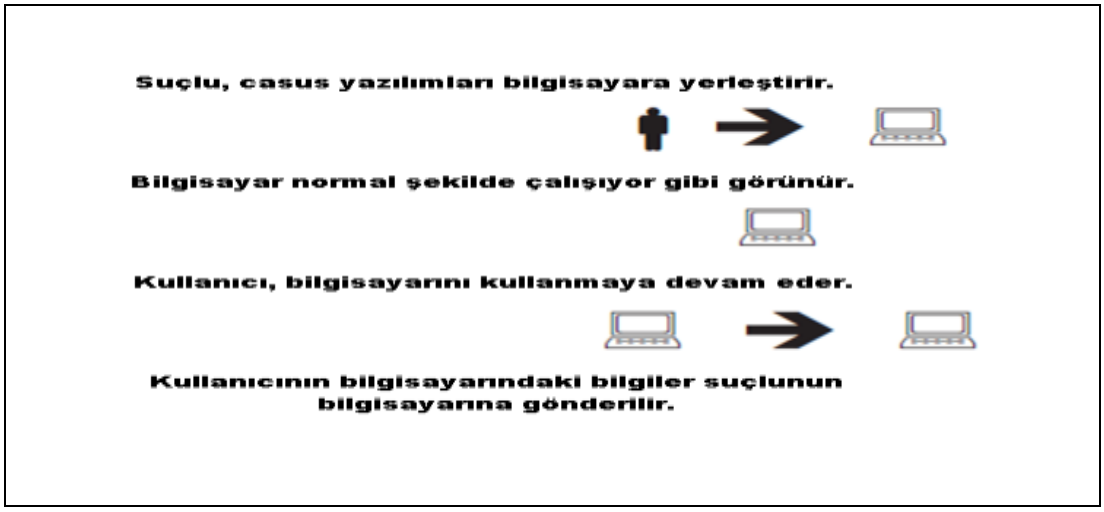
[632] European Union Agency For Cybersecurity (ENISA), "Botnets", *https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets*, (Erişim Tarihi: 15 Nisan 2020).
[633] Meisam Eslahi, Rosli Salleh & Nor Badrul Anuar, "Bots and Botnets: An Overview of Characteristics, Detection and Challenges", *2012 IEEE International Conference on Control System, Computing and Engineering*, 23-25 Kasım 2012, Penang, Malezya, s. 349.
[634] Norton, "What Are Bots?", *https://us.norton.com/internetsecurity-malware-what-are-bots.html*, (Erişim Tarihi: 15 Nisan 2020).
[635] Ken Dunham & Jim Melnick, *Malicious Bots: An Inside Look Into The Cyber-Criminal Underground of The Internet*, CRC Press, Auerbach Publications, Florida 2009, s. 2.
[636] Panda, "What Is A Botnet?", *https://www.pandasecurity.com/mediacenter/security/what-is-a-botnet/*, (Erişim Tarihi: 15 Nisan 2020).

doğrudan hedef unsuru haline gelebilmekte ve büyük zararlar alabilmektedir.[637] Dolayısıyla gelişmeye devam eden bot ve botnet tasarımları, sadece bilgisayar ağları ve İnternet için tehditler oluşturmamakta, aynı zamanda büyük saldırı türlerinin gerçekleştirilebilmesi için altyapı olarak da kullanılabilmektedirler.

1.5. Casus Yazılımları (*Spywares*)

"Casus Yazılımlar" (*Spywares*); klasik bilgisayarlar, İnternet tarayıcı uygulamaları veya mobil cihaz uygulamaları fark etmeksizin, kullanıcıların kişisel ve gizli bilgilerini, kullanıcı onayı olmadan ele geçiren kötü amaçlı yazılımlardır.[638] Genellikle virüsler ile kıyaslanan casus yazılımlar, davranış olarak virüslerden ayrılmaktadırlar. Buna göre kendilerini kopyalamak ve cihazların ağları üzerinden yaymak için bir ana programa ihtiyaç duyan virüslerin aksine casus yazılımlar, bulaştığı her aygıtta algılanamayacak şekilde tasarlanmışlardır. Üstelik bazı virüs türleri yayılırken beraberinde casus yazılımları da taşıyabilmektedirler.[639]

Tablo-27: Casus Yazılımların İşleyişi



Kaynak: Michael Erbschloe, *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*, Elsevier Butterworth–Heinemann, Massachusetts 2005, s. 26.

---

[637] Shui Yu, Guojun Wang & Wanlei Zhou, "Modeling Malicious Activities in Cyber Space", *IEEE Network*, Cilt 29, Sayı 6, Kasım-Aralık 2015, ss. 83-84.
[638] Kaspersky, "What Is Spyware? - Definition", *https://www.kaspersky.com/resource-center/threats/spyware*, (Erişim Tarihi: 16 Nisan 2020).
[639] Avast, "Spyware: Detection, Prevention, and Removal", *https://www.avast.com/c-spyware*, (Erişim Tarihi: 16 Nisan 2020).

Tablo 27'de sunulan casus yazılımların çalışma işleyişinden anlaşılacağı üzere kaydedilmiş parolalar, kullanıcı tarafından ziyaret edilen çevrimiçi sayfaların listesi, bilgisayarda yüklü uygulamalar ve işletim sistemleri gibi çeşitli bilgilerin toplanmasında casus yazılımların rolü büyüktür. Ayrıca, cihaz rehberlerindeki isimler, telefon numaraları, kredi kartı numaraları vb. kişisel bilgileri de toplayabilmektedirler. Bu yazılımlar sayesinde ele geçirilen kişi, aile, çalışma grubu ya da şirket bilgileri, pazarlama amacıyla kullanılabilmekte ve profiller oluşturulabilmektedir.[640] Casus yazılımlar değişik şekillerde ve boyutlarda bilgisayarlara bulaşabilmektedir. En bilinen örnekleri şu şekilde sıralanabilir: Kolluk kuvvetleri tarafından kullanılmak üzere tasarlanan ancak siber saldırganların eline geçen *FinFisher*; Tüketicilerin kişisel verilerine ulaşan ve *Google Play* uygulamalarından kolaylıkla geçebilen *GO Klavye*; Bilgisayarları daha güvenli hale getirme uygulaması olarak servis edilen *Look2Me*; Kullanıcıları gözetleyen, *pop-up* reklamlar yayınlayan ve bilgisayar kontrol ayarlarına nüfuz eden *Trojan.Zlob*.[641] Bu tarz çeşitli casus yazılım türleri, çoğunlukla kullanıcıların e-posta ve İnternet kullanım etkinliklerini ve rutinlerini kullanmaktadırlar. Dahası, casus yazılımları önleyici yazılımlar tarafından algılanmamak adına programları devre dışı bırakmak için söz konusu önlem paketlerine karşı saldırı yapan casus yazılımlar da bulunmaktadır.[642] Buna karşın, şekli ve yöntemi ne olursa olsun, casus yazılımların en tehlikeli olanları, kullanıcılar tarafından farkında olmadan cihazlarına yüklenirler. Bundan dolayı bilinmeyen göndericilerin e-postalarına dikkat edilmeli, güvenli olmayan kaynaklardan dosyalar indirilmemeli, *pop-up* reklamlara tıklanmamalı ve antivirüs kullanımına azami özen gösterilmelidir; çünkü casus yazılımlar, diğer kötü amaçlı yazılım türlerine kıyasla oldukça güçlü ve tespit edilebilmesi çok zor karakteristiğe sahiptirler. Buna ek olarak, diğer kötü amaçlı yazılım türleri genellikle işletim sistemlerine ya da sistem üzerindeki spesifik verilere zarar verirlerken, casus

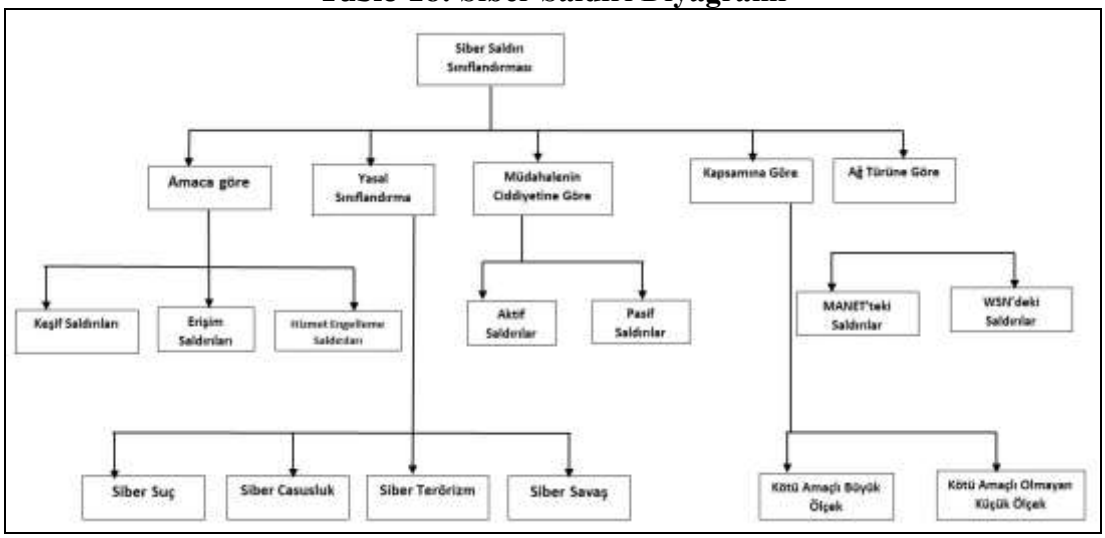
[640] Michael Erbschloe, *a.g.e.*, s. 26.
[641] Joseph Regan, "What Is Spyware?", *https://www.avg.com/en/signal/what-is-spyware*, (Erişim Tarihi: 16 Nisan 2020).
[642] University of Central Arkansas, Information Technology, "What Is Spyware?", *https://uca.edu/it/knowledgebase-legacy/what-is-spyware/*, (Erişim Tarihi: 16 Nisan 2020).

yazılımlar kullanıcıların kariyerlerine ve finansal durumlarına ağır hasarlar bırakabilirler ve söz konusu hasarların eski haline getirilmesi uzun zaman alabilir.[643]

2. Siber Olayların Sınıflandırılması

Siber olayların karmaşık doğası ve değişik boyutlardaki yansımaları göz önünde bulundurulduğunda, süreçlerin daha iyi idrak edilebilmesi adına sınıflandırmalar yapıldığı tespit edilmiştir. Buna karşın, siber uzay sahasının dinamik yapısı ve siber gelişmelerin birçok faktöre dayanan altyapıları, üzerinde fikir birliğine varılmış ideal bir sınıflandırmayı mümkün kılmamaktadır. Bununla birlikte pratik ana kategoriler tespit edilerek ve çeşitli sınıflandırmalar arasında kompozisyonlar oluşturmak suretiyle evrensel perspektife sahip modellemeler oluşturulabilir. Bu bağlamda siber olayların tehdit niteliğinde mi yoksa eylem niteliğinde mi olduğuna bakılarak nedenlerin, etkilerin ve sonuçların daha anlaşılabilir hale getirilmesi söz konusu olabilmektedir. Ardından saldırganların, saldırıların ve amaçların tanımlanması, bunlara hizmet eden araçların tasnif edilmesi ve güvenlik açıklarının tespit ve teşhis edilmesi yerinde olacaktır.[644]

Tablo-28: Siber Saldırı Diyagramı



Kaynak: M. Uma & Padmavathi Ganapathi, "A Survey on Various Cyber Attacks and Their Classification", *International Journal of Network Security*, Cilt 15, Sayı 5, Eylül 2013, s. 392.

---

[643] Bruce C. Brown, *How To Stop E-Mail Spam, Spyware, Malware, Computer Viruses, and Hackers From Ruining Your Computer or Network: The Complete Guide For Your Home and Work*, Atlantic Publishing Group, Florida 2011, s. 122.

[644] John D. Howard & Thomas A. Longstaff, *A Common Language for Computer Security Incidents*, Technical Report, SAND98-8667, Sandia National Laboratories, California Ekim 1998, ss. 6-17.

İlerleyen bölümlerde eylemsel siber örnek olayların üzerinde durulması planlanlanmaktadır. Bu nedenle Tablo 28'de sunulan saldırı diyagramının, eylemsel nitelikteki siber saldırıların sınıflandırılmasında fayda sağlayacağı öngörülmektedir. Öyle ki, çeşitli siber saldırı türleri, yayılma biçimleri ve şiddetlerine bağlı olarak farklı farklı siber aktörlerin savunmasızlıklarına dair göreceli bir anlayış eksikliği söz konusudur. Uygun güvenlik önlemlerinin geliştirilebilmesi ise bu tür saldırıların ve bunların sınıflandırılma modellerinin tam olarak anlaşılabilmesini gerekli kılmaktadır. Dolayısıyla bu tür sınıflandırmalar, siber güvenlik girişimlerinin önemli bir bileşenini oluşturmakta ve bu tür saldırıların arkasındaki motivasyonların daha iyi anlaşılabilmesine vesile olmaktadır.[645] Diğer taraftan günümüzde kötü amaçlı yazılımların işlevselliklerine ve değişim hızlarına bağlı olarak virüs, solucan truva atı, bot ya da casus yazılım gibi türlerden hangisi olup olmadıklarının belirlenmesinin giderek zorlaşması, siber saldırı sınıflandırmalarındaki geçmişe ait uyarlamalara dayalı alt başlıkların somut şemalardan ziyade açıklama süreçlerinin birer parçası haline evrilmesine neden olmuştur.[646] Siber saldırıların efektif şekilde anlaşılması ve değerlendirilmesi, risklerin azaltılması için gerekli olan doğru kararların alınmasına yardımcı olmaktadır. Saldırılara karşı etkin korumanın sağlanabilmesi; saldırı faaliyetleri, bilgisayar ve ağ varlıkları üzerindeki durum ve performans etkileri gibi saldırı özellikleri hakkında yeterli bilgiyi ve anlayışı elzem kılmaktadır.[647] Bu doğrultuda siber saldırılarının amacına, yasal sınıflandırmasına, katılım ciddiyetine, kapsamına ve ağ türüne göre beş ana kategoride yapılan sınıflandırmasında, özellikle amaca dayalı siber saldırı yöntemleri öne çıkmaktadır. Söz konusu yöntemlerin detaylandırılması, bu bölümün son kısmında sunulacak olan Siber Uluslararası İlişkiler örnek olaylarının teknik açıdan anlaşılabilmesi açısından yerinde olacaktır.

---

[645] M. Uma & Padmavathi Ganapathi, "A Survey on Various Cyber Attacks and Their Classification", *International Journal of Network Security*, Cilt 15, Sayı 5, Eylül 2013, s. 390.

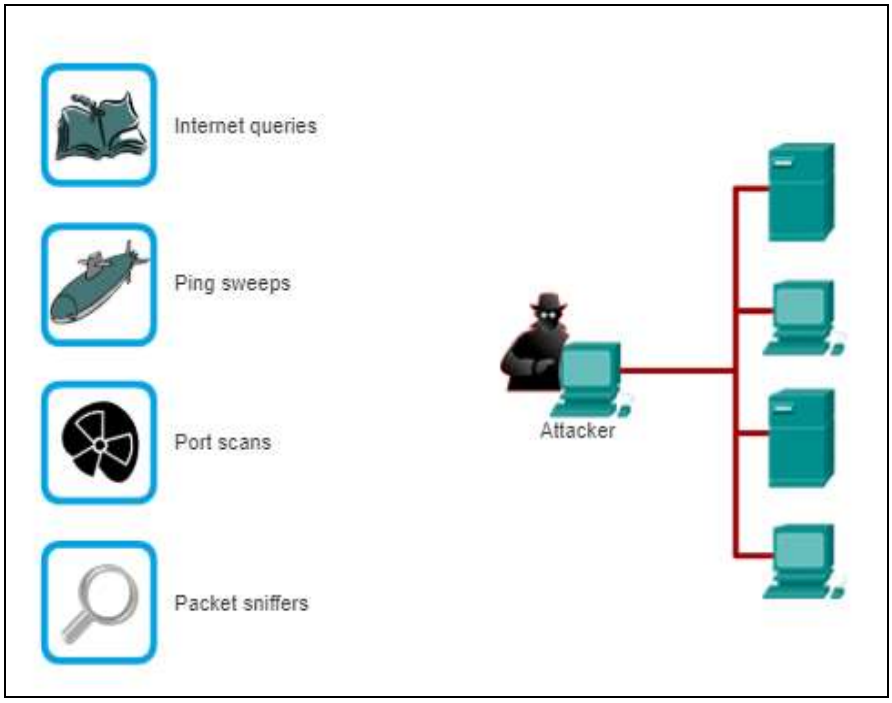
[646] European Union Agency For Network and Information Security (ENISA), *Reference Incident Classification Taxonomy: Task Force Status and Way Forward*, Athens Office, Ocak 2018, s. 10.

[647] Nong Ye, Clark Newman & Toni Farley, "A System-Fault-Risk Framework for Cyber Attack Classification", *Information, Knowledge, Systems Management*, Cilt 5, 2006, s. 135.

2.1. Keşif Saldırıları (*Reconnaissance Attacks*)

"Keşif Saldırıları" (*Reconnaissance Attacks*), hedeflenen cihaz, sistem veya ağların zayıf ve savunmasız noktalarının belirlenmesi amacıyla gerçekleştirilen saldırılardır. Hedef unsurların savunmasındaki zayıflıkların bulunması, aynı zamanda sahip olduğu yeteneklerin tespit edilmesiyle doğrudan alakalıdır ve bu aşamada yeterli kaynak uygulanması gerekmektedir.[648] Yetkisiz algılamalar, sistem haritalandırmaları ve hizmetler, "keşif saldırıları" olarak adlandırılmaktadır. Gerçek yaşam üzerinden örneklendirmek gerekirse; bir mahalle içerisindeki terkedilmiş konutlar ya da sağlam kapı ve pencereye sahip olmayan evlerden gerçekleştirilen hırsızlık olaylarına benzemektedir.[649]

Tablo-29: Keşif Saldırıları (*Reconnaissance Attacks*)



Kaynak: Cisco Networking Academy (NUM), "Keeping The Network Safe: Vulnerabilities and Network Attacks", *http://cisco.num.edu.mn/CCNA_R&S1/course/module11/11.2.2.2/11.2.2.2.html*, (Erişim Tarihi: 18 Nisan 2020).

[648] H. P. Sanghvi & M. S. Dahiya, "Cyber Reconnaissance: An Alarm Before Cyber Attack", *International Journal of Computer Applications (0975 – 8887)*, Cilt 63, Sayı 6, Şubat 2013, s. 36.
[649] M. Uma & Padmavathi Ganapathi, *a.g.m.*, s. 393.

Buna göre saldırganlar, belirli bir şirket ya da kuruma tanımlanan IP adres alanını belirleyebilmek için çeşitli İnternet araçlarını –*nslookup, whois* vb.– yardımcı program olarak kullanabilirler. IP adres alanı belirlendikten sonra aktif olan adreslerin tanımlanması ve aralıklarının belirlenmesi adına genel kullanıma açık olan IP adreslerine "ping atmak" olarak tabir edilen bağlantı durum kontrolü gerçekleştirilir. Sonrasında hangi bilgisayar hizmetlerinin iyi bilinen bir bağlantı noktası numarasıyla ilişkili olduğunu öğrenmek için saldırgan tarafından hedef cihaza bir dizi mesaj gönderilir ve tarama gerçekleştirilir. Nihayetinde de ağa bağlı bilgisayarlar arasındaki trafik tespit edilir ve diğer bilgisayarlara gönderilen veriler yakalanarak analiz için saldırgana gönderilir.[650] Keşif saldırıları aktif ve pasif olmak üzere ikiye ayrılır: Pasif keşif saldırılarında, hedefin gözetimine takılmaksızın yani kullanıcı uyarılmaksızın bilgi toplanması söz konusudur. Örneğin; hedefin çevrimiçi sayfasının ziyaret edilmesi, saldırganın IP adresinin hedefin web sunucusuna bir TCP bağlantısı kurduğu izini geride bırakabilir ancak sık ziyaret yapılmazsa, günlük gerçekleştirilen çok sayıda ziyaretten biri olarak görünür ve sunucuya aşırı yüklenme olmadığında kullanıcı uyarılmaz. Aktif keşif saldırılarında ise daha fazla müdahaleci olunması söz konusudur. Yukarıda da belirtilen ping atmak, port taramak gibi araçlar, aktif keşif saldırılarında daha spesifik bilgilere ulaşılması adına yoğun olarak tercih edilmektedir. Dolayısıyla hedef olan ana bilgisayarlara daha fazla anormal bağlantılara neden olabilmekte ve hedef kullanıcısının potansiyel bir siber saldırıya karşı uyarılması riskini arttırabilmektedir.[651]

2.2. Erişim Saldırıları (*Access Attacks*)

"Erişim Saldırıları" (*Access Attacks*), bilgisayar kaynaklarına yetkisiz erişimin tüm biçimlerini kapsayan saldırılardır. Erişim saldırıları, ağ dışındaki siber aktörlerce çeşitli yöntemler kullanılarak gizli bilgilerin çalınması veya kaynaklarının imha edilmesi gibi amaçlarla gerçekleştirilmektedir. Diğer taraftan, ağ içerisinde yer

---

[650] Cisco Networking Academy (NUM), "Keeping The Network Safe: Vulnerabilities and Network Attacks", *http://cisco.num.edu.mn/CCNA_R&S1/course/module11/11.2.2.2/11.2.2.2.html*, (Erişim Tarihi: 18 Nisan 2020).

[651] United States Naval Academy (USNA), "Cyber Operations: Phases of A Cyber Attack / Cyber-Recon", *https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l32/lec.html*, (Erişim Tarihi: 18 Nisan 2020).

alan aktörlerin, kullanım yetkilerinin olmadığı alanlara girmeleriyle de erişim saldırıları yapılabilmektedir. Dış ve iç saldırganlar, merak ya da maddi çıkar gibi farklı amaçlarla bu saldırıları düzenleyebilirler.[652] Bu tarz saldırılar, izinsiz giriş yeteneği gerektirmektedir ve herhangi bir hesap sahibinin yabancı bir donanımı doğrudan ağ altyapısına bağlamak için kimlik bilgilerini elde etmek kadar basit yöntemlerden oluşabilmektedir.[653] Uygun güvenlik önlemleri alınmadığı takdirde ağlar, erişim saldırılarına karşı savunmasız kalabilmektedirler. Ağ yöneticileri, sorumlu oldukları ağlara sadece yetkili kullanıcıların erişmesini sağlamaktan sorumludurlar ve yetkisiz erişim saldırılarının tamamı, kimlik doğrulama sürecini dört yolla atlatmaya çalışmaktadır: Şifre saldırıları; Güven suistimali; Bağlantı noktasının yeniden yönlendirilmesi; ve Ortadaki adam saldırıları.[654] Şifre saldırıları, saldırganlar tarafından bilgisayarın ya da sistemin şifreleri tahmin edilerek erişim elde etme girişimleridir. En bilinen ve en fazla kullanılan kelimelerin sırayla denendiği "sözlük saldırısı", bunun en yaygın örneklerindendir. Güven suistimali ise iki şekilde gerçekleşmektedir: İstemcinin bir sunucuda sahip olduğu güvene itimat ve sunucunun istemciye duyduğu güvene itimat. Bu tür saldırılarda, ağ içerisindeki bir saldırgan, sisteme yetkisiz olarak tanınan ayrıcalıkları kullanabilmekte ve oturumu ele geçirebilmektedir. Bağlantı noktasının yeniden yönlendirilmesinde ise tehlikeye atılmış bir sistemin diğer hedeflere saldırmak için kullanılması söz konusudur. Buna göre güvenilmez bir kaynağın güvenlik duvarındaki bir bağlantı noktasından trafik ilerletmek için iç ağ erişimi olan bir makine kullanması söz konusudur. Son olarak ortadaki adam saldırıları, bilgisayar korsanlarının ağ trafiğini dinlemeleri ve veri iletimlerini engellemeleriyle gerçekleşmektedir. Bu bağlamda saldırganlar, iki meşru taraf arasındaki iletişimin ortasında kendilerini konumlandırırlar ve kimlik

---

[652] Cisco Certified Security Professional Certification (CCSP), "The Four Primary Types of Network Attacks", *http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+I+Introduction+to+Network+Security/Chapter+1+Understanding+Network+Security+Threats/The+Four+Primary+Types+of+Network+Attack/*, (Erişim Tarihi: 19 Nisan 2020).

[653] The State of Security, "3 Types of Network Attacks to Watch Out For", *https://www.tripwire.com/state-of-security/vulnerability-management/3-types-of-network-attacks/*, (Erişim Tarihi: 19 Nisan 2020).

[654] David Minutella, Jeremy Cioara & Heather Stevenson, "CCENT Exam Prep: General Network Security", Pearson It Certification, *https://www.pearsonitcertification.com/articles/article.aspx?p=1151753&seqNum=2*, (Erişim Tarihi: 19 Nisan 2020).

bilgilerinin yakalanmasından oturumun ele geçirilmesine kadar çeşitli saldırıları gerçekleştirebilmektedirler.[655]

2.3. Hizmet Engelleme Saldırıları (*Denial of Service Attacks*, DoS) ve Dağıtılmış Hizmet Engelleme Saldırıları (*Distributed Denial of Service Attacks*, DDoS)

"Hizmet Engelleme Saldırıları" (*Denial of Service Attacks*, DoS) veya diğer tabirle "DoS Saldırıları", kötü niyetli siber aktörler tarafından bilgi sistemlerine, cihazlara ya da diğer ağ kaynaklarına erişim engeli getiren saldırılardır. E-posta, çevrimiçi sayfalar, kamuya ve finans sektörüne ait çevrimiçi hesapların yanı sıra etkilenen bilgisayar veya ağlara dayalı olan hizmetler de DoS saldırılarından doğrudan etkilenebilmektedir. Bu saldırıların ana koşulu; hedeflenen sunucuların ya da ağların cevap veremez hale gelene kadar –yani çökene kadar– trafik yoğunluğuna tabi tutulmasıdır. Böylece yasal kullanıcılar açısından söz konusu çevrimiçi sayfalara ya da uygulamalara erişim engellenmiş olmaktadır.[656] İlk DoS saldırısı, 1974 yılında David Dennis isimli 19 yaşındaki bir genç tarafından gerçekleştirilmiştir. Buna göre Dennis, "*external*" veya "*ext*" komutu kullanarak, evinin yakınındaki bir üniversite araştırma laboratuvarındaki bazı bilgisayarları kapanmaya zorlamıştır.[657] Bu örnek üzerinden de anlaşılacağı üzere DoS saldırıları, en genel anlamda, bir hizmeti erişilemez hale getirmek için tasarlanmış siber saldırı sınıfının nihai hedefini tanımlamaktadır. Çoğunlukla yüksek profilli çevrimiçi sayfalara para ve zaman kayıpları yaratmak için yapılan bu saldırılar, aynı zamanda kritik süreçleri destekleyen endüstriyel kontrol sistemleri de dâhil olmak üzere her türlü sisteme uygulanabilmekte ve hizmet erişim engelleri yaratabilmektedir. DoS saldırılarının görünen etkileri ise bakış açılarına bağlı olarak değişebilmektedir. Örneğin; sıradan bir kullanıcı açısından çevrimiçi sayfanın içerik göstermeyi durdurması olarak

---

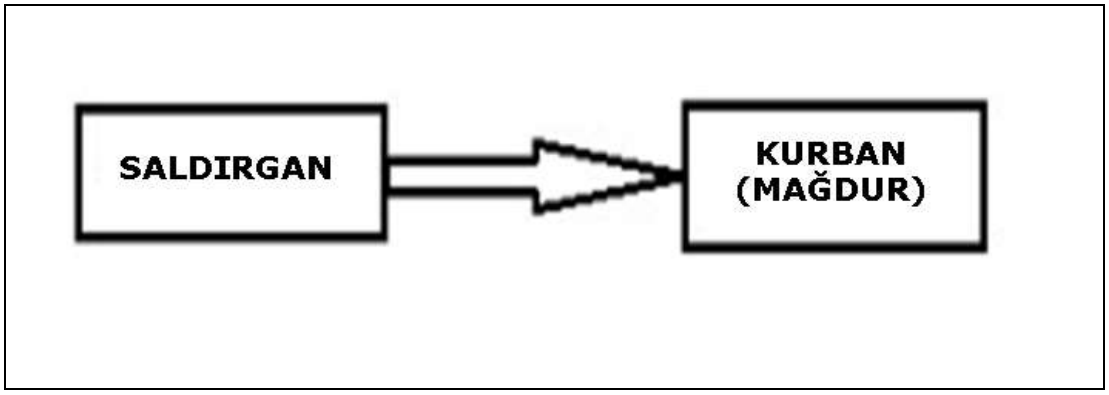
[655] CertificationKits, "CCNA Security: Common Network Attacks", *https://www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-describe-security-threats/ccna-security-common-network-attacks/*, (Erişim Tarihi: 19 Nisan 2020).

[656] The Cybersecurity and Infrastructure Security Agency, "Security Tip (ST04-015): Understanding Denial-of-Service-Attacks", *https://www.us-cert.gov/ncas/tips/ST04-015*, (Erişim Tarihi: 20 Nisan 2020).

[657] Norton, "Emerging Threats: What Are Denial of Service (DoS) Attacks? DoS Attacks Explained", *https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html*, (Erişim Tarihi: 20 Nisan 2020).

yorumlanırken, işletmeler açısından bağlı bulundukları çevrimiçi sistemlerin yanıt vermeyi kesmesi anlamı gelebilir. Endüstriyel kontrol sistemlerinde ise sensör verilerinin alınamaması ya da kritik süreçlerinin kontrol edilememesini içerebilmektedir.[658]

Tablo-30: DoS Saldırısı



Kaynak: Monika Malik & Yudhvir Singh, "A Review: DoS and DDoS Attacks", *International Journal of Computer Science and Mobile Computing*, Cilt 4, Sayı 6, Haziran 2015, s. 262.

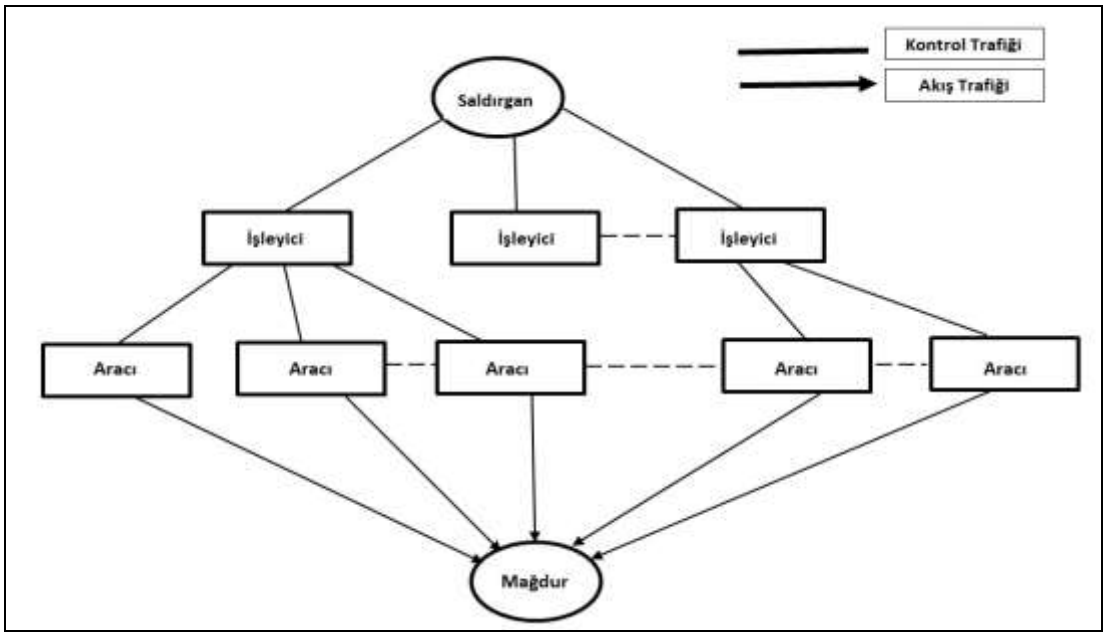
DoS saldırıları, tek bir bilgisayar ve İnternet bağlantısı kullanılarak hedef kaynak sunucularında trafik yoğunluğu yaratmaktadır (Tablo 30). Pek çok saldırı tekniği, hizmetleri devre dışı bırakabildiği veya hizmet sağlamak için kaynakları tüketerek hizmet performansını düşürebildiği sürece DoS saldırı amaçları doğrultusunda kullanılabilmektedir.[659] Çok sayıda DoS saldırı tekniği bulunmakla birlikte geniş çaplı olarak bakıldığında, yazılım istismarları ve *flood* saldırıları şeklinde sınıflandırılması mümkündür. Buna göre yazılım istismarlarında, saldırgan tarafından hedefin devre dışı bırakılabilmesi adına hedef işletim sistemi veya uygulaması içerisindeki yazılım hataları uygulanmaktadır. *Flood* saldırılarında ise bir veya

[658] National Cyber Security Centre (NCSC), "Denial of Service (DoS) Guidance", *https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection*, (Erişim Tarihi: 20 Nisan 2020).
[659] Monika Malik & Yudhvir Singh, "A Review: DoS and DDoS Attacks", *International Journal of Computer Science and Mobile Computing*, Cilt 4, Sayı 6, Haziran 2015, s. 262.

birden fazla saldırgan, bağlantı bant genişliğine ya da bilgi işlem kaynaklarına zarar vermek için sürekli paket akışları göndermektedirler.[660]

Diğer taraftan; bir veya birden fazla hedefe yönelik koordineli bir DoS saldırısı başlatmak için birçok bilgisayar kullanılmasına "Dağıtılmış Hizmet Engelleme Saldırısı" (*Distributed Denial of Service Attacks*, DDoS) ya da diğer tabirle "DDoS Saldırısı" adı verilmektedir. Tablo 31'de de görüldüğü üzere saldırgan, istemci/sunucu teknolojisi üzerinden saldırı platformları olarak hizmet eden çok sayıda bilgisayarın kaynağını kullanarak hizmet engellenmesini önemli ölçüde çoğaltabilmektedir. Genellikle DDoS ana programları, çalınan bir hesap kullanılarak bilgisayarlara yüklenmekte, ardından belirlenen bir zamanda, İnternetin herhangi bir yerindeki bilgisayarlara kurulan çeşitli sayılardaki aracı programlarla iletişim kurulmakta ve verilen komutla saniyeler içerisinde yüzlerce hatta binlerce aracı programı başlatarak saldırı yapabilmektedirler.[661]

Tablo-31: DDoS Saldırıları



Kaynak: Monika Malik & Yudhvir Singh, "A Review: DoS and DDoS Attacks", *International Journal of Computer Science and Mobile Computing*, Cilt 4, Sayı 6, Haziran 2015, s. 263.

---

[660] Alefiya Hussain, John Heidemann & Christos Papadopoulos, *A Framework for Classifying Denial of Service Attacks*, Technical Report ISI-TR-2003-569b, USC/Information Sciences Institute, Şubat 2003, s. 100.

[661] The World Wide Web Consortium (W3C), "The World Wide Web Security FAQ: Securing Against Denial of Service Attacks", *https://www.w3.org/Security/Faq/wwwsf6.html*, (Erişim Tarihi: 20 Nisan 2020).

DDoS saldırıları, bir bilgisayar ve bir İnternet bağlantısı kullanmak yerine, hedeflenen uygulama ve hizmetleri kötü amaçlı trafik istekleriyle doldurmak için birden fazla bilgisayar ve birçok bağlantı kullanmaktadırlar. Böylelikle çevrimiçi hizmetleri kullanılamaz hale getirmektedirler. Bu tür saldırıların arkasındaki kaynak bilgisayarlar genellikle dünya çapında dağıtılmıştır. Kötü amaçlı yazılım formları kullanılarak kullancıların rızası olmaksızın ve toplu olarak botnet'in parçası olarak kullanılabilirler.[662] DDoS saldırıları üç ana kategoride değerlendirilmektedir: Saldırganın ana hedefinin, mağdurun sitesinin bant genişliğini tüketmek olan "hacim tabanlı saldırılar". ICMP ve UDP *flood* saldırıları ile birlikte diğer sahte paket saldırılarını kapsayan hacim tabanlı saldırıların büyüklüğü saniyelik *–bits per second,* Bps– olarak ölçülmektedir. İkinci olarak, saldırganın ana hedefinin güvenlik duvarı gibi gerçek sunucu kaynaklarını tüketmek olan "protokol tabanlı saldırılar"dır. SYN *flood* saldırıları, parçalanmış paket saldırıları, Ölüm pingi, Şirin saldırıları bu kapsamda değerlendirilmektedir. Son olarak ise saldırganın güvenlik açıklarını ve daha fazlasını hedeflediği "uygulama katmanı tabanlı saldırılar" içerisinde *Zero-day* saldırısı, *Slowloris* vb. yerler almaktadır.[663]

DDoS saldırıları, kötü amaçlı siber aktörler tarafından 2000 yılından itibaren kullanılmaya başlamıştır. Ağların, sunucuların ve çevrimiçi sayfaların bozulması için DDoS saldırılarının tercih edilen bir siber silah haline gelmesinin nedeni de budur. Söz konusu saldırılar, hedeflerine zarar verebilmek için Nesnelerin İnterneti'ni oluşturan web kameraları ve akıllı televizyonlar gibi sürekli artan diğer elektronik cihazları kullanabilmektedir. Nesnelerin İnterneti'ni oluşturan cihazlardaki güvenlik açıkları, anonim ve kolay şekilde DDoS saldırıları gerçekleştirmek isteyen siber saldırganlarca erişilebilir olmaktadır. Öte yandan, DoS saldırılarının tek bilgisayar ve tek İnternet kaynağı kullanması sebebiyle DDoS saldırılarına kıyasla savunulması daha kolay gerçekleşebilmektedir ve bu nedenle DDoS saladırıları daha fazla tercih edilmektedir.[664] Bu bağlamda DoS ve DDoS saldırılarının yeni yöntemler geliştirme hızları da dikkate alınarak saldırılara karşı önlem girişimleri her geçen gün

---

662 Aarnet, "What Is A Do Sor DDoS Attack?", *https://support.aarnet.edu.au/hc/en-us/articles/115001952194-What-is-a-DoS-or-DDoS-attack-*, (Erişim Tarihi: 20 Nisan 2020).
663 Monika Malik & Yudhvir Singh, *a.g.m.*, s. 264.
664 Norton, "Emerging Threats: What Are Denial of Service (DoS) Attacks? DoS Attacks Explained", *https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html*, (Erişim Tarihi: 20 Nisan 2020).

genişlemektedir. Genel olarak imza tabanlı ve anomali tabanlı iki tür algılama öne çıkmaktadır. İmza tabanlı algılamada, gelen saldırılar hakkında önceden ayrıntılı bilgiye sahip olma durumu söz konusudur ve saldırı özellikleri veritabanıyla kıyaslanarak önlemler tespit edilir; ancak bu yöntem, daha önce benzeri yaşanmamaış saldırıların tespit edilmesi hususunda yetersiz kalmaktadır. Anomali tabanlı algılama yönteminde ise sistemin normal trafiğinde farklılıklar tespit edilir, protokol bilgileri, kaynak adresi ve ağ trafiğindeki kötü amaçlı davranışların paket düzeyindeki analizlerine göre önlemler tanımlanır.[665]

3. Siber Olaylar Tarihinin Aşamaları

Günümüzde devletler ve devlet temsilcileri başta olmak üzere devlet dışı aktörler, gruplar veya bireyler tarafından bilgi ve bilgisayar ağlarını savunmak, bilgi saldırılarını caydırmak ve rakip aktörlerin benzer eylemleri yapabilme kabiliyetlerini sınırlamak gibi çeşitli savunma, suç, saldırı, casusluk, terörizm ve caydırıcılık faaliyetlerinin siber uzay sahasında yürütülmesi anlamında kapsayıcı şekilde kullanılmakta olan siber savaş perspektifi, farklı boyutlarda farklı etkilere sahip ve farklı yapılardaki çeşitli siber olayların tarihsel olarak çeşitli aşamalardan geçmesi neticesinde ortaya çıkmıştır.[666] Artan siber olaylar ve gelişmeler sayesinde siber uzay sahasının etkileri siber alandan reel alana taşmış ve ulusal/uluslararası ilişkilerin nitelikleri, formları, çıkarları, altyapıları ve hedefleri, siber alanın söz konusu yayılma etkisinden doğrudan etkilenmiştir. Ek olarak; bilgi ve iletişim teknolojilerinde yaşanan muazzam gelişmeler ve ilerlemeler ışığında yeniden yapılandırılan ilişkiler, dünyanın her yerinden milyarlarca insanı anlık ve küresel iletişim yoluyla birbirine bağlamıştır. Yerel ve küresel ağlara bağlı bilgi işlem gücünün hızla yayılmasıyla birlikte ise güvenlik kavramı, çok daha önemli bir pozisyona evrilmiştir. Bir taraftan gerçek dünya, siber alanın içerisine eklemlenerek giderek küçülürken, diğer taraftan ise güvenliğin belirleyiciliği ve güvenlik açıkları

---

[665] Ramin Fadaei Fouladi, Tina Seifpoor & Emin Anarim, "Frequency Characteristics of DoS and DDoS Attacks", *2013 21st Signal Processing and Communications Applications Conference (SIU)*, Haspolat, 24-26 Nisan 2013, s. 1.

[666] Gary D. Solis, "Cyber Warfare", *Military Law Review*, Cilt 219, Bahar 2014, s. 3.

şaşırtıcı şekilde genişlemiştir.[667] Öyle ki; bugünün dünyasında bilgisayarı olmayan insanlar dahi kötü amaçlı siber aktörlerin doğrudan ve dolaylı tehditleri ve riskleri altında yer alıyorken, Uluslararası İlişkileri şekillendiren büyük aktörlerin söz konusu tehditlerden etkilenmemesi veyahut da görmezden gelmesi mümkün değildir. Bu bağlamda siber olaylar tarihinin incelenmesi, siber çatışmaların, saldırıların ve savaşların karmaşık ve belirsiz dinamiklerine ilişkin içgörü sağlayabilmekte, çeşitli teorilerin ve test edilebilir hipotezlerin formülasyonunu arttırabilecek vaka çalışmaları ve veri kümeleri de dâhil olmak üzere geniş bir bilgi deposu sunabilmektedir. Bununla birlikte devletlerin ve devlet unsurlarının yeteneklerini çevreleyen gizlilik ve saldırganların anonimliği, siber olaylar tarihinin belgelenmesini zorlaştırmakla birlikte hala çok miktarda veri, örnek olay raporu ve çeşitli belgeler analiz edilmeyi beklemektedir.[668]

Geçmişte yaşanan her türlü siber saldırı eylemi, gelecekteki siber zorlukların somutlaştırılması ve kurumların güvenlik açıklarının tespit edilmesine dair uyarı niteliği oluşturmaktadır. Dolayısıyla yaşanan her tür siber olay, siber uzay alanının kurumsal evrimi açısından katalizör etkisinde bulunmaktadır. Teknoloji bağımlılığının giderek artması ve derinleşmesi ise yaşanan spesifik siber alan ihlallerindeki yetersiz güvenliğin olası etkilerinin boyutunu giderek arttırmaktadır. Tüm bu anlatılanların ışığında siber olaylar tarihinin üç aşamada sınıflandırılması ve değerlendirilmesi yerinde olacaktır: İnternetin erken dönemindeki olayları kapsayan "gerçekleşme" aşaması; Saldırıların çoğunlukla bilgi toplama niteliğinde olduğu ve giderek arttığı "yükseliş" aşaması; ve Siber yeteneklerin kritik altyapılara ve devletlerin stratejik hedeflerine kinetik saldırılar boyutunda hasarlar yaratabildiği "militarizasyon" aşaması.[669]

---

[667] Michael Warner, "Cybersecurity: A Pre-history", *Intelligence and National Security*, Cilt 27, Sayı 5, Ekim 2012, s. 781.

[668] Max Smeets & Jason Healey, "Cyber Conflict History", *Tech & Policy Initiative, Working Paper Series 2*, Cyber Conflict Studies Association (CCSA), School of International and Public Affairs (SIPA), 2017, ss. 203-204.

[669] Omry Haizler, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking", *Cyber, Intelligence, and Security*, Cilt 1, Sayı 1, Ocak 2017, ss. 32-33.

3.1. Gerçekleşme Aşaması

Bilgisayarların, bilgisayar ağlarının ve İnternetin ortaya çıktığı erken dönemi ifade eden "gerçekleşme" (*realization*) aşaması, siber alanın küresel anlamda temellerinin oluşmaya başladığı, bu alanın kullanımının salt dostça olmadığının anlaşıldığı ve güvenlik endişelerinin geliştiği süreci yansıtmaktadır. "Bilgisayar korsanlığı" veya "bilgisayar korsanı saldırısı" anlamına gelen "*hacking*" terimi, ilk olarak bu dönemde kullanılmıştır. Bir ürünün ya da prosedürün normal işlevini değiştirmek veya tespit edilen bir sorunu düzeltmek için değişiklik yapmak anlamında kullanılan bu terim, 1960'larda tren modellerinde değişim faaliyetlerinde yoğun olarak kullanılmıştır. Bilimsel deneyler ile kişisel merak ve girişimler doğrultusunda erken dönem bilgisayarların programlarında kullanılan kodlar üzerinden değişiklikler yapılabilmesi, sorunların çözümüne akılcı yollar ve işlevselliğin iyileştirilmesine pratik fırsatlar sağlamıştır.[670] Dolayısıyla bilgisayar tabanlı cihazların tüm yapısını yeniden tasarlamaksızın belirli fonksiyonlar üzerinde güncellemeler yapılarak amaca uygun genel değişikliklerin üretilebilmesinin yolları keşfedilmiştir.

Diğer taraftan, 1970'lerden itibaren bilgisayarlı telefon sistemlerini eğlence ve çıkar amaçlı hedef haline getiren ve uzun mesafe telefon hizmetlerinin yazılım ve donanımı üzerinde müdahalelerde bulunarak sistemden kişisel fayda sağlayan saldırılar, ilk kötü amaçlı "*hacking*" uygulamalarından olmuştur.[671] Bundan sonrasında da "*hacking*" anlamı olumsuzlaşmıştır.[672] 1980'lerden itibaren ise ilk büyük ölçekli siber casusluk saldırıları gerçekleştirilmeye başlamış ve yüksek düzeyde birbirlerine bağlı bilgisayar ağlarının potansiyel tehlikelerinin farkına varılmıştır. Bunlara ek olarak ise ortaya çıkmaya başlayan siber alanın yapısında ve yeteneklerindeki savunmasızlık hali, kurumsallaşma ihtiyacını öne çıkarmaya

---

[670] Vanessa Pitts, *Cyber Crimes: History of World's Worst Cyber Attacks*, Alpha Editions, Vij Books, Darya Ganj 2017, s. 8.

[671] Phil Lapsley, "Phone Phreaks: What We Can Learn From the First Network Hackers?", The Advanced Computing Systems Association (USENIX), *https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/phone-phreaks-what-we-can-learn-first*, (Erişim Tarihi: 22 Nisan 2020).

[672] Günümüzde TDK'ya göre bilgisayar korsanı yani "*hacker*" ve eylemleri yani "*hacking*" şu şekilde tanımlanmaktadır: "Bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse." TDK, Türk Dil Kurumu Sözlükleri, *https://sozluk.gov.tr/*, (Erişim Tarihi: 22 Nisan 2020).

başlamıştır. 1986 yılındaki *Cuckoo's Egg* saldırısı, bilinen ilk büyük ölçekli siber saldırı olmakla birlikte söz konusu "gerçekleşme" aşamasının da başlangıç noktası olarak yorumlanmaktadır. Buna göre Clifford Stoll isimli bir uzay bilimci, sistem yöneticisi olarak çalışmakta olduğu Lawrence Berkeley Ulusal Laboratuvarı'ndaki bir bilgisayar programındaki açıktan yararlanılarak saldırı yapıldığını tespit etmiştir. Saldırının takibini yapan Stoll, Markus Hess isimli saldırganın Almanya'da yaşadığını ve Amerikan askeri bilgisayar sistemlerini tarayarak nükleer silahlar ve stratejik bilgiler üzerine araştırma yaptığını tespit etmiştir. Sonrasında Alman yetkililer tarafından tutuklanan Hess'in, Sovyet istihbarat kurumu olan KGB'ye hizmet ettiği ve elde ettiği bilgileri sattığı öğrenilmiştir.[673] Bu saldırı sonrasında 1988 yılında gerçekleşen *Morris Worm* saldırısı ise "gerçekleşme" aşamasının en dikkat çekici olayı olmuş ve daha düzenlenmiş bir siber uzay sahasına yönelik ilk adımlar için katalizör etkisinde bulunmuş, kavramsal ve operasyonel olarak dramatik değişikliklere yol açmıştır.[674]

Netice olarak, siber olaylar tarihinin bu "gerçekleşme" aşaması, şekillenmeye başlayan siber sahanın kötü amaçlı yaklaşımlar açısından oldukça savunmasız olduğunu göstermiştir. Yine bu dönemde bilgisayar tabanlı cihaz, sistem ve ağlarda total bazlı yeniden mühendislik gerektirmeksizin fonksiyonel müdahalelerle çeşitli değişiklikler ve dönüşümler yaratılabileceği keşfedilmiştir. Bütün bu gelişmeler ışığında da ilk küçük ve büyük ölçekli siber saldırı türleri yaşanmaya başlamıştır. Bu bağlamda siber olaylar tarihinin "gerçekleşme" aşamasında değerlendirilen ve kayıtlara geçen en dikkat çekici saldırılar şu şekilde listelenmektedir:

---

673 Brian Lamb, "Clifford Stoll Röportajı", C-SPAN, 13 Ekim 1989, *https://www.c-span.org/video/?10122-1/the-cuckoos-egg*, (Erişim Tarihi: 22 Nisan 2020).; Andy Greenberg, "Meet the Mad Scientist Who Wrote the Book on How to Hunt Hackers", Wired, 12 Ekim 2019, *https://www.wired.com/story/meet-the-mad-scientist-who-wrote-the-book-on-how-to-hunt-hackers/*, (Erişim Tarihi: 22 Nisan 2020).; Ayrıca Cuckoo's Egg hakkında detaylı bilgi için bkz.: Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, New York 1989.

674 Omry Haizler, *a.g.m.*, ss. 33-34.

Tablo-32: Gerçekleşme Aşamasındaki Siber Olaylar (1980-1998)

Tarih	Saldırı	Saldırgan	Hedef	Kategori
Haziran, 1981	Babylon Operasyonu / Opera Operasyonu	İsrail Hava Kuvvetleri	Osirak Nükleer Reaktörü, Irak	Siber Saldırı / Siber Savaş
Ağustos, 1985	Cuckoo's Egg	Markus Hess, KGB, SSCB	Lawrence Berkeley Ulusal Laboratuvarı, ABD	Siber Casusluk
Kasım, 1988	Morris Worm	Robert Tappan Morris, Cornell Üniversitesi	İnternete bağlı yaklaşık 60.000 civarı bilgisayar	Kötü Amaçlı Yazılım
1989	Wank Worm	Avusturalyalı Anonim Bilgisayar Korsanları	DEC VMS Bilgisayarları	Kötü Amaçlı Yazılım
1990	SunDevil Operasyonu	ABD Gizli Servisi	ABD'deki İllegal Aktiviteler Yapan Bilgisayar Korsanları	Siber Saldırı / Siber Casusluk
1990-1994	Dutch and British Hackers	Holladalı ve İngiliz Anonim Bilgisayar Korsanları	Hollandalılar -> ABD Askeri Tesisleri İngilizle-> Güney Kore Hedefleri	Siber Saldırı / Siber Savaş
Şubat, 1991	Michelangelo Virüsü	Anonim	Disk İşletim Sistemleri	Kötü Amaçlı Yazılım
Mart, 1994	"Rome Labs" - Rome Air Development Center, Griffiss Air Force Base, New York Intrusion	Datastream Cowboy & Kuji (Bilgisayar Korsanları)	Roma Laboratuvarları Bilgisayarları, New York (ABD Hava Kuvvetlerinin Süper Laboratuvarlarından)	Siber Casusluk

Haziran-Ekim, 1994	Citibank Caper	Rus Siber Saldırganlar	Citibank Hesapları, ($10 milyon transfer edildi)	Siber Saldırı / Siber Casusluk
Haziran, 1997	Eligible Receiver / Eligible Receiver 97	Kırmızı Takım - ABD Ulusal Güvenlik Dairesi (NSA) & ABD Siber Komutanlığı (USCYBERCOM)	ABD Kurumları ve Kritik Altyapıları (ABD'nin siber güvenliğini test etmek amaçlı "Siber Tatbikat" olarak tanımlanmaktadır.)	Siber Saldırı / Siber Savaş

Kaynak: Max Smeets & Jason Healey, "Cyber Conflict History", *Tech & Policy Initiative, Working Paper Series 2*, Cyber Conflict Studies Association (CCSA), School of International and Public Affairs (SIPA), 2017, ss. 203-212.; Paul J. Springer, *Encyclopedia of Cyber Warfare*, ABC-CLIO, California 2017.; Alexander Gamero-Garrido, *Cyber Conflicts in International Relations: Framework and Case Studies*, Explorations in Cyber International Relations (ECIR) Working Paper, MIT & Harvard University, 2014.; Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, ABC-CLIO, California 2013.; Omry Haizler, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking", *Cyber, Intelligence, and Security*, Cilt 1, Sayı 1, Ocak 2017, ss. 31-45.; Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, 1. Basım, Simon & Schuster, New York 2016.; Bruce Middleton, *A History of Cyber Security Attacks: 1980 to Present*, CRC Press, New York 2017.; Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt & Joseph Weiss, *Cyber Security Policy Guidebook*, 1. Basım, John Wiley & Sons, Inc., New Jersey 2012.; A. Kiyuna & L. Conyers, *Cyberwarfare Sourcebook*, Lulu.com, 2015.; Vanessa Pitts, *Cyber Crimes: History of World's Worst Cyber Attacks*, Alpha Editions, Vij Books, Darya Ganj 2017.

3.2. Yükseliş Aşaması

Siber olaylar tarihinin ikinci aşaması olarak belirtilen "yükseliş" dönemi, 9/11 Terör Saldırıları öncesi ve sonrasındaki ara süreci kapsamaktadır. Jason Healey, siber çatışmalardan siber savaşlara dek uzanan siber olaylar tarihinin gerçekleşme fazının tarih aralığını 1980-1998, yükseliş fazının 1998-2003 ve militarizasyon fazının ise 2003'ten günümüze dek uzandığını belirtmektedir.[675] Bu evrelendirmeler arasındaki temel farklılıkların özünü ise siber yeteneklerin aktörler arasındaki artan ve hızla değişen dağılımları ile siber olaylara yönelik gelişmiş ve resmileşmiş örgütsel

[675] Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association (CCSA), Virginia 2013, s. 18.

yaklaşımların etki boyutları oluşturmaktadır.[676] Siber olaylar tarihinin bu yükseliş aşamasının gerçekleşme aşamasından en önemli farkı; siber yeteneklere sahip aktör sayısındaki ve dolayısıyla düşman çeşitliliğindeki artıştır. Buna göre ABD karşısında güçlü bir Rusya gerçeği çıkmakta, düşman unsur ve yöntemler ise gerçekleşme evresinde bilgisayar korsanlarıyla sınırlıyken, bu dönemde bilgisayar korsanlarına ek olarak hactivistler, milliyetçi bilgisayar korsanları, virüsler ve solucanlar dâhil olmaktadır. Gerçekleşme aşamasındaki olaylar karşısında oluşturulan devlet politikaları ve doktrinlerindeki istihbarat savaşı anlayışının aksine bu dönemde operasyonel tutumlar ve önlemler öne çıkmaktadır. Diğer taraftan iki aşamada ve hatta militarizasyon aşaması da dâhil olmak üzere tüm aşamalarda ortak olan ve değişmeyen tek dinamik gerçeğin ise saldırgan tarafın avantajlı olduğuna dayandığı görülmektedir. Yani siber olaylarda saldırganlar, her daim önlem alan ve savunma yapan aktörlere kıyasla avantajlı olan taraf olarak öne çıkmaktadır.[677]

Bu aşamada yaşanan olaylar, siber alandaki çatışmalarda ya da savaşlarda zafer kazanmanın ve kaybetmenin karmaşık yapısını daha belirgin hale getirmiştir. Temel analiz birimlerinin bilgisayar sistemlerinden ve ağlardan oluştuğu bu beşinci alanda kazanmak ile kaybetmenin arasında net bir ayrımın olmadığı anlaşılmıştır.[678] Teknik alanın daha fazla öne çıktığı ve taktik karmaşanın oldukça fazla olduğu bu yeni alanda uluslararası normların inşa edilmesi ve kurumsal yapının gerekliliğine dair tartışmalar, bu yükseliş aşamasındaki periyotta ortaya çıkmaya başlamıştır. Öyle ki, siber savaş gerçeğine yönelik ilk uluslararası ciddi odaklanma girişimi, 1998 yılında Rusya Federasyonu'nun BM Genel Kurulu Birinci Komitesi'nde "Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanında Gelişmeler" (*Developments in the Field of Information and Telecommunications in the Context of Security*)[679] başlıklı karar taslağında diğer silah kontrol anlaşmalarına benzer şekilde siber silahların kontrolü için de gereklilik olduğu önerisiyle gerçekleşmiştir.[680] Öyle ki bu öneri,

---

[676] Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*, University of Nebraska Press, Nebraska 2015, s. 162.
[677] Omry Haizler, *a.g.m.*, s. 32.
[678] Jason Healey, "Winning and Losing in Cyberspace", *2016 8th International Conference on Cyber Conflict (CyCon)*, 4 Ağustos 2016, Tallinn, s. 38.
[679] United Nations, Office for Disarmament Affairs, "Developments In The Field of Information and Telecommunications In The Context of International Security", *https://www.un.org/disarmament/ict-security/*, (Erişim Tarihi: 24 Nisan 2020).
[680] Brian M. Mazanec, *a.g.e.*, s. 245.

ABD tarafından o dönem için reddedilmiş ve siber suçluların yakalanması için daha yakın işbirliği yapılmasının tercih edilebileceği karşı önerisi geliştirilmiştir.[681] Bu dönemin en önemli olayı olarak gösterilen *Moonlight Maze* saldırısı, ABD açısından ilk kez güvenlik, gizlilik, aktif izleme ve ulusötesi tehditlere maruz kalma kavramları hakkında siyasi ve hukuki soruları gündeme getirmiş, siber alandaki asimetrik savaş yapısına yönelik açık politikalara, stratejilere ve teknolojik çıkarımlara olan ihtiyacın anlaşılmasına neden olmuştur.[682] Öyle ki ABD, artık sadece saldıran değil, aynı zamanda güçlü şekilde siber saldırılar alabilen ve ciddi zararlar görebilen taraf konumuna da evrilmiştir. Söz konusu yükseliş aşamasında gerçekleşen, kayıtlara geçen ve tespit edilebilen saldırılar şu şekilde tablolanmaktadır:

Tablo-33: Yükseliş Aşamasındaki Siber Olaylar (1998-2003)

Tarih	Saldırı	Saldıran	Hedef	Kategori
Şubat, 1998	Solar Sunrise Operasyonu	İki Amerikalı Anonim Bilgisayar Korsanı ile İsrailli Bilgisayar Korsanı Ehud Tenenbaum	ABD Savunma Bakanlığı	Siber Casusluk
Mart, 1998	Moonlight Maze	Rus Siber Ajanlar	NASA, PENTAGON, Üniversiteler, Araştırma Laboratuvarları ve Çeşitli Devlet Kurumları	Siber Casusluk
Eylül, 1998	Electronic Disturbance Theater (EDT)	İki Amerikalı Hacktivist: Stefan Wray & Ricardo Dominguez	PENTAGON Çevrimiçi Sayfası	Siber Saldırı / Siber Savaş

[681] Jeffrey Carr, *Inside Cyber Warfare*, O'Reilly Media, Inc., California 2010, s. 34.
[682] Omry Haizler, *a.g.m.*, s. 35.

1999-2001	"Patriotic Hackers" Saldırıları	Amerikalı, Rus, Hollandalı, Sırp ve Çinli Anonim Bilgisayar Korsanları	Kosova Savaşı esnasındaki aktörlerin çevrimiçi sayfalarına gerçekleştirilmiştir.	Siber Saldırı / Siber Savaş
Mayıs, 2000	ILOVEYOU	Onel de Guzman, Filipinler	Microsoft Outlook üzerinden Windows İşletim Sistemli Kişisel Bilgisayarlar	Kötü Amaçlı Yazılım
Temmuz, 2001	Code Red Solucanı	Çin Kaynaklı Anonim Saldırganlar	Microsoft IIS Web Server Kullanan Bilgisayarlar	Kötü Amaçlı Yazılım
Eylül, 2001	Nimda Solucanı	Anonim	Microsoft IIS Web Server Kullanan Bilgisayarlar	Kötü Amaçlı Yazılım

Kaynak: Max Smeets & Jason Healey, "Cyber Conflict History", *Tech & Policy Initiative, Working Paper Series 2*, Cyber Conflict Studies Association (CCSA), School of International and Public Affairs (SIPA), 2017, ss. 203-212.; Paul J. Springer, Encyclopedia of Cyber Warfare, ABC-CLIO, California 2017.; Alexander Gamero-Garrido, *Cyber Conflicts in International Relations: Framework and Case Studies*, Explorations in Cyber International Relations (ECIR) Working Paper, MIT & Harvard University, 2014.; Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, ABC-CLIO, California 2013.; Omry Haizler, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking", *Cyber, Intelligence, and Security*, Cilt 1, Sayı 1, Ocak 2017, ss. 31-45.; Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, 1. Basım, Simon & Schuster, New York 2016.; Bruce Middleton, *A History of Cyber Security Attacks: 1980 to Present*, CRC Press, New York 2017.; Mike Chapple & David Seidl, *Cyberwarfare: Information Operations in a Connected World*, Jones & Barlett Learning, Massachusetts 2015.; A. Kiyuna & L. Conyers, *Cyberwarfare Sourcebook*, Lulu.com, 2015.; Vanessa Pitts, *Cyber Crimes: History of World's Worst Cyber Attacks*, Alpha Editions, Vij Books, Darya Ganj 2017.

3.3. Militarizasyon Aşaması

2003 yılında ABD'nin çeşitli kritik kurumlarına gerçekleştirilen Çin tabanlı *Titan Rain* saldırılarıyla birlikte başlayan siber olaylar tarihinin militarizasyon aşaması, günümüze dek uzanan süreci kapsamaktadır. Bu dönemde ABD ve Rusya

Federasyonu gibi Siber Uluslararası İlişkilerin en güçlü aktörlerine Çin Halk Cumhuriyeti'nin dâhil olduğu görülmektedir. Bunlara ek olarak ise siber alanda azımsanamayacak yeteneklere sahip aktör çeşitliliğinde önemli bir artış yaşanmıştır. Özellikle 9/11 Terör Saldırıları sonrasında elektronik ağların potansiyel terörizm kullanımına olan açıklığının yarattığı endişe ve devletlerin siber alandaki istihbarat araçlarındaki yaşanan seçenek artışı, saldırgan enformasyon savaşı yeteneklerinin sessizce genişlemesine ve özellikle büyük aktörler tarafından benimsenmesine yol açmıştır. Siber alanın bu askerileşme süreci, sivil altyapıların hedef haline gelmesinden silahlı saldırılara ya da bilgi toplama, soruşturma ve propaganda şekillerine kadar çeşitli alanlarda soru işaretlerinin oluşmasına vesile olmuştur.[683] Bu dönemde giderek karmaşıklaşan siber olaylar ve medyanın siber olaylara artan ilgisi neticesinde siber güvenlik sorunları iki yönde ilerlemiştir: Uzman seviyesinden karar vericilere ve politikacılara uzanan yukarı yönlü etkiler ve sadece ABD, RF, ÇHC gibi büyük devletlerle ilgili bir konu olmaktan çıkarak daha fazla devleti ve aktörü doğrudan ilgilendiren tehdit unsurlarından başlıcası haline getiren yatay yönlü etkiler.[684] Bu etkiler bağlamında söz konusu militarizasyon aşamasında devletlerin bir taraftan siber güvenlik strateji belgeleri yayınlamaya başladıkları görülürken, bir taraftan siber uluslararası işbirliği girişimleri söz konusu olmaktadır. Diğer taraftan ise saldırgan siber operasyonların önemli miktarlarda arttığı ve dahası devletler tarafından bu tarz saldırıların çoğunlukla organize edildiği belgelenir hale gelmektedir. Dolayısıyla da uluslararası siber norm inşasını teşvik edici etkiler olumsuz zarar almaktadır.[685] Siber olaylar tarihinin militarizasyon aşamasında yaşanan operasyonlar, yalnızca teknoloji ve stratejinin paradigma değişimini değil, aynı zamanda da güç düzenlemeleri ve genişletilmiş gelecek için yönetişim sorunlarının potansiyelini de göstermektedir. Dahası, mevcut savunma yapılarının yetersizliği, yargı sorumlulukları, gizlilik hakları ve güvenlik için hesap verilebilirlik gibi konularda devletlerin ve özel sektörün rollerinin sorunlu boyutlarını ortaya

---

683 Ronald J. Deibert, "Black Code Redux: Censorship, Surveillance, and the Militarization of Cyberspace", Editör: Megan Boler, *Digital Media and Democracy: Tactics in Hard Times,* The Massachusetts Institute of Technology Press, Massachusetts2008, ss. 152-153.

684 Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better", *2012 4th International Conference on Cyber Conflict (CYCON),* 5-8 Haziran 2012, Tallinn, ss. 1-2.

685 Brian M. Mazanec, *a.g.e.,* s. 186.

çıkarmaktadır.[686] Siber güvenlik açıklarına yönelik operasyonel veya taktiksel çözümlerin tasarlanmasının ve uygulanmasının zorluğu, asimetrik tehditlerin varlığının ve boyutunun giderek artması ve siber olayların öngörülemezliği karşısında uygun teknik ve taktik aksiyonların yeterli zaman içerisinde geliştirilememesi, siber aktörlerin güvenlik ve çıkarlarına dair endişelerinin büyümesine neden olmaktadır.[687] Böyle bir ortamda da karar vericilerin politikaları ve doktrinleri, doğal olarak siber savaş anlayışına kaymaktadır. 2010 yılındaki *Stuxnet* saldırısı, bu aşamanın en dikkat çeken ve kayıtlara geçen en büyük çaplı saldırılarından olmuştur. Dördüncü bölümde detaylandırılacak olan bu saldırı, siber alandaki çatışmaların gerçek dünyaya taşarak fiziksel olarak ve hatta potansiyel can kaybı boyutunda verebileceği zararın en iyi şekilde tecrübe edildiği örnek olmuştur. Yukarıda paylaşılan bilgiler ışığında, siber olaylar tarihinin militarizasyon aşaması olarak tanımlanan söz konusu sürecinde görülen, kayıtlara geçen ve tespit edilen siber olayları şu şekilde listelenmektedir:

Tablo-34: Militarizasyon Aşamasındaki Siber Olaylar (2003-Günümüz)

Tarih	Saldırı	Saldırgan	Hedef	Kategori
2003	Titan Rain / Byzantine Hades Operasyonu	Çin Kaynaklı Anonim Saldırganlar	Lockheed Martin, Sandia Ulusal Laboratuvarları, Redstone Arsenal, NASA, Amerikan Savunma Bakanlığı, İngiliz Savunma Bakanlığı	Siber Saldırı

[686] Jack Jarmon, "Cyber-Terrorism", *Journal on Terrorism and Security Analysis (JTSA)*, Cilt 6, Bahar 2011, ss. 106-107.
[687] James J. Wirtz, "The Cyber Pearl Harbor", Editörler: Emily O. Goldman & John Arquilla, *Cyber Analogies*, Technical Report: NPS-DA-14-001, Naval Postgraduate School, California 2014, s. 12.

Ocak, 2003	SQL Slammer Solucanı	Anonim	Dünya çapındaki İnternet Sunucularına DoS saldırıları gerçekleştirmiş ve İnternet trafiğini yavaşlatmıştır.	Kötü Amaçlı Yazılım
Ağustos, 2003	MS Blaster Solucanı	Anonim	Winodws XP ve Windows 2000 İşletim Sistemli Bilgisayarlar & ABD Kamu Kurum Bilgisayar Ağları	Kötü Amaçlı Yazılım
Aralık, 2003-Mayıs, 2005	Stakkato	İsveçli Bilgisayar Korsanı Philip Gabriel Pettersson	NASA, Amerikan Askeri Tesisleri, Çeşitli Üniversiteler ve Araştırma Merkezleri	Siber Saldırı
2005-2013	Poison Ivy RAT	Anonim	Çeşitli Hükümet Organizasyonları, Kimyasal Üreticileri, İnsan Hakları Grupları	Siber Saldırı
Ocak, 2004	MyDoom Virüsü	Anonim	Windows İşletim Sistemli Bilgisayarlar	Kötü Amaçlı Yazılım
2005-2012	Chinese Cyber Espionage	Çin Devlet Sponsorlu Bilgisayar Korsanları	ABD'deki Çeşitli Kamu ve Özel Sektör Kurumları	Siber Casusluk
2006	Shady RAT Operasyonu	Anonim	Birleşmiş Milletler, Uluslararası Olimpiyat Komitesi, Çeşitli Devlet Kurumları, İş Dünyası, Savunma Şirketleri	Siber Saldırı
2006-2011	Rustock Botnet	Anonim	Windows İşletim Sistemli Bilgisayarlar	Botnet

Nisan-Mayıs, 2007	Estonia	Anonim olmakla birlikte Rus Devlet Kaynaklı Bilgisayar Korsanlarının arkasında olduğu düşünülmektedir.	Estonya Devlet Kurumları, İş Dünyası ve Bankacılık Sektörü	Siber Saldırı veya Siber Savaş
2007	TJX Corporation Hack	Amerikalı Bilgisayar Korsanı Albert Gonzalez ve Anonim Saldırganlar	TJX Şirketleri Dataları	Siber Casusluk
Eylül, 2007	Orchard Operasyonu	İsrail Gizli Servisi, MOSSAD	Suriye'ye ait Nükleer Tesisin Güvenlik Sistemi	Siber Saldırı / Siber Savaş
2006-2016-Günümüz	WikiLeaks	Julian Assange Önderliğindeki Küresel Bilgisayar Korsanı Grubu.	Devletlere ve Kurumlara ait çeşitli gizli ve hassas bilgiler	Gizli Devlet Bilgilerinin Kamuya Açıklanması
2007	The Defence Industrial Base	Anonim	Amerikan Savunma Sanayi, silah tasarım ve elektronik sistemleri	Siber Casusluk
Temmuz, 2007	Zeus, ZeuS, or Zbot	Anonim	Windows İşletim Sistemli Bilgisayarlar	Botnet
2006-2009	Night Dragon Operasyonu	Çin Kaynaklı Anonim Siber Saldırganlar	ABD, Tayvan, Kazakistan ve Yunanistan'daki Küresel Enerji Şirketleri	Siber Saldırı / Siber Savaş
2008	Buckshot Yankee Operasyonu	Rus Kaynaklı Anonim Saldırganlar	ABD Askeri Bilgisayar Ağları	Siber Saldırı / Siber Savaş

2008	Georgia	Rus Devlet Sponsorlu Bilgisayar Korsanları	Gürcistan Devletine ait Kurumlar ve Çevrimiçi Sayfalar	Siber Saldırı / Siber Savaş
Kasım, 2008	Conficker Solucanı	Anonim	Windows İşletim Sistemli Bilgisayarlar	Kötü Amaçlı Yazılım
Aralık, 2008-Ocak, 2009	Operation Cast Lead	Arap ve Müslüman dünyasına ait Anonim Bilgisayar Korsanları ve İsrailli Bilgisayar Korsanları	İsrail Çevrimiçi Siteleri, Hamas Televizyon İstasyonu, Anti-İsrail Çevrimiçi Sayfaları	Siber Saldırı / Siber Savaş
2009	Joint Strike Fighter (JSF)	Çin Kaynaklı Anonim Bilgisayar Korsanları	Müşterek Saldırı Uçağı Tasarım ve Elektronik Dataları	Siber Casusluk
2009	GhostNet	Çin Devlet Sponsorlu Bilgisayar Korsanları	103 ülkede 1000'den fazla bilgisayardaki diplomatik, siyasi, ekonomik ve askeri bilgiler	Siber Casusluk
Temmuz, 2009	The Korean DDoS Saldırıları	Kuzey Kore Kaynaklı Anonim Saldırganlar	ABD ve Güney Kore'ye ait çeşitli devlet kurumları	Siber Saldırı / Siber Savaş

Aralık, 2009-Ocak, 2010	Aurora Operasyonu	Çin Devlet Sponsorlu Bilgisayar Korsanları	Google, Adobe Systems, Juniper Neyworks, Rackspace, Yahoo!, Symantec, Northrop Grumman, Morgan Stanley, Dow Chemical, BlackBerry	Siber Saldırı / Siber Savaş
Şubat, 2010	Australian Cyberattacks	"Anonymous" isimli Hacktivist Grubu	Avusturalya Devleti Çevrimiçi Sayfaları	Siber Saldırı
Haziran, 2010	Stuxnet (Olympic Games)	ABD ve İsrail Devlet Sponsorlu Bilgisayar Korsanları	İran Nükleer Çalışmaları	Siber Saldırı / Siber Savaş
Eylül, 2010	Payback Operasyonu	"Anonymous" isimli Hacktivist Grubu	WikiLeaks'ten bankacılık olanaklarını geri çeken bankalar başta olmak üzere çeşitli kurumlar: Amazon, MasterCard, Visa, PayPal, Pirate Bay, Motion Picture Association of America (MPAA)	Siber Saldırı
Mayıs, 2011	Operation Potao Express	Anonim	Ukrayna, Belarus ve Rusya'daki yüksek değerli hedefler	Cyber Espionage
Şubat, 2011	Canadian Government Hackings	Çin Kaynaklı Anonim Bilgisayar Korsanları	Kanada Devlet Kurumları	Siber Saldırı / Siber Savaş

Mart, 2011	FinFisher / FinSpy	Lench IT Soultions plc tarafından pazarlanan bu gözetleme yazılımı, lisanslı olarak satılmaktadır.	Yazılıma sahip olanların hedefleri doğrultusunda kullanılmaktadır.	Siber Casusluk
Nisan, 2011	Stars Virus	Amerikan Kaynaklı Anonim Bilgisayar Korsanları	İran'daki çeşitli kurumlarda kullanılan Windows İşletim Sistemli Bilgisayarlar	Kötü Amaçlı Yazılım
Eylül, 2011	Duqu 1.0 & 2.0	İsrail Devlet Sponsorlu Bilgisayar Korsanları	Başta İran olmak üzere çeşitli ülkelerdeki endüstriyel kontrol sistemleri	Siber Saldırı / Siber Savaş
Şubat, 2012	Mahdi	İran Kaynaklı Anonim Bilgisayar Korsanları	İran ve diğer Orta Doğu ülkelerindeki yaklaşık 800 bilgisayar	Kötü Amaçlı Yazılım
Nisan, 2012	Opi Israel/OpIsrael	"Anonymous" isimli Hacktivist Grubu	İsrail Devlet Kurumları ve Çevrimiçi Sayfaları	Siber Saldırı / Siber Savaş
Mayıs, 2012	Flame Solucanı	Anonim	Windows İşletim Sistemli Bilgisayarlar	Kötü Amaçlı Yazılım
Haziran, 2012	Gauss Solucanı	Anonim	Çoğunlukla İsrail, Filistin ve Lübnan topraklarındaki Windows İşletim Sistemli Bilgisayarlar	Kötü Amaçlı Yazılım
Ağustos, 2012	Saudi Aramco Saldırısı / Shamoon Virüsü	İran Kaynaklı Anonim Bilgisayar Korsanları	Saudi Aramco Petrol Firması	Siber Saldırı / Siber Savaş

Eylül-Ekim, 2012	Ababil Operasyonu	İran Devlet Sponsorlu "Izz ad-Din al-Qassam Siber Savaşçıları" isimli Bilgisayar Korsanları Grubu	Amerikan Finansal Kurumları: Bank of America, New York Stock Exchange, Chase Bank, Capital One, SunTrust, Regions Bank	Siber Saldırı / Siber Savaş
2012-2013	The New York Times Saldırısı	Çin Kaynaklı Anonim Bilgisayar Korsanları	The New York Times Çevrimiçi Sayfası ve Dataları	Siber Casusluk
Aralık, 2012	Dexter	Anonim	Windows İşletim Sistemli Bilgisayarlar ve PoS Sistemleri	Kötü Amaçlı Yazılım
Mart, 2013	South Korea Cyberattack	Kuzey Kore ve ABD Kaynaklı Anonim Bilgisayar Korsanları	Güney Kore'deki çeşitli bankalar ve televizyon kanalları	Siber Saldırı / Siber Savaş
Mayıs, 2013-Ocak, 2014	Michaels Stores Saldırısı	Anonim	Michaels Stores şirketinin yaklaşık üç milyon müşterisinin kredi kartı ve mail bilgileri çalındı.	Siber Saldırı / Siber Casusluk
Haziran, 2013	Edward Snowden's NSA Leaks	Edward Snowden, elektronik iletişim ile ilgili veriler yönelik Amerikan Ulusal Güvenlik Dairesi'nin (NSA) gizli programlarını açıklamıştır.	ABD Ulusal Güvenlik Dairesi (NSA)	Gizli Devlet Bilgilerinin Kamuya Açıklanması

Kasım, 2013	Singapore Cyberattacks	"Anonymous" isimli Hacktivist Grubu	Singapur Devlet Kurumları ve Siyasi Partilerin Çevrimiçi Sayfaları	Siber Saldırı
Aralık, 2013	Target Corporation Hack / Target Data Breach	Anonim	Target Corporation kapsamındaki yaklaşık 40 milyon kredi kartı ve 70 milyon civarı e-mail adresi ve müşteri bilgisi çalındı.	Siber Saldırı / Siber Casusluk
Ocak, 2014	Havex	Anonim	ABD ve Avrupa'daki çeşitli enerji, havacılık, petrokimya, savunma ve ilaç sektörü firmaları	Kötü Amaçlı Yazılım
Eylül, 2014	JPMorgan Chase Hack	Dört Bilgisayar Korsanı: İsrailli Gery Shalon ve Ziv Orenstein, Amerikalı Joshua Samuel Aaron ve kimliği belirlenemeyen bilgisayar korsanı	JPMorgan Chase yatırım bankasının yaklaşık 83 milyon müşterisinin bilgileri ve hesapları çalındı.	Siber Saldırı / Siber Casusluk
Eylül, 2014	Home Depot	Anonim	Home Depot şirketinin yaklaşık 56 milyon müşterisinin kredi kart bilgileri ile 53 milyon müşterisinin de e-mail bilgileri çalındı.	Siber Saldırı / Siber Casusluk

Kasım, 2014	Sony Pictures Hack	Kuzey Kore Kaynaklı Anonim Bilgisayar Korsanları	Kuzey Kore lideri Kim Jong-un'un suikastini tasvir eden The Interview isimli filmin yayınlanması engellemek için California'daki Sony Pictures Entertainment sunucularına saldırıldı.	Siber Saldırı
2014-2019	ISIS Hacking Division Attacks	IŞİD'e bağlı Bilgisayar Korsanları	Fransız TV5Monde kanalı, Avustralya havalimanı çevrimiçi sayfası, ABD'nin çeşitli kurumları, İngiliz devlet görevlilerinin mailleri ve çeşitli Twitter hesapları	Siber Saldırı / Siber Savaş
Şubat, 2015	Anthem Healthcare Attack	Asya Kaynaklı Anonim Bilgisayar Korsanları	Sağlık sigortası şirketi olan Anthem Inc.'ye kayıtlı yaklaşık 79 milyon kişinin kişisel bilgileri ve Sosyal Güvenlik numaraları çalındı.	Siber Saldırı / Siber Casusluk
Aralık, 2015	Ukrayna Güç Dağıtım Şebekesi Saldırısı	Rus Kaynaklı Anonim Bilgisayar Korsanları	Ukrayna'nın elektrik dağıtım şirketleri SCADA sistemleri	Siber Saldırı / Siber Savaş
Mart, 2016 – Haziran, 2017	Petya & NotPetya	Rus Kaynaklı Anonim Bilgisayar Korsanları	Windows İşletim Sistemine sahip bilgisayarlar, dünya çapında çeşitli kurumlar. 2017 yılında ise başta Ukrayna olmak üzere çeşitli ülkeler doğrudan hedeflenmiştir.	Siber Saldırı / Siber Savaş

Mayıs, 2016	Panama Papers	"John Doe" takma isimli muhbir, Panama kaynaklı *Mossack Fonseca* hukuk firmasından 11.5 milyondan fazla belgeyi *Süddeutsche Zeitung* gazetesine servis etmiştir.	Çeşitli kurumlar, yöneticiler, siyasetçiler, üst düzey devlet yetkilileri	Gizli Devlet Bilgilerinin Kamuya Açıklanması
Mayıs, 2017	WannaCry	Kuzey Kore Kaynaklı Anonim Bilgisayar Korsanları	Windows İşletim Sistemine sahip bilgisayarlar, dünya çapında çeşitli kurumlar ve üniversiteler: Telefónica, NHS, FedEx, TSMC, Nissan, Renault, Deutsche Bahn, Hitachi	Siber Saldırı

Kaynak: Max Smeets & Jason Healey, "Cyber Conflict History", *Tech & Policy Initiative, Working Paper Series 2*, Cyber Conflict Studies Association (CCSA), School of International and Public Affairs (SIPA), 2017, ss. 203-212.; Jeffrey Carr, *Inside Cyber Warfare*, O'Reilly Media, Inc., California 2010.; Paul J. Springer, *Encyclopedia of Cyber Warfare*, ABC-CLIO, California 2017.; Richard Stiennon, "A Short History of Cyber Warfare", Editör: James A. Green, *Cyber Warfare: A Multidisciplinary Analysis*, 1. Basım, Routledge, New York 2015, ss. 7-32.; Alexander Gamero-Garrido, *Cyber Conflicts in International Relations: Framework and Case Studies*, Explorations in Cyber International Relations (ECIR) Working Paper, MIT & Harvard University, 2014.; Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, ABC-CLIO, California 2013.; Omry Haizler, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking", *Cyber, Intelligence, and Security*, Cilt 1, Sayı 1, Ocak 2017, ss. 31-45.; Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, 1. Basım, Simon & Schuster, New York 2016.; Bruce Middleton, *A History of Cyber Security Attacks: 1980 to Present*, CRC Press, New York 2017.; Mike Chapple & David Seidl, *Cyberwarfare: Information Operations in a Connected World*, Jones & Barlett Learning, Massachusetts 2015.; A. Kiyuna & L. Conyers, *Cyberwarfare Sourcebook*, Lulu.com, 2015.; Vanessa Pitts, *Cyber Crimes: History of World's Worst Cyber Attacks*, Alpha Editions, Vij Books, Darya Ganj 2017.; Kenneth Geers, *Strategic Cyber Security*, NATO Cooperative Cyber Defence Centre of Excellence (NATO-CCDCOE) Publication, Tallinn Haziran 211.; Center For Strategic & International Studies (CSIS), "Significant Cyber Incidents", *https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents*, (Erişim Tarihi: 28 Nisan 2020).

4. 21. Yüzyılın Öne Çıkan Siber Uluslararası İlişkiler Örnek Olayları

21. yüzyıl, Uluslararası İlişkilerin siber alanda en yoğun görüldüğü ve söz konusu alanın sınırlarının reel dünyanın çeşitli boyutlarını kapsayacak şekilde derinleştiği bir süreç olarak nitelendirilmektedir. Aynı zamanda siber olaylar tarihinin birinci ve ikinci aşamalarında yaşanan siber alana yönelik ciddiyetin farkına varma, kötü amaçlara hizmet edebilme boyutları, güvenlik gereklilikleri ve siber eylem çeşitliliğinin geliştirilmesi gibi durumlar, üçüncü aşama olarak nitelendirilen militarizasyon sürecinin 2003 yılındaki Titan Rain Operasyonu ile başlaması neticesinde farklı bir boyuta evrilmiştir. Buna göre artan aktör ve siber eylem çeşitliliği, yerel ve küresel boyutlarda karmaşık, çok yönlü, eş zamanlı ve muazzam boyutlarda zararlar yaratabilmenin yanı sıra fiziksel hayatta tahmin edilemeyecek seviyelerde doğrudan yıkım oluşturuabilir hale evrilmiştir. Birinci ve İkinci aşamalarda çoğunlukla siber casusluk türünde gerçekleşen olaylar, 21. Yüzyıl itibariyle yaşanan bu Üçüncü aşamada yoğunlukla siber saldırı ve siber savaş şeklinde gerçekleşmektedir. Dolayısıyla ilk iki aşamaya kıyasla çok daha büyük etkiler ve sonuçlar oluşmaktadır. Bu bölümde 21. yüzyılın en dikkat çeken Siber Uluslararası İlişkiler olayları olarak şunlar tespit edilmiştir: Titan Rain Operasyonu (2003), Estonya Saldırıları (2007), Gürcistan Saldırıları (2008), Stuxnet Saldırısı (2010), WikiLeaks (2010), Snowden (2013) ve Ukrayna Saldırıları (2017). Takip eden alt başlıklarda söz konusu olaylar sırasıyla detaylandırılacaktır.

4.1. Titan Rain Operasyonu (2003)

2000'li yılların başıyla birlikte siber alanda Çin'in aktörel etkileri doğrudan görülmeye başlamıştır. ABD'nin savunma ağlarını hedefleyerek sistematik olarak taramaya ve sızmaya çalışan Çinli siber aktörler, çoğunlukla Amerikan Savunma Bakanlığı ile enerji ve iç güvenlik birimlerine saldırılar gerçekleştirmişlerdir. Çin devlet sponsorlu olduğundan şüphelenilen anonim siber aktörlerin saldırıları ABD Hükümeti tarafından ilk olarak 2005 yılında açıklanmış ve 2003 yılından beri saldırıların sistematik olarak Amerikan kurumlarını hedeflediği belirtilmiştir.[688] Saldırıların Çin kaynaklı olduğu tespit edilmesine rağmen saldırganların gerçek kimlikleri bilinememekte olduğundan ve tek bir saldırıdan ziyade zamana yayılan bir dizi siber saldırıdan oluştuğu için Amerikan Hükümeti tarafından "Titan Rain Operasyonu" (*Operation Titan Rain*) olarak adlandırılmıştır. Gelişmiş kalıcı tehdit (*advanced persistent threat*, APT) olarak sınıflandırılan saldırılarda zombi bilgisayarları, proxy sunucuları, virüs ve casus yazılım bulaşmış kaynaklar kullanıldığından saldırıların bireysel mi, kurumsal mı yoksa devlet destekli mi olduğuna dair doğasının belirlenmesini oldukça zorlaştırmıştır.[689] 2001 yılında "*Red Code*" ve "*Lion*" adı verilen solucanlar kullanılarak başlayan bilgi tahribatı saldırıları, kolaylıkla tespit edilen ve tehdit olmaktan öte zaman kaybettiren küçük çaplı saldırılar olarak kayıtlara geçmiş, 2003 yılından itibaren ise saldırıların boyutları ve yapılanmaları değişmeye başlamıştır. Sandia Ulusal Laboratuarı'nda (*Sandia National Laboratory*, SNL) ağ güvenlik analisti olarak çalışan Shawn Carpenter, *Lockheed Martin* şirketine gerçekleştirilen bir dizi saldırıyı araştırırken benzer saldırıların birkaç ay öncesinde SNL'e yönelik de başladığını tespit etmiş ve saldırganların izini Çin'in Guangdong eyaletine kadar takip edebilmiştir.[690] 2003 ila 2007 yılları arasındaki saldırıların hedefleri arasında SNL, *Lockheed Martin*, NASA, *Redstone Arsenal*, ABD Savunma İstihbarat Teşkilatı (*U.S. Defense Intelligence Agency*, DIA), İngiliz Savunma Bakanlığı (*British Ministry of Defense*, MoD), ABD Ordusu Bilgi Sistemleri Mühendisliği Komutanlığı (*U.S. Army Information Systems*

[688] Council on Foreign Relations, "Titan Rain", Ağustos 2005, *https://www.cfr.org/interactive/cyber-operations/titan-rain*, (Erişim Tarihi: 29 Nisan 2020).
[689] Paul J. Springer, *a.g.e.*, s. 227.
[690] Gary Adkins, "Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism", *Journal of Strategic Security*, Cilt 6, Sayı 3, Güz 2013, s. 6.

Engineering Command, USAISEC), Savunma Bilgi Sistemleri Teşkilatı (*Defense Information Systems Agency*, DISA) gibi son derece kritik kurumların altyapı sistemleri yer almıştır.[691]

Titan Rain Operasyonu, ABD Hükümeti ve askeri sistemlerine ait gizli bilgilere geniş çaplı erişim ihlali sağlayan siber casusluk saldırıları dizisi olarak kabul edilmektedir. Bu saldırılar neticesinde 2003-2007 döneminde ABD İnternet trafiğine ve ABD Savunma Bakanlığı'na ait yaklaşık 10 ila 20 terabayt arasında çok gizli verilerin kaybının yaşandığı belirtilmiştir.[692] İlk saldırılarda orduya ait gizli ağlar İnternete bağlı olmadığından hedef olmamasına rağmen yine ABD Hükümetine ve Savunma Bakanlığı'na ait gizli olmayan ağlardaki özellikle silahlı kuvvetlerin lojistiğine dair hassas bilgilerin hedeflendiği tespit edilmiştir. Sonrasında analistlerin yoğunlaştırdığı çalışmalar neticesinde saldırıların sıklığının ve etkisel yoğunluğunun giderek artarak gizli ağlara kadar ulaştığı görülmüştür. Titan Rain saldırganlarının Çin Hükümeti ile doğrudan ilişkili olup olmadıkları tespit edilememekle birlikte endüstriyel bilgi toplama, rakip ülkenin savunma sistemlerine sızma ya da bir siber aktörün/topluluğun siber yeteneklerini test etme tatbikatı gibi çeşitli amaçlara hizmet edebileceği düşünülmekte ve ABD Hükümeti açısından ise gelecekte yaşanabilecek olası büyük saldırılara karşı uyarı niteliği oluşturmaktadır.[693]

Özellikle 2006-2007 yılındaki saldırılarda ABD dışında başta Almanya ve İngiltere olmak üzere bir dizi Batı Avrupalı devlet söz konusu saldırılara maruz kaldıklarını açıklamıştır. Bu dönemde Alman Şansöylesi Angela Merkel ile eski ABD Savunma Bakanı Robert Gates'in bilgisayarları saldırıya uğramış, İngiliz Hükümeti'ne ait Dışişleri Ofisi ile çeşitli kilit departmanların bilgisayar ağlarına müdahaleler gerçekleştirilmiş ve hatta Avam Kamarası'nın bilgisayar sisteminin bir kısmının erişime kapatılması söz konusu olmuştur.[694] Diğer taraftan ise saldırganlar

---

[691] Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt & Joseph Weiss, *a.g.e.*, s. 233.

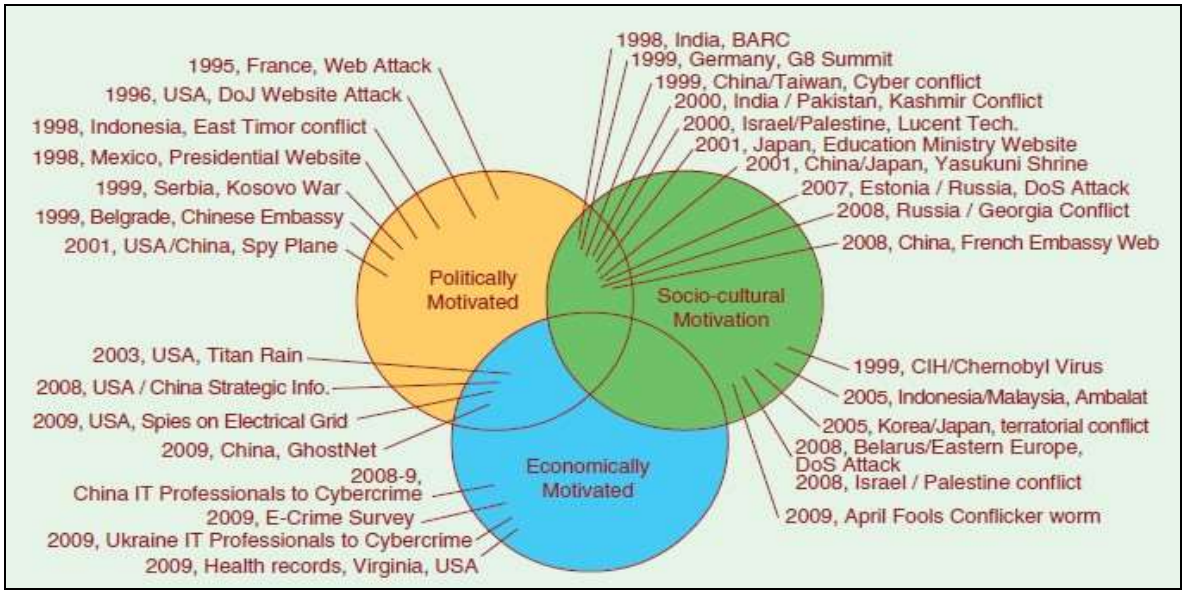
[692] Yiannos Charalambides, "The Invisible Cyber War", *21st Century*, Cilt 13, Sayı 1, 2013, s. 23.

[693] Nathan Thornburgh, "Inside The Chinese Hack Attack", Time, 25 Ağustos 2005, *http://content.time.com/time/nation/article/0,8599,1098371,00.html*, (Erişim Tarihi: 29 Nisan 2020).

[694] Jan-Frederik Kremer & Benedikt Müller, "SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World", Editörler: Jan-Frederik Kremer & Benedikt Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer-Verlag, Berlin Heidelberg 2014, s. 52.; Richard Norton-Taylor, "Titan Rain – How Chinese Hackers Targeted Whitehall", The Guardian, 5 Eylül 2007,

tarafından ABD'nin askeri telekomünikasyon ağlarının haritalaması yapılarak, kimin kiminle ve hangi yöntemle iletişim kurduğu gözlemlenmiştir. Dolayısıyla siber alanda Çin'in belirleyici bir aktör olarak öne çıkabilmesinin gerekliliği olan siber keşiflerin Titan Rain Operasyonları ile başladığı iddia edilebilmektedir.[695] Buna karşın, Çinli Hükümet yetkilileri tarafından Titan Rain Operasyonu saldırılarının sorumluluğu ısrarla reddedilmiş ve bilgisayar korsanlarının kendilerini gizlemek adına Çin ağlarını kullandığına dair değerlendirmeler kamuoyuna servis edilmiştir.[696] Ek olarak Çin'in ABD, İngiltere gibi büyük devletlerle olan ikili ilişkilerine zarar vermek amacıyla bu saldırıların planlandığını ifade eden Çinli görüşlerin aksine ABD tarafından dünyanın en aktif ve kalıcı siyasi ve ekonomik motivasyonlu casusluk faillerinin başında Çin hedef gösterilmiştir.

Tablo-35: Siber Saldırıların Motivasyonel Boyutları



Kaynak: Robin Gandhi, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu & Phillip Laplante, "Dimensions of Cyber-Attacks: Social, Political, Economic, and Cultural", *IEEE Technology and Society Magazine*, Cilt 30, Sayı 1, Bahar 2011, s. 31.

---

https://www.theguardian.com/technology/2007/sep/04/news.internet, (Erişim Tarihi: 29 Nisan 2020).

[695] John J. Tkacik, Jr., "Trojan Dragon: China's Cyber Threat", *Backgrounder*, The Heritage Foundation, Sayı 2106, 8 Şubat 2008, ss. 3-4.

[696] Ryan Richard Gelinas, *Cyberdeterrence and The Problem of Attribution*, (Georgetown University, Faculty of the Graduate School of Arts and Sciences, Basılmamış Master Tezi), Washington, D.C. Nisan 2016, s. 19.

Tablo 35'deki Venn şemasında sunulduğu üzere 2003 yılında başladığı tespit edilen Titan Rain Operasyonu saldırıları, ilk geniş kapsamlı siyasi ve ekonomik motivasyonlu saldırılar olması hasebiyle siber olaylar tarihindeki militarizasyon aşamasının ilk gelişmesi olarak nitelendirilmiştir.[697] Netice olarak Çin kaynaklı olan bu saldırıların kısa ve uzun vadeli etkileri oldukça büyük olmuştur. NSA ve ABD Siber Komutanlığı (USCYBERCOM) tarafından ABD'ye yönelik gerçekleştirilen bu siber casusluk saldırılarının tarihin en büyük vurgunlarından biri olduğu ve fikri mülkiyet hırsızlığı üzerinden Amerikan şirketlerine yıllık maliyetinin yaklaşık 250 Milyar Doları bulduğu belirtilmiştir.[698] 2013 yılındaki *Mandiant* siber güvenlik firması tarafından yayınlanan raporda belirtildiği üzere 2003 yılından beri giderek artan sayıda Çin kaynaklı bilgi hırsızlığı siber saldırılarının, ABD Hükümetini, bakanlıklarını, altyapısını ve finans sektörünü hedef aldığı gözlenmiştir.[699] Başta *Google*'un kaynak kodu ve silah sistemleri tasarımları olmak üzere kullanıcı adları, şifreler ve pek çok gizli bilginin ilerleyen dönemlerdeki "*Byzantine Hades*", "*GhostNet*", "*Aurora*" gibi çeşitli siber casusluk saldırılarında çalındığı belirtilmiştir.[700] ABD hedefli Çin siber operasyonları halen devam etmekle birlikte ABD ile Çin arasında yaşanan siber savaşın boyutları ve kapsamı her geçen gün daha da derinleşmektedir. Bu bağlamda uluslararası hukuk, uluslararası işbirliği ve organizasyonların gerekliliği her zamankinden çok daha önemli görünmektedir. Öyle ki, reel dünyanın iki süper gücünün siber alanda yaşadıkları sürtüşme ve savaş halinin boyutlarının ve etkilerinin nerelere kadar ulaşabileceği öngörülememekle beraber oluşturabileceği risk faktörünün oldukça büyük olduğu düşünülmektedir.

---

[697] Robin Gandhi, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu & Phillip Laplante, "Dimensions of Cyber-Attacks: Social, Political, Economic, and Cultural", *IEEE Technology and Society Magazine*, Cilt 30, Sayı 1, Bahar 2011, s. 32.

[698] Paul J. Springer, *a.g.e.*, s. 229.

[699] The Mandiant Report, "APT1: Exposing One of China's Cyber Espionage Units", Mart 2013, s. 26, *https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf*, (Erişim Tarihi: 29 Nisan 2020).; Nadiya Kostyuk, "The Digital Prisoner's Dilemma: Challenges and Opportunities for Cooperation", *2013 World Cyberspace Cooperation Summit IV (WCC4)*, 4-6 Kasım 2013, California, s. 3.

[700] Dorothy Denning, "Cyberwar: How Chinese Hackers Became A Major Threat To The U.S.", Newsweek, 10 Mayıs 2017, *https://www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-678378*, (Erişim Tarihi: 29 Nisan 2020).

4.2. Estonya Saldırıları (2007)

2007 yılının Nisan ayı başlarında Estonya Hükümeti, başkent Tallinn'in merkezindeki Tõnismägi Parkında yer alan ve "Bronz Asker" (*The Bronze Soldier*) olarak bilinen heykelin, şehrin dışında kalan Tallinn Askeri Mezarlığına taşınması kararını duyurmuştur. Bunun nedeni olarak ise II. Dünya Savaşı esnasında Nazi Almanyası ile savaşırken hayatını kaybeden Sovyet askerlerinin anısına dikilen bu heykelin, Estonya'nın Sovyet kurtuluşu ve dolayısıyla yabancı işgali olarak algılanması gösterilmiştir.[701] 1947 yılında Sovyet yetkililer tarafından dikilen bu anıt, başlangıçta "Tallinn Kurtarıcıları Anıtı" (*Monument to the Liberators of Tallinn*) olarak adlandırılmıştır. Estonya'da yaşan Rus kökenli vatandaşlar için Nazizme karşı Sovyetlerin kazandığı zaferi temsil eden bu anıt, etnik Estonyalılar açısından ise yarım asırlık Sovyet baskısının ve işgalciliğin acı verici bir sembolü olarak görülmüştür.[702] Dolayısıyla 2007 yılında yaşanan saldırıların özünde Estonya ile Rusya arasındaki ikili ilişkilerde yaşanan çekişmeli uzun tarih ve etnik nüfus arasındaki sorunlar yatmaktadır. 1940 yılındaki Baltık ülkelerinin Sovyet ilhakı ve sonrasındaki Soğuk Savaş süreci boyunca Doğu Bloku'ndaki uyumun arttırılması ve Estonya kültürünün Ruslaştırılması amacıyla çok sayıda Rus vatandaşı Estonya'ya taşınmıştır. Günümüzde Estonya nüfusunun etnik dağılımına bakıldığında bu durum çok daha net anlaşılmaktadır: Estonyalı (%68.7), Rus (%24.8), Ukraynalı (%1.7), Belarus (%1), Fin (%0.6) ve diğer (%3,2).[703] Soğuk Savaşın sona ermesi ve SSCB'nin dağılmasının ardından ise Estonya Hükümeti, kültürü üzerindeki Rus etkilerini en aza indirecek politikaları yoğunlukla tercih etmiştir. 2004 yılında NATO'ya katılmasına rağmen Estonya, Rusların niyetlerine ve saldırganlığına karşı güvensiz yaklaşmaya devam etmiştir. Böyle bir arka plana sahip Estonya-Rusya ilişkileri, 27 Nisan 2007 tarihinde söz konusu anıtın kaldırılmasıyla iyice gerilmiştir. İki gece boyunca Rus kökenli vatandaşlar sokağa dökülmüş, çeşitli saldırılar ve

---

[701] Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", *Journal of Conflict & Security Law*, Cilt 17, Sayı 2, 2012, s. 218.

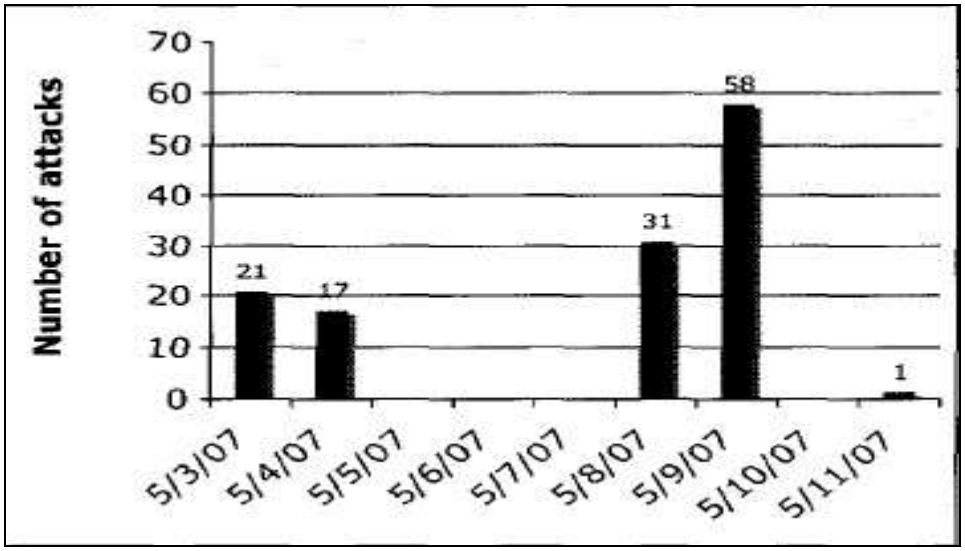
[702] Damien McGuinnes, "How A Cyber Attack Transformed Estonia", BBC News, 27 Nisan 2017, *https://www.bbc.com/news/39655415*, (Erişim Tarihi: 1 Mayıs 2020).; Mark Landler & John Markoff, "In Estonia, What May Be The First War In Cyberspace", 28 Mayıs 2007, *https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html*, (Erişim Tarihi: 1 Mayıs 2020).

[703] CIA, "The World Factbook: Estonia", *https://www.cia.gov/library/publications/the-world-factbook/geos/en.html*, (Erişim Tarihi: 1 Mayıs 2020).

yağmalamalar yapılmıştır. Yaşanan olaylarda toplamda 156 kişi yaralanmış, yaklaşık 1000 kişi gözaltına alınmış ve 1 kişi hayatını kaybetmiştir.[704]

Diğer taraftan bu şiddetli protestolara ek olarak Estonya'ya yönelik siber saldırılar gerçekleşmeye başlamıştır. Başta devlet kurumları olmak üzere, medya istasyonları, bankalar ve çeşitli özel sektör kurumları yoğun spam ve DDoS saldırılarına maruz kalmıştır. Öyle ki başlangıçta bu saldırılar, oldukça acemice organize edilmiş ve siber savunma sistemleri tarafından kolaylıkla hafifletilmiştir. Nisan ayının son günü itibariyle ise DDoS saldırıları çok daha organize ve çok yönlü hale gelmiştir.[705] Saldırıların kapsamında ve teknik seviyesinde yaşanan bu artış, Estonya sunucularının DNS sistemini ana hedef haline getirmiş ve Estonya İnternet Servis Sağlayıcılarını ve Estonya medyasını da kapsayacak şekilde genişlemiştir.[706]

Tablo-36: Saldırı Sayıları



Kaynak: William A. Barletta, "Cyberwar or Cyber-Terrorism: The Attack On Estonia", *International Seminar on Nuclear War and Planetary Emergencies*, The Science and Culture Series, Nuclear Strategy and Peace Technology, 38th Session, 19-24 Ağustos 2007, Erice, İtalya 2008, s. 482.

[704] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, Cilt 4, Sayı 2, Yaz 2011, ss. 50-51.
[705] Russell Buchan, *a.g.m.*, s. 218.
[706] Kari Alenius, "Victory in Exceptional War: The Estonian Main Narrative of the Cyber Attacks" , Editörler: Jari Rantapelkonen & Mirva Salminen, *The Fog of Cyber Defence*, National Defence University, Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection No 10, Helsinki 2013, s. 80.

2 ile 5 Mayıs 2007 tarihleri arasında dünya çapındaki İnternet Servis Sağlayıcılarının işbirliği ile saldırıların kaynağı olarak tespit edilen Rus IP adresi gruplarından gelen trafiğin blokajının genişletilmesi ve Estonya bankacılık sisteminin tüm uluslararası İnternet trafiğinden uzaklaştırılması hedeflenmiştir. Buna karşın, Tablo-36'da da görüldüğü üzere 8 ve 9 Mayıs 2007 tarihlerinde çok daha yoğun ve organize saldırılar yaşanmıştır. Estonya Hükümeti, üç günlük durgunluğun ardından 8 ve özellikle 9 Mayıs –Nazi Almanyası'nın SSCB'ye resmen teslim olduğu 9 Mayıs 1945 tarihi "Zafer Günü" olarak kutlanmaktadır– tarihinde saldırıların en üst seviyeye ulaşması üzerine, Rusya'yı suçlayarak saldırıların arkasında Rus devlet yetkilerinin olduğu ve üç günlük durgunluk döneminde saldırıların Zafer Günü'ne denk gelecek şekilde organize edildiğini açıklamıştır.[707] 19 Mayıs 2007 tarihindeki son büyük dalganın ardından siber saldırılar aniden ve eş zamanlı şekilde durmuştur. DDoS saldırıları, daha önce de bahsedildiği üzere, doğası gereği kapsamlı veya onarılamaz hasarlara neden olmamakla birlikte önemli ölçüde bozulmaların ve aksamaların yaşanmasına neden olabilmektedir. Resmi ve resmi olmayan trafiğin ayırt edilmesinin zorluğu sebebiyle de DDoS saldırılarının önlenmesi oldukça zordur. Estonya'da gerçekleşen bu üç haftalık siber saldırıların alınan karşı önlemlere tepki olarak değişim gösterebilen dinamik yapısı ve eş zamanlı olarak durması, saldırıların devlet sponsorlu ve organize olduğu şüphelerinin daha da kuvvetlenmesine vesile olmuştur.[708]

Anıtın taşınması kararı sonrasında bozulan Estonya-Rusya ilişkileri, üç haftalık siber saldırılar boyunca Estonya Hükümetinin Rusları suçlayıcı açıklamalarıyla iyice gerilmiş ve Rus tarafından resmi olmayan ciddi yaptırımlar uygulanmıştır. Buna göre Rus tarafı, iki ülke arasındaki ticaret bağı açısından kritik öneme sahip otoyol köprülerinin ve Tallinn-St. Petersburg arasındaki demiryolunun acil onarıma ihtiyacı olduğu iddasıyla kullanıma kapatmış, Estonya'ya petrol, petrol ürünleri ve kömür teslimatlarını ulaşımın kesilmesine dayandırırarak durdurmuş ve

---

[707] William A. Barletta, "Cyberwar or Cyber-Terrorism: The Attack On Estonia", *International Seminar on Nuclear War and Planetary Emergencies*, The Science and Culture Series, Nuclear Strategy and Peace Technology, 38th Session, 19-24 Ağustos 2007, Erice, İtalya 2008, s. 482.

[708] The NATO Strategic Communications Centre of Excellence (NATO StratCom COE), "Hybrid Threats: 2007 Cyber Attacks on Estonia", *https://www.stratcomcoe.org/hybrid-threats-2007-cyber-attacks-estonia*, (Erişim Tarihi: 3 Mayıs 2020), ss. 53-54.

Rus medyası tarafından Estonya mallarına boykot çağrısı yapılmıştır.[709] Dahası, bu süreçte Estonya-Rusya adli yardım ve hukuki ilişkiler anlaşmalarına uygun olarak Estonya'nın adli kurumlarından Rus adli kurumlarına resmi olarak adli yardım talebi iletilmesine rağmen, anlaşmaların bu tarz olayları kapsamadığı gerekçesiyle Rus tarafından ilgili talepler reddedilmiştir.[710]

Bu arada, söz konusu saldırıların etki boyutu değerlendirilirken Estonya'nın siber yapısı da göz önünde bulundurulmalıdır. Yaklaşık 1.4 milyonluk nüfusa sahip bu küçük ülkede elektronik hizmetlere bağlılık üst seviyededir. "E-stonia" olarak da adlandırılan ve "kağıtsız hükümet" olarak bilinen bu ülkedeki kamu işlemlerinin neredeyse tamamı İnternet üzerinden gerçekleştirilmektedir. Ek olarak; bankacılık işlemlerinin %98'i elektronik olarak gerçekleştirilmekte ve nüfusun İnternete bağlılık oranı %90 üzerinde seyretmektedir. Yine Estonyalıların 2/3'nün geniş bant hizmeti bulunmakla beraber çalışan nüfusun %80'inden fazlası vergilerini çevrimiçi ödemektedir.[711] Siber alana bağımlılığın bu derece yüksek olduğu bir ortamda ülkenin sadece en büyük iki bankasına gerçekleştirilen yoğun DDoS saldırıları neticesinde iletişimin kesilmesinin maliyetinin 1 milyon Dolardan fazla olduğu tespit edilmiştir.[712] Elektronik hizmetlere olan yüksek bağımlılık ve Estonya'nın ağ yapısının bu tarz saldırılara karşı yüksek derecedeki savunmasızlığı, yaşanan siber saldırıların etkilerinin felaket boyutunda yaşanmasına neden olmuştur. Başta Estonya Cumhurbaşkanlığı ve Parlamentosu olmak üzere, Devlet Bakanlıkları, siyasi partiler, medya kanalları, bankacılık sektörü ve iletişim altyapısı doğrudan ve eş zamanlı olarak saldırı altında kalmış, kritik iş süreçlerinde kısmi duraksamalar yaşanmıştır. Kontrolden çıkan bu gidişatın tekrardan kontrol altına alınabilmesi adına NATO, AB, İsrail ve ABD'den çeşitli güvenlik uzmanları Tallinn'e gelmiş ve saldırılarının Estonya'nın güç ve su şebekelerine ulaşmasına fırsat tanınmadan kontrol altına alınmış ve yeniden normalleşme sağlanmıştır.[713]

---

[709] Alison Lawlor Russell, *Cyber Blockades*, Georgetown University Press, Washington, D. C. 2014, s. 78.
[710] William A. Barletta, *a.g.m.*, s. 482.
[711] Muhammad Saleem & Jawad Hassan, "'Cyber Warfare', The Truth In A Real Case", *Project Report for Information Security Course*, University of Linköping, Sweden, 2009, s. 2.
[712] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare", *NATO Science and Technology Organization RTO - Meeting Proceedings Paper*, ST-076/RSY-017, Tallinn, 10 Mart 2008, s. 10.
[713] Paul J. Springer, *Encyclopedia of Cyber Warfare*, ABC-CLIO, California 2017, ss. 104-105.

Netice olarak 2007 yılındaki Estonya saldırıları, bir ulus-devletin kararlarının ve eylemlerinin siber silahlar kullanılarak başka bir devletin sponsorluğundaki anonim kaynaklar –"Nashi" isimli devlet destekli Rus gençlik hareketi vb.– aracılığıyla etkilenmeye çalışıldığı ilk siber savaş örneği olarak kabul edilmektedir. Diplomatik bağlamdaki devletlerarası ilişkilerdeki hoşnutsuzluk, farklı bir boyutta değişik yöntemlerle ifade edilmiştir. Diğer taraftan dünyanın İnternete en bağımlı ülkelerinden biri olarak Estonya'ya güvenlik açığı konusunda ciddi mesajlar verilmiştir. Öyle ki Rus devlet yetkilileri tarafından saldırı sorumluluğunun ısrarla reddedilmesi, diğer taraftan Rusya'nın Estonya'ya "hacktivistler, gençlik hareketleri ve vatansever bilgisayar korsanları bu derece etki yaratabilirse, devletin doğrudan siber saldırısının şiddeti çok daha büyük ve sert olur" mesajı şeklinde yorumlar yaratmıştır. Daha da önemlisi ise ciddi bir siber saldırının potansiyel sonuçları, dünya tarafından ilk elden tecrübe edilmiştir.[714]

Öte yandan, bu saldırıların Estonya açısından etkileri politik, sosyal ve ekonomik bazlı gerçekleşmiştir. Siyasal etkiler açısından bakıldığında, kalıcı siyasi hasar tespit edilememekle birlikte siber saldırı süreci içerisinde devletin normal kanallar üzerinden vatandaşlarıyla iletişim kurması engellenmiş ve bu durum, devletin vatandaşlarına hizmet verebilme yeteneğinin kısıtlanması şeklinde yorumlanmıştır. Sosyal açıdan etkilere bakıldığında ise ilk defa barış zamanında bir ülkenin iletişim altyapısı saldırıya uğrayarak geçici olarak bozulmuştur. Halkın bu durumdan haberdar olmaması ve saldırıların ani ve yoğun gerçekleşmesi toplumsal panik ve korkuya yol açmıştır. Ekonomik etkiler ise özellikle bankacılık sektörünün zararlarına dayanmıştır ancak saldırıların yarattığı doğrudan maddi kaybın yanı sıra kritik altyapıların ve siber sistemlerin içinde bulunduğu siber güvenlik zafiyetinin telafi edilebilmesi adına yeni altyapı güvenlik ve koruma yatırım maliyetleri doğurmuştur.[715]

Diğer bir önemli husus ise bu üç haftalık yoğun saldırı süreci içerisinde Estonya'nın Kuzey Atlantik Antlaşması'nın 5. Maddesi'ne[716] dayanarak NATO'yu

---

[714] Emilio Iasiello, "Cyber Attack: A Dull Tool to Shape Foreign Policy", *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 4-7 Haziran 2013, Tallinn 2013, ss. 5-6.
[715] Alison Lawlor Russell, *a.g.e.*, ss. 80-81.
[716] "**Madde 5:** Taraflar, Kuzey Amerika'da veya Avrupa'da içlerinden bir veya daha çoğuna yöneltilecek silahlı bir saldırının hepsine yöneltilmiş bir saldırı olarak değerlendirileceği ve eğer böyle

çağırmasıyla ilgilidir. Buna göre Estonya, Rusya tarafından saldırıya uğradığını ve kolektif savunmaya ihtiyacı olduğunu açıklamış ancak NATO tarafından 2007 yılındaki Estonya siber saldırıları, 5. Madde'deki "silahlı saldırı" kapsamında değerlendirilmemiştir.[717] Bununla birlikte 2014 yılında gerçekleşen Galler Zirvesi'ndeki NATO-Ukrayna Komisyonu Ortak Beyanı'nda (*Joint Statement of the NATO-Ukraine Commission*) siber savunma, kolektif savunmanın temel bir parçası haline getirilerek, bir siber saldırının NATO'nun kurucu antlaşmasının 5. Maddesi'ndeki kolektif savunma çağrısına yol açabileceği ilan edilmiştir.[718] 2016 yılındaki Varşova Zirvesi'nde ise müttefiklerce siber alan, askeri operasyonların gerçekleştiği alanlardan biri olarak kabul edilmiş ve ayrıca ulusal ağların ve altyapıların siber güvenliğinin geliştirilmesi temel hedeflerden biri haline getirilmiştir.[719] Sonuç olarak 2007 Estonya saldırıları, hükümetin ve sivil toplumun işleyişini kesintiye uğratarak düşmanca bilgi akışları oluşturmuş ve düzgün çalışma yeteneklerini sekteye uğratmıştır. Bu bağlamda fiziksel unsurlara doğrudan maddi zarar verilmemesine rağmen Estonya varlığına karşı bir tür enformasyonel şiddet yaratılmıştır.[720] Söz konusu şiddet hali, sonraki dönemlerde gerçekleşecek saldırıların fiziksel boyutlara uzanabileceğinin habercisi olarak yorumlanmıştır.

---

bir saldırı olursa BM Yasası'nın 51. Maddesinde tanınan bireysel ya da toplu öz savunma hakkını kullanarak, Kuzey Atlantik bölgesinde güvenliği sağlamak ve korumak için bireysel olarak ve diğerleri ile birlikte, silahlı kuvvet kullanımı da dâhil olmak üzere gerekli görülen eylemlerde bulunarak saldırıya uğrayan Taraf ya da Taraflara yardımcı olacakları konusunda anlaşmışlardır. Böylesi herhangi bir saldırı ve bunun sonucu olarak alınan bütün önlemler derhal Güvenlik Konseyi'ne bildirilecektir. Güvenlik Konseyi, uluslararası barış ve güvenliği sağlamak ve korumak için gerekli önlemleri aldığı zaman, bu önlemlere son verilecektir." Detaylı bilgi için bkz.: NATO, "Kuzey Atlantik Antlaşması", 4 Nisan 1949, Washington, D. C., *https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=tr*, (Erişim Tarihi: 4 Mayıs 2020).

[717] Richard Stiennon, "A Short History of Cyber Warfare", Editör: James A. Green, *Cyber Warfare: A Multidisciplinary Analysis*, 1. Basım, Routledge, New York 2015, s.18.

[718] NATO, "Joint Statement of the NATO-Ukraine Commission", Wales Summit, 4-5 Eylül 2014, *https://www.nato.int/cps/en/natohq/news_112695.htm?selectedLocale=en*, (Erişim Tarihi: 4 Mayıs 2020).

[719] NATO, "Cyber Defence Pledge", Warsaw Summit, 8-9 Temmuz 2016, *https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en*, (Erişim Tarihi: 4 Mayıs 2020).; Ayrıca detaylı bilgi için bkz.: Laura Brent, "NATO's Role In Cyberspace", NATO Review, 12 Şubat 2019, *https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html*, (Erişim Tarihi: 4 Mayıs 2020).

[720] Samuli Haataja, " The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach", *Law, Innovation and Technology*, Cilt 9, Sayı 2, 2019, s. 188.

4.3. Gürcistan Saldırıları (2008)

Gürcistan ile Rusya arasındaki karmaşık ilişkilerin tarihi yüzlerce yıl öncesine dayanmaktadır. İki ülke halkı arasındaki bazı dini ve tarihi bağlara rağmen ilişkiler her daim karmaşık ve gergin yapıda olmuştur. Rus İmparatorluğu'nun uzun yıllar bir parçası olarak kalan Gürcistan, 1918 yılında bağımsızlığını elde etmiş, 1921 yılında ise Bolşevik Rusya tarafından işgal edilerek 1922 yılında oluşturulan SSCB'nin parçası haline getirilmiştir. 1991 yılında SSCB'nin dağılmasıyla bağımsızlığını geri kazanan Gürcistan'ın bağımsız enerji politikaları ve NATO'ya katılma niyeti, Rus-Gürcü ikili ilişkilerinin tekrardan gerilmesine neden olmuştur.[721] Gürcistan'ın 1992 yılında NATO ile ilişkilerini resmen başlatması ve 2002 yılında NATO üyeliği için başvuru yapması, Rus tarafı açısından NATO tehdidinin giderek artması ve Kafkaslar bölgesindeki Rus etkinliğinin azaltılması girişimi şeklinde okunmuştur.[722] 2008 yılındaki NATO Bükreş Zirvesi'nde (*The Bucharest Summit*), Ukrayna ile Gürcistan'ın üye eylem planına (*membership action plan*, MAP) başvurularının desteklendiği ve bu bağlamda ilişkilerin yoğunlaştırılacağı açıklaması yapılmıştır.[723] Bunun üzerine Rusya tarafından Gürcü hava sahasına daha büyük saldırılar gerçekleştirilmiş, Güney Osetya milisleri Gürcü vatandaşlara saldırılar başlatmış ve Rus silahlı kuvvetleri bölgeye yakın konumlanmaya başlamıştır. 2008 yılının Şubat ayında Kosova'nın bağımsızlığını ilan etmesi, Rusya tarafından Gürcistan sınırı içerisindeki ayrılıkçı Güney Osetya ve Abhazya'nın bağımsızlıklarının tanınması yönündeki baskısı, Rusların Gürcülere ait bir insansız hava aracını vurması, hem Gürcistan'ın hem de Rusya'nın bu iki bölgedeki asker saysını arttırması ve iki taraftan gelen sert söylemler neticesinde artan gerilim, 8 Ağustos 2008 tarihinde

---

[721] Mohan B. Gazula, *Cyber Warfare Conflict Analysis and Case Studies*, Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, Massachusetts Institute of Technology, Working Paper CISL# 2017-10, Massachusetts Mayıs 2017, s. 38.

[722] Ahmet Nafiz Ünalmış & Şafak Oğuz, "2008 Rusya-Gürcistan Savaşının Vekâlet Savaşı Teorisi Açısından İncelenmesi", *Karadeniz Araştırmaları*, Cilt 16, Sayı 61, 2019, s. 34.; David Kachkachisvili, "NATO'dan Rusya'ya 'Gürcistan'ın Egemenliğine Saygı Duy' Çağrısı", Anadolu Ajansı, 3 Ekim 2019, *https://www.aa.com.tr/tr/dunya/natodan-rusyaya-gurcistanin-egemenligine-saygi-duy-cagrisi/1601543*, (Erişim Tarihi: 5 Mayıs 2020).

[723] NATO, "Bucharest Summit Declaration", 3 Nisan 2008, *https://www.nato.int/cps/en/natolive/official_texts_8443.htm*, (Erişim Tarihi: 5 Mayıs 2020).

"Güney Osetya Savaşı" olarak da adlandırılan savaşın patlak vermesine neden olmuştur.[724]

Güney Osetya Savaşı, Rusya ile Gürcistan arasında tam ölçekli olarak beş gün süren kinetik bir savaştır. Buna karşın, Rusya ile Gürcistan arasındaki siber savaş, söz konusu kinetik savaştan bir ay öncesinde başlamıştır. 18-20 Temmuz 2008 tarihleri arasında Gürcistan Cumhurbaşkanı Mikheil Saakashvili'nin web sitesi, yalnızca Rusça botnetlerde görülen bir kod tabanına dayanan DDoS saldırısına uğramıştır. Gönüllü bir botnet izleme ekibi olan *ShadowServer* tarafından ABD'deki bir komut ve kontrol sunucusuyla DDoS saldırısı için iletişim kurduğu tespit edilen "*Machbot*" isimli botnetin Cumhurbaşkanlığı çevrimiçi sayfasını http, tcp ve icmp paketleriyle doldurarak 24 saat boyunca kullanılamaz hale getirdiği belirtilmiştir. Ayrıca aynı sunucu üzerindeki diğer devlet kurumlarına ait çevrimiçi siteler de erişime geçici olarak kapatılmıştır. Bu saldırılar, bir sonraki ayda gerçekleşecek olan kitlesel siber saldırıların ana provaları olarak yorumlanmaktadır.[725] Ağustos ayındaki sıcak savaşla birlikte ise siber saldırıların şiddeti giderek artmıştır. İnternet üzerindeki *Arbor Peakflow* ve *ATLAS* canlı trafik monitörleri tarafından siber saldırılar sırasında kaydedilen en yüksek bant genişliğinin 800 Mbps'in üzerine çıktığı gözlemlenmiş ve bir yıl önceki Estonya saldırılarına kıyasla çok daha yoğun ve şiddetli siber saldırıların yaşandığı görülmüştür.[726] Rus siber aktörler tarafından Gürcistan iletişim ağlarının sürekli olarak tarandığı bu dönemde, sıcak savaşın başlangıcına paralel olarak siber saldırılar şu şekilde gerçekleşmiştir: 8 Ağustos 2008 tarihinde Gürcistan Cumhurbaşkanlığı, Başbakanlığı, Dışişleri Bakanlığı ve Parlamentosunun resmi çevrimiçi sayfaları, bilgilendirici portallar ve Gürcü olmayıp Gürcistan'ı destekleyen medya siteleri ve forumlar kullanılamaz hale getirilmiştir. 9 Ağustos 2008 tarihinde Gürcistan'ın o dönemki en büyük ticari bankası olan *TBC Bank*'in çevrimiçi işlemlerine saldırılmıştır. 10 Ağustos 2008'de Gürcistan Parlamentosu ile Cumhurbaşkanlığı kanallarına ikinci saldırı dalgası düzenlenmiş, 11

---

[724] Lionel Beehner, Liam Collins, Steve Ferenzi, Robert Person & Aaron Brantly, *Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia*, Modern War Institute, United States Military Academy, Report, 2018, ss. 19-20.
[725] Richard Stiennon, *a.g.m.*, s. 18.
[726] Jose Nazario, "Politically Motivated Denial of Service Attacks", Editörler: Christian Czosseck & Kenneth Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare*, IOS Pres, Washington, D.C. 2009, s. 6.

Ağustos 2008 tarihinde ise devlete ait çevrimiçi kanalların büyük çoğunluğu hizmet dışı bırakılmıştır. Bunlarla beraber sıcak savaşı objektif ya da Gürcistan lehine ele alan çeşitli uluslararası haber sayfalarıyla Rusya'daki muhalif siyasetçilerin çevrimiçi sayfalarına da çeşitli DDoS saldırıları düzenlenmiştir.[727]

Öte yandan Gürcistan siber saldırılarının daha yenilikçi ve organize bir yapısı bulunmaktadır. En yüksek siber saldırı aktiviteleri, Rus tanklarının Güney Osetya'ya girdikleri 8-9-10 Ağustos 2008 tarihlerinde gerçekleşmiştir. Saldırılar esnasında Rusça çevrimiçi sayfalar, bloglar ve forumlar üzerinden hedef Gürcü sitelerinin listesi ve saldırı talimatlarını içeren komut dosyaları yayınlanmıştır. Bununla beraber saldırıları başlatmak için yürütülebilir yazılımlar içeren indirilebilir dosyalar servis edilmiştir. Ayrıca sıcak savaşın başlamasının hemen ardından faaliyete alınan çeşitli Rus bilgisayar korsanlığı çevrimiçi forumları –Xaker.ru ve Stopgeorgia.ru– dünyadaki acemi bilgisayar korsanlarına uzman tavsiye ve yönlendirmeleri sağlayarak Rusya lehine saldırıya katılma imkanı sunmuştur. Böylelikle Gürcistan İnternet ağlarının yaklaşık %35'i kullanılamaz hale getirilmiş, %60 civarı ise saldırılar sırasında verimsizleştirilmiştir.[728]

Gürcistan saldırılarının bir diğer önemli özelliği ise ilk defa bir ulus-devlein uluslararası bir siyasi ve askeri çatışmayla eşgüdümlü olarak siber saldırılara maruz kalmış olmasıdır. Gürcistan ise bu saldırılara tepki verme konusunda yetersiz kalmıştır. Bunun nedeni; SSCB'nin dağılmasında sonra dünya jeopolitiği ve küresel ekonomik sistem içerisinde yer arayışında olan bu eski Sovyet cumhuriyetinin ülke olarak İnternet erişiminin oldukça düşük ve Bilgi ve İletişim teknolojilerinde ise oldukça geri kalması gösterilmektedir. Bunlara ek olarak mevcut siber sistemlerini güvence altına almak, siber saldırılara karşı stratejiler oluşturmak ve siber saldırıların önlenebilmesi için gerekli olan politikalar, kurumlar, bilgi, beceri ve kaynak yoksunluğu da hesaba katıldığında mecburen uluslararası yardım talebi söz konusu olmuştur.[729] Bu bağlamda AB, Gürcistan ile Rusya arasındaki 2008 savaşında çatışma çözüm müzakerelerinde resmi bir taraf olmamakla birlikte o dönemin AB

[727] Andria Gotsiridze, "The Cyber Dimension of the 2008 Russia-Georgia War", Georgian Foundation For Strategic And International Studies, 9 Ağustos 2019, *https://www.gfsis.org/blog/view/970*, (Erişim Tarihi: 6 Mayıs 2020).
[728] Alison Lawlor Russell, *a.g.e.*, ss. 104-105.
[729] Ellada Gamreklidze, "Cyber Security In Developing Countries, A Digital Divide Issue: The Case of Georgia", *Journal of International Communication*, Cilt 20, Sayı 2, 2014, s. 202.

Başkanı olan Fransa Cumhurbaşkanı Nicholas Sarkozy, 12 Ağustos 2008 yılındaki ateşkesin sağlanmasında arabulucuk yapmıştır; ancak Gürcistan'daki siber saldırılara yönelik uluslararası yardım ve tepkilere bakıldığında Estonya ve Polonya dışında pek kayda değer bir gelişme yaşanmamıştır. Estonya Bilgisayar Acil Müdahale Ekibi'nden (*Estonian Computer Emergency Response Team*) siber savunmaya yardım etmek ve 2007 yılındaki Rusya saldırılarından edinilen bilgi ve tecrübeyi paylaşmak adına iki siber güvenlik danışmanı 13 Ağustos 2008 tarihinde Gürcistan'a gönderilmiş, Polonya ise kendi Başkanlık çevrimiçi sayfasını Cumhurbaşkanı Mikheil Saakashvili'nin gelişmekte olan durumlar ilgili toplumu ve uluslararası camiayı bilgilendirebilmesi amacıyla güncellemeler yayınlayabileceği şekilde kullanımına açmıştır.[730]

Gürcistan'a yönelik gerçekleştirilen bu siber saldırıların devlet ve toplum açısından üç temel hedefi olduğu görülmektedir. Buna göre ilk olarak, Gürcistan açısından yabancı bir aktörle yaşanan ulusal ve uluslararası bir kriz ortamında bilgi ve iletişime getirilen erişim sınırlamasıyla Gürcistan izole edilmiş ve dolayısıyla uluslararası siyasi destek ve tavsiyeler açısından da sınırlandırılmıştır. İkinci olarak, yaşanan bu blokajdan dolayı finansal işlemler yapma yeteneği olumsuz yönde etkilenmiş ve elektronik finansal işlemlerin on günden fazla durmasına neden olarak ciddi anlamda ekonomik zarar oluşturmuştur. Son olarak ise yaşanan yoğun siber saldırılarla oluşturulan kısıtlama hali, Gürcistan Hükümetini ve toplumunu psikolojik olarak etkileyerek Rusya'nın isteklerine uyulması yönünde baskı yaratmıştır. Bir diğer boyut ise, sadece birkaç hafta süren bu siber saldırılar neticesinde Gürcistan'ın siber uzay sahasındaki varlığının yabancı aktörlerce kontrol edilebilir hale gelmesi, gelecek açısından örtülü bir tehdit olarak yorumlanmasına vesile olmuştur.[731]

Netice olarak siber uzay sahasının fiziksel altyapılarının kontrolünün hem stratejik hem de taktik açılardan son derece kritik önem taşıdığı 2008 Gürcistan saldırılarından tecrübe edilmiştir. Erişim ve engel yollarıyla kamuoyunun şekillendirilebildiği, çatışmaya taraf olanların siber alanın fiziksel altyapısına olan göreceli bağımlılıkları ya da erişebilme yetenekleri tarafından kapasitelerinin ve

[730] Richard Stiennon, *a.g.m.*, s. 20.
[731] Alison Lawlor Russell, *a.g.e.*, s. 122.

zayıf noktalarının belirlenebildiği görülmüştür.[732] Gürcistan saldırılarında, Gürcü ağlarına kalıcı hasara neden olabilecek saldırılardan kaçınıldığı ve Endüstriyel Kontrol Sistemleri (*Industrial Control Systems*, ICS) ile Denetleyici Kontrol ve Veri Toplama (*Supervisory Control and Data Acquisition*, SCADA) sistemlerinin hedef alınmadığı gerçeği göz önünde bulundurulduğunda söz konusu siber fiziksel altyapıların güvenliğinin ne derece önemli olduğu daha iyi anlaşılmaktadır. Bu tarz sistemler, enerji santrallerinden petrol/gaz boru hatlarına, rafinerilerden su şebekelerine kadar çeşitli kritik altyapıların gerçek zamanlı verilerinin toplanarak kontrol ve izlemelerinin yapıldığı tasarımlardır ve söz konusu sistemlerde yaşanabilecek saldırılar, ülkenin kalıcı olarak çok büyük hasarlar almasına neden olabilmektedir.[733] Dolayısıyla Gürcistan saldırılarından çıkarılabilecek en önemli ders, her ülkenin siber savaş ve siber saldırı türevleriyle doğrudan karşılaşabileceği riskine karşı kendini hazırlama sorunluluğudur. Yukarıda da belirtildiği üzere ICS ve SCADA sistemlerinin hedef alınmaması ve Gürcü ağlarına kalıcı hasar verilmemesi, Rusların gerçek siber yeteneklerinin bir tür test edilmesi şeklinde okunmalıdır. Bu saldırılarda çeşitli siber enstrümanların gücü sınanmış ve siber saldırganlığa karşı uluslararası tepki ölçülmüştür. Gelecekte yaşanabilecek kinetik saldırılarda ve hibrit savaş modellerinde siber bileşenlerin sıkı koordinasyonla etki boyutlarının muazzam seviyelere ulaşabileceği öngörülmüştür.[734] Dolayısıyla ulusal güvenlik anlayışlarının siber-fiziksel sistemlere olan bağlılığının giderek derinleşmesi ve dijital uçurumun/boşluğun (*digital divide*) dezavantajlı tarafında yer alan devletlerin, siber güvenliğin sağlanabilmesi ve sürdürülebilmesi açısından yaşayabileceği zorlukların gözlenebilmesi açısından Gürcistan saldırıları son derece önemli bir Siber Uluslararası İlişkiler örnek olayı olarak dikkate alınmalıdır.

---

[732] Ronald J. Deibert, Rafal Rohozinski & Masashi Crete-Nishihata, "Cyclones In Cyberspace: Information Shaping and Denial In the 2008 Russia–Georgia War", *Security Dialogue*, Cilt 43, Sayı 1, 2012, s. 17.

[733] Paulo Shakarian, Jana Shakarian & Andrew Ruef, *Introduction To Cyber-Warfare: A Multidisciplinary Approach*, Syngress Elsevier, Massachusetts 2013, s. 27.

[734] Marian Lazăr, "The Russian Cyber Campain Against Georgia (2008)", *The International Scientific Conference Strategies XXI: The Complex and Dynamic Nature of the Security Environment*, "Carol I" National Defence University Publishinghouse, Bükreş, 22-23 Kasım 2012, s. 504.

4.4. Stuxnet Saldırısı (2010)

Stuxnet saldırısının arka planına bakıldığında İran'ın son elli yıllık süreç içerisindeki nükleer hırsları ve girişimleri öne çıkmaktadır. 1960'larda ABD Başkanı Richard Nixon'ın desteğiyle İran'ın nükleer program çalışmaları başlamış ancak 1979 yılında Muhammed Rıza Şah Pehlevi'nin devrilmesiyle birlikte Orta Doğu'da büyük güçlerin değişen çıkar dengelerine bağlı olarak nükleer program planları henüz ciddi olarak başlamadan yarıda kesilmiştir.[735] İslam Devrimi sonrası ABD'nin İran'a yönelik değişen tutumu ve dünyadaki potansiyel nükleer tedirikçilere İran'a barışçıl nükleer teknoloji bile sağlanmaması yönündeki baskılara rağmen Pakistan nükleer programının babası olarak da bilinen Abdul Qadeer Khan öncülüğünde Pakistan ile İran devletleri arasında nükleer işbirliği pazarlıkları yapılmış ve nükleer silah tasarımlarıyla çeşitli donanımlar Dubai üzerinden İran'a transfer edilmiştir. Dolayısıyla İslam Devrimi sonrası 1980 ortalarında İran'da nükleer program çok iyi donanımlandırılmamakla birlikte AR-GE programı çerçevesinde gizlice ilerlemiş ve nükleer silah programı hedefinin temelleri atılmıştır.[736] Uranyum zenginleştirme teknolojisinin geliştirilmesi, İran'a nükleer silah potansiyeli sağlayacağından ABD'li ve Avrupalı yetkililer tarafından İran'ın asıl hedefinin nükleer silah sahibi olmak şeklinde uluslararası kamuoyu oluşturulmasına rağmen İranlı yetkililer tarafından ise tamamen sivil bir nükleer program amaçlandığı ve tıbbi araştırma reaktörlerine yakıt sağlanmasının yanı sıra yurtdışı pazarına satılan petrol arzından bağımsız olarak elektrik üretiminin hedeflendiği belirtilmiştir.[737] 2006 yılına gelindiğinde Tahran'ın yaklaşık 200 km güneyindeki Natanz şehrinde 300'den fazla çalışan gaz santrifüjüne sahip ilk pilot uranyum zenginleştirme tesisi kurulmuş ve 2007 yılının Eylül ayında ise söz konusu tesis, ticari ölçekli yakıt zenginleştirme tesisine dönüştürülmüş ve

---

[735] John Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield", *Journal of Computer & Information Law*, Cilt 29, Sayı 1, Güz 2011, s. 3.

[736] Alex Gibney (Yapımcı & Yönetmen), *Zero Days*, [Belgesel], Magnolia Pictures, ABD 2016.

[737] Ivanka Barzashka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme", *The RUSI Journal*, Cilt 158, Sayı 2, 2013, s. 48.; Mohammad Sahimi, Pirouz Mojtahed-Zadeh & Kaveh L. Afrasiabi, "Energy: Iran Needs Nuclear Power", The New York Times, 14 Ekim 2003, *https://www.nytimes.com/2003/10/14/opinion/IHT-energy-iran-needs-nuclear-power.html*, (Erişim Tarihi: 8 Mayıs 2020).; Voice of America (VOA), "Iran's New Nuclear Power Plant to be Closely Monitored", 31 Ekim 2010, *https://www.voanews.com/world-news/middle-east-dont-use/irans-new-nuclear-power-plant-be-closely-monitored*, (Erişim Tarihi: 8 Mayıs 2020).; BBC News, "Iran's Key Nuclear Sites", 14 Temmuz 2015, *https://www.bbc.com/news/world-middle-east-11927720*, (Erişim Tarihi: 8 Mayıs 2020).

uranyum zenginleştirmeye yarayan üç bine yakın santrifüjün başarıyla tesis edildiği duyurulmuştur. Ayrıca bu süreç zarfında nükleer enerji ya da nükleer silahlar için gerekli olan zenginleştirilmiş uranyumun hammaddesi olan uranyum hekzaflorürden (*uranium hexafluoride*) de uzun yıllar yetecek stok yapıldığı tespit edilmiştir.[738] Bunun üzerine çeşitli ülkelerden ve uluslararası kurumlardan İran'ın uranyum zenginleştirme programının Nükleer Silahların Yayılmasını Önleme Antlaşması'ndaki (*Nuclear Non-Proliferation Treaty*, NPT) nükleer enerji teknolojisinin meşru barışçıl amaçlar doğrultusunda kullanılması prensibinin ötesine geçtiği ve İran'ın acilen uranyum zenginleştirme programını durdurması gerektiğine dair çeşitli siyasi açıklamalar yapılmıştır.[739] Bunlara ek olarak ise 2006-2010 yılları arasında BM Güvenlik Konseyi'nde (*United Nations Security Council*, UNSC) İran'ın uranyum zenginleştirmeyle ilgili her türlü faaliyeti askıya almasının yanı sıra Uluslararası Atom Enerjisi Kurumu'nun (*International Atomic Energy Agency*, IAEA) ağır su reaktörü yapımının yeniden gözden geçirilmesi ve IAEA Ek Protokolünün onaylanması ve çeşitli güven artırıcı önlemler alınması gibi talepleri içeren, uyulmadığı takdirde de nükleer malzeme temini, seyahat yasağı, silah ambargosu ve finansal kısıtlamalar gibi çeşitli yaptırımları içeren altı karar –Karar 1969 (2006); Karar 1737 (2006); Karar 1747 (2007); Karar 1803 (2008); Karar 1835 (2008); Karar 1929 (2010)– alınmıştır.[740] Tüm bu uyarılara, taleplere, yaptırımlara ve baskılara rağmen İranlı yetkililer tarafından programın amacının sadece barışçıl amaçlarla zenginleştirilmiş uranyum üretilmesi olduğu savunulmuş ve programın devam edeceği ifade edilmiştir. Dahası 2010 yılında İran Atom Enerjisi Kurumu Başkanı Ali Akbar Salehi tarafından İran'ın Buşehr şehrinde yeni bir nükleer tesisin

---

[738] David Albright & Jacqueline Shire, "A Witches' Brew? Evaluating Iran's Uranium-Enrichment Progress", Arms Control Association (ACA), *https://www.armscontrol.org/act/2007-11/iran-nuclear-briefs/witches%E2%80%99-brew-evaluating-iran%E2%80%99s-uranium-enrichment-progress*, (Erişim Tarihi: 8 Mayıs 2020).

[739] Sascha Knoepfel, "Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War", Editörler: Jan-Frederik Kremer & Benedikt Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer-Verlag, Berlin Heidelberg 2014, s. 246.

[740] Kelsey Davenport, "UN Security Council Resolutions on Iran", Arms Control Association (ACA), Ağustos 2017, *https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran#res1696*, (Erişim Tarihi: 8 Mayıs 2020).; Anthony H. Cordesman & Adam C. Seitz, *Iranian Weapons of Mass Destruction, Iran's Nuclear Weapons Programs: Work In Progress?*, Center For Strategic & International Studies (CSIS), Working Draft for Review and Comments, Burke Chair in Strategy, 6 Kasım 2008, ss. 4-17.; BBC News, "UN Sanctions Against Iran", 26 Temmuz 2010, *https://www.bbc.com/news/world-middle-east-10768146*, (Erişim Tarihi: 8 Mayıs 2020).

yapımının tamamlanma aşamasına geldiği ve 2011 yılında açılacağı duyurulmuştur.[741]

Bir taraftan arka planda bu tarz gerginlikler ve karmaşık gelişmeler yaşanırken, diğer taraftan da enerji, ulaşım, bankacılık ve finans, iletişim, kimyasal tesisler ve çeşitli üretim alanları gibi kritik altyapılara yazılım tabanlı saldırı olasılıkları her geçen gün artmıştır. 2010 yılına dek uzmanlarca tartışılan söz konusu altyapılara dayanan ICS'lere yazılımsal saldırı olasılıkları, Stuxnet saldırısıyla ilk defa pratiğe dönüşmüştür. Stuxnet, kötü amaçlı yazılımların (*malwares*) modern devletler tarafından kullanılan ICS'ler hedef alınarak üzerinde stratejik olarak önemli, fiziksel olarak ise yıkıcı etkilere sahip olabileceğine dair geliştirilen teorilere ilk ispat niteliğindedir.[742] Stuxnet solucanı, 2010 yılının Haziran ayında Belarus'un Minsk şehrindeki "VirusBlokAda"[743] isimli bir anti-virüs şirketinde analist olan Sergey Ulasen tarafından keşfedilmiştir.[744] Bir ay sonrasında da Alman sanayi devlerinden *Siemens*, *Microsoft Windows* üzerinde çalışan *WinCC* adlı bir *Siemens* yazılımının bu solucan tarafından hedeflendiğini ve vanaları, boru hatlarını ve endüstriyel ekipmanları kontrol eden *Siemens* SCADA yönetim sistemlerinin söz konusu solucanlara karşı savunmasız kaldığı konusunda müşterilerini uyarmıştır.[745] Yine 2010 yılında İran tarafından başlangıçta reddedilse de nihayetinde kabul edilen bir siber silahın Natanz şehrindeki uranyum zenginleştirme tesisindeki gaz santrifüjlerine zarar verdiği açıklanmıştır.[746] Stuxnet yazılımı, belirli bir endüstriyel kontrolü hedefleyerek Natanz'daki yaklaşık 5000 civarı gaz santrifüjünün neredeyse 1000 tanesini doğrudan etkileyerek kontrolden çıkmasına neden olmuştur.[747]

---

[741] Sputnik News, "Iran installs Reactor Cap at Bushehr NPP", 23 Kasım 2010, *https://sputniknews.com/world/20101123161458962/*, (Erişim Tarihi: 8 Mayıs 2020).

[742] Eric P. Oliver, "STUXNET: A Case Study in Cyber Warfare", Editörler: Panayotis A. Yannakogeorgos & Adam B. Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, Taylor & Francis, Florida 2014, s. 128.

[743] Detaylı bilgi için bkz.: VirusBlokAda, *http://anti-virus.by/en/index.shtml*, (Erişim Tarihi: 9 Mayıs 2020).

[744] Paul J. Springer, *a.g.e.*, s. 279.

[745] Solange Ghernaouti, *a.g.e.*, s.151.

[746] BBC News, "Stuxnet 'Hit' Iran Nuclear Plans", 22 Kasım 2010, *https://www.bbc.com/news/technology-11809827*, (Erişim Tarihi: 9 Mayıs 2020).; Parisa Hafezi, "Iran Admits Cyber Attack On Nuclear Plants", Reuters, 29 Kasım 2010, *https://www.reuters.com/article/us-iran/iran-admits-cyber-attack-on-nuclear-plants-idUSTRE6AS4MU20101129*, (Erişim Tarihi: 9 Mayıs 2020).

[747] Emilio Iasiello, *a.g.m.*, s. 8.

Teknik olarak bakıldığında 500 kilobaytlık bir bilgisayar solucanı olan Stuxnet'in, bir flash sürücü veya evrensel seri veriyolu (*Universal Serial Bus,* USB) üzerinden bilgisayara yüklenip, sonrasında bir yerel alan ağı (*Local Area Network,* LAN) içerisinde yer alan bilgisayar sisteminden bir diğerine geçecek şekilde tasarlandığı görülmektedir. Natanz'daki İnternet bağlantısı olmayan nükleer tesise sızması da bu şekilde gerçekleşmiştir.[748] Öte yandan Stuxnet, kötü amaçlı yazılımlarda daha önce hiç görülmemiş bir düzeyde teknik karmaşıklık ve entegrasyon sergilemiştir. Örneğin; saldırı amaçlı kodların içerisinde her zaman hatalar (*bugs*) olmasına rağmen ortalama bir siber saldırı kodundan yirmi kat daha büyük olan Stuxnet'in içerisinde neredeyse hiç hata barındırmadığı tespit edilmiştir. Oldukça ender görülen bu durum, "*zero-day*"[749] adı verilen sıfır gün güvenlik açığı saldırı programlarından dört tane tespit edilmesiyle daha da karmaşıklaşmıştır. Programın içerik oluşturucusunun farkında olmadığı ve daha önce algılanamamış olan bir güvenlik açığı "sıfır gün" (*zero-day*) olarak adlandırılmaktadır. Sıfır gün saldırı programları ise içeriğini saldırgan dışında kimsenin bilmediği ve karşısında koruyucu bir yama bulunmayan, bir kodun saldırgan bir şey yapmaksızın yayılmasını sağlayan ender görülen tiplerdir ve siber-güvenlik şirketleri her yıl keşfettiği ortalama on iki milyondan fazla kötü amaçlı yazılımdan sadece bir düzine civarı sıfır gün güvenlik açığından yararlanmaktadır.[750] Ayrıca Stuxnet solucanının bilgisayar koruma yazılımlarını ve uygun güvenlik duvarı hizmetlerini yanlış yönlendirmek için tasarlanmış bir dizi anti-virüs kaçırma tekniği sayesinde 2009-2010 yılları arasında Natanz nükleer tesisi sisteminde tespit edilemediği belirtilmiştir.[751] Özellikle ana bilgisayara bulaşan virüsün kendini gizleyebilmesi için ana bilgisayarı meşru bir yazılım parçası olduğuna inandırması gerekmektedir. Bu bağlamda da bir bilgisayardan diğerine geçen yazılımlar için pasaporta benzeyen dijital imzalar kullanılmaktadır. Geçmişteki saldırılarda kötü amaçlı yazılım geliştiricileri

---

[748] Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt & Joseph Weiss, *a.g.e.*, s. 210.

[749] Kasperky, "Sıfır Gün Güvenlik Açığı Saldırısı Nedir?", *https://www.kaspersky.com.tr/resource-center/definitions/zero-day-exploit*, (Erişim Tarihi: 9 Mayıs 2020).

[750] Alex Gibney (Yapımcı & Yönetmen), *Zero Days*, [Belgesel], Magnolia Pictures, ABD 2016.

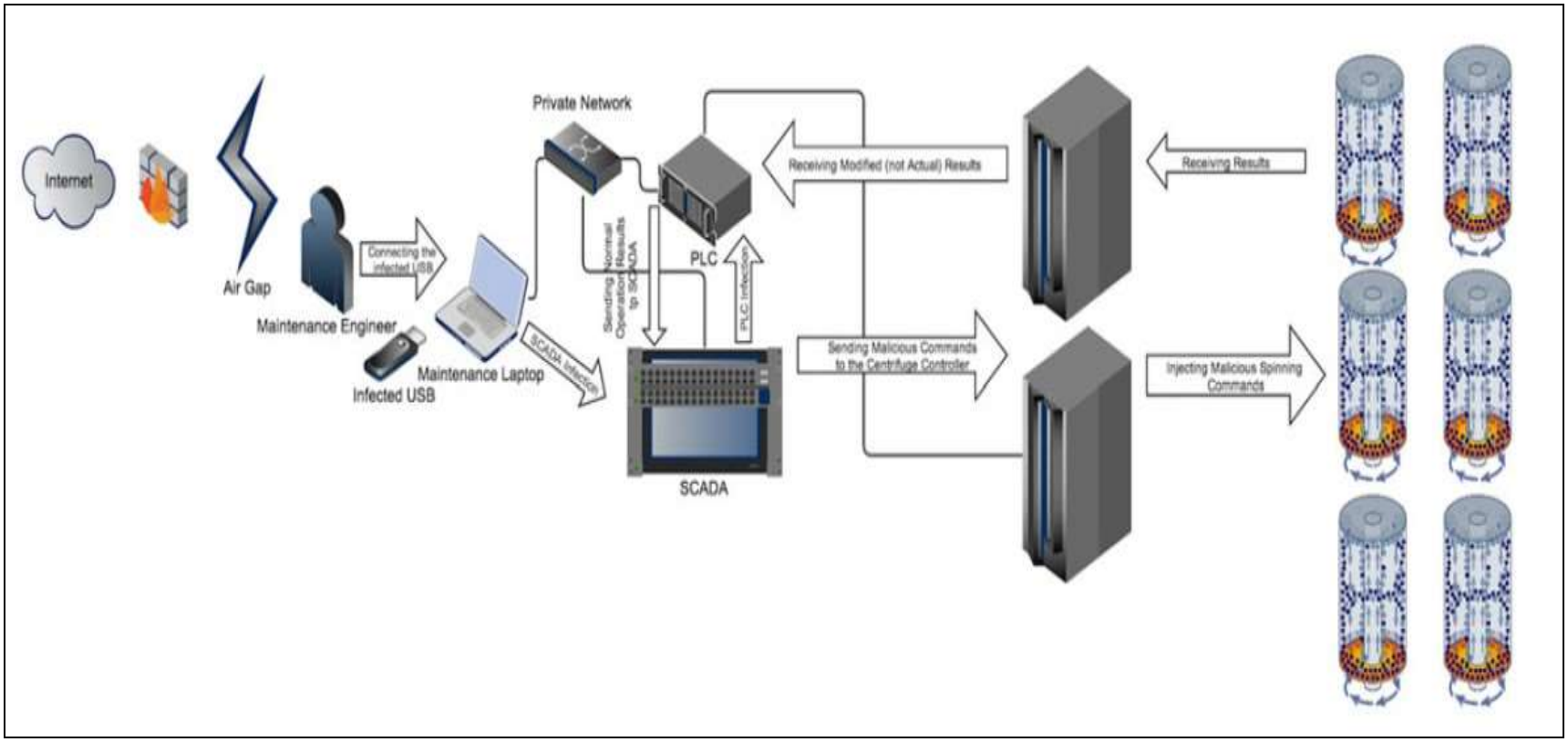
[751] Chris Masciotra, "International Law and Cyber Warfare: The Case of Stuxnet", Editör: Jocelyn McGrandle, *Political Science Graduate Student Journal: Challenges, Disconnects, and Clashes in Political Studies, Volume III*, Concordia University, Department of Political Science, Montréal, Québec 2014, ss. 103-104.

tarafından hedef bilgisayarları kandırabilmek için sahte dijital imzalar kullanılırken, Stuxnet olayında siber dünyanın en güvenilir firmalarından olan Realtek'ten çalınan iki gerçek dijital imzanın kullanıldığı tespit edilmiştir.[752] Tablo 37'de sunulan Stuxnet saldırı diyagramı, saldırının enfekte edilmesi, aktive edilmesi ve başlatılması süreçlerinin daha iyi anlaşılabilmesi ve saldırının nasıl dikkatlice tasarlandığının idrak edilebilmesi adına önem arz etmektedir. Buna göre dış dünya ile siber bağlantısı olmayan (*air-gapped*) hedef uranyum zenginleştirme tesisinin altyapısına harici bir cihaz üzerinden bulaşan solucan, ana cihaza enfekte olmasının ardından etkinleştirilmiş ve sonrasında tüm ağ aygıtlarına –yazıcılar, bilgisayarlar, veritabanı sunucuları ve uygulama sunucuları– bulaşmıştır. İlk bulaşma sonrasında gaz santrifüjlerine karşı herhangi bir kötü amaçlı faaliyet başlatılmadan öncesinde ise tam çalışma döngüsü için normal işlemlerin gizlice kaydedilmesi, çalınan dijital imzaların uygun şekilde kullanılmasıyla meşru bir varlık görünümünün korunması, diğer bilgisayarlara bulaşılması, virüslü bilgisayarların listelenmesi, yayılmanın izlenmesi ve saldırıya uğramış bilgisayarlarda başarının belirlenmesi gibi temel görevler gerçekleştirilmiştir. Sonrasında ise tesisin altyapısında yaygın olarak kullanılan Siemens S7/WinCC ürünleri hedef alınmış ve S7 ürünündeki uranyum zenginleştirme altyapısındaki santrifüjlerin kontrolünden sorumlu PLC'ler, saldırının başlatılması için hedef unsur haline getirilmiştir. Ayrıca yine aynı diyagramda görüleceği üzere SCADA yönetim sisteminden sensör okuyucularına kadar büyük sistem bileşenleri tam anlamıyla enfekte edilmiştir.[753] Böylelikle santrifüjlerin dakikada yaklaşık 63.000 devirlik (1000 hertz) güvenli işlem hızı bozularak dakikada 80.000 devire (1400 hertz) çıkması sağlanmış, ardından da hızla yavaşlatılarak 2 hertze düşürülmüştür. Neticede ana bilgisayar ekranında gaz basıncı ve hızın normal olduğu görünmeye devam etmesine rağmen santrifüjlerin patlaması sağlanmıştır.[754] Dolayısıyla Stuxnet saldırısı, bir siber fiziksel sistemi doğrudan hedef alan en karmaşık tasarıma sahip kötü amaçlı yazılımlardan biri olarak kayda geçmiştir.

---

[752] Lawrence J. Trautman & Peter C. Ormerod, "Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things", *University of Miami Law Review*, Cilt 72, Sayı 3, 2018, s. 790.
[753] Arash Nourian & Stuart Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet", *IEEE Transactions on Dependable and Secure Computing*, Cilt 15, Sayı 1, Ocak/Şubat 2018, ss. 5-6.
[754] Alex Gibney (Yapımcı & Yönetmen), *Zero Days*, [Belgesel], Magnolia Pictures, ABD 2016.

Tablo-37: Stuxnet Saldırı Diyagramı



Kaynak: Arash Nourian & Stuart Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet", *IEEE Transactions on Dependable and Secure Computing*, Cilt 15, Sayı 1, Ocak/Şubat 2018, s. 6.

Kamuoyundaki çeşitli spekülasyonlar ile basın-yayın kurumları tarafından servis edilen raporlara göre Stuxnet saldırısının, ABD ile İsrail istihbarat servisleri arasında "Olimpiyat Oyunları" (*Olympic Games*) olarak adlandırılan ortak bir operasyonun parçası olduğu ortaya çıkmıştır.[755] Saldırgan bir siber yeteneğin, uzak bir sistemi uluslararası sınırlarda fiziksel hasara neden olabilecek şekilde hedefleyebileceğini ve tehlikeye atabileceğini göstermesi açısından Stuxnet, siber savaş tartışmalarında bir dönüm noktası olarak tanımlanmaktadır.[756] Diğer taraftan ise Stuxnet'in çeşitli varyasyonlarının keşfedilmesi, söz konusu saldırının kısa-orta-uzun dönem etki ve sonuçlarının tespit edilenlerin çok daha ötesinde olabileceği olasılığını da akıllara getirmektedir. 2011 yılının Ekim ayında güvenlik uzmanlarınca keşfedilen ve Stuxnet ile aynı kod grubunun çoğunluğuna sahip olan "Duqu" virüsünün, Stuxnet'i oluşturan ekip tarafından yazıldığı ya da Stuxnet'in tersine mühendislik uygulamasının başarılı bir versiyonu olduğu düşünülmektedir; ancak Stuxnet'ten farklı olarak Duqu'nun amacının; gelecekteki olası saldırılar için endüstriyel kontrol sistemi üreticileri gibi çeşitli kuruluşlardan istihbarat verileri ve varlıkları toplamak olduğu tespit edilmiştir.[757] Benzer şekilde 2012 yılının Mayıs ayında ise Stuxnet ve Duqu'nun bir başka versiyonu olan "Flame" virüsü araştırmacılar tarafından keşfedilmiştir. Flame, tasarım olarak Stuxnet ile Duqu'ya çok benzemekle birlikte daha spesifik hedefli saldırılarda bir dizi modüler bileşene sahip karmaşık bir virüs olarak tanımlanmıştır.[758] Yine çeşitli medya kanallarında servis edilen raporlara göre ise Stuxnet, Duqu ve Flame kötü amaçlı yazılımlarının, ABD Ulusal Güvenlik Dairesi (NSA) tarafından Olimpiyat Oyunları operasyonları için geliştirildiği iddia edilmektedir.[759]

---

[755] Kay Hearn, Patricia A. H. Williams & Rachel J. Mahncke, "International Relations and Cyber Attacks: Official and Unofficial Discourse", *11th Australian Information Warfare and Security Conference,* Edith Cowan University, Perth Western Australia, 30 Kasım-2 Aralık 2010, s. 10.
[756] Damien Van Puyvelde & Aaron F. Brantly, *a.g.e.*, s. 153.
[757] Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, ABC-CLIO, California 2013, s. 11.
[758] Lawrence J. Trautman & Peter C. Ormerod, *a.g.m.*, ss. 800-801.
[759] Ellen Nakashima, Greg Miller & Julie Tate, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say", The Washington Post, 19 Haziran 2012, *https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html*, (Erişim Tarihi: 10 Mayıs 2020).

Netice olarak Stuxnet saldırılarının Siber Uluslararası İlişkilere yansımalarına bakıldığında birtakım gerçeklerin ortaya çıktığı görülmektedir: Buna göre söz konusu saldırılar, İran'ın nükleer planlarını değiştirmesine neden olmamıştır. Siber silahların siber fiziksel sistemlere doğrudan zarar verdiği bu saldırılar, İran Hükümetinin zenginleştirilmiş uranyum üretimini durdurmadığı gibi ABD ve AB ile herhangi bir anlaşma yapmaya da teşvik etmemiştir. Potansiyel bir politika aracı olarak saldırılar ele alındığında ise iki beklenmedik sonuç yaşanmıştır: Birincisi, saldırılar her ne kadar İran'ın nükleer planlamalarının gecikmesine neden olsa da, zarar gören santrifüjler hızla yenileriyle değiştirilerek İran'ın nükleer kalkınmaya olan bağlılığı daha da artmıştır. İkinci olarak ise ABD ve İsrail tarafından resmi sorumluluk kabulü gelmediğinden İran'ın siber uzay alanını karşı atak olarak militarize etmesi söz konusu olmamasına rağmen İranlıları siber güvenlik yapılarını iyileştirmeye zorlamış ve ABD'nin SCADA sistemlerini İranlılar tarafından misilleme saldırılarına hedef haline getirmiştir.[760] ABD tarafından bakıldığında ise İran nükleer programının Stuxnet saldırısı nedeniyle minimum iki yıl geriye çekildiği ve esas hedefin de tam ölçekli kinetik bir savaş yaşanmaksızın İran'ın nükleer kapasite hedeflerinin sekteye uğratılması olduğu ve dolayısıyla da saldırının amacına ulaştığı görüşleri ağır basmaktadır. Siyasi ve stratejik bağlamlardaki etkileri dikkate alındığında, siber suç ile devlet eylemlerinin yakınlaştığı ve dolayısıyla devletlerin siber suçların yol açtığı teknoloji gelişiminden faydalanabildiği görülmüştür. Dahası, devletlerin bu teknolojiyi kullanma yeteneğinin zayıf olması durumunda üçüncü tarafların dâhil edilerek söz konusu siber saldırıların yürütülebilmesi imkânı da doğmuştur.[761] Maliyet açısından yaklaşıldığında ise ABD, İsrail ve diğer bölge ülkeleri açısından İran'ın nükleer kapasitesinin sınırlandırılması ve nükleer programının geciktirilmesi için olası geleneksel bir askeri saldırının maliyeti, Stuxnet'in maliyetinden çok daha fazla olmakla birlikte mevcut sorunu çözmek yerine çok daha büyük sorunlar yaratması söz konusu olabilirdi.[762]

---

[760] Emilio Iasiello, *a.g.m.*, ss. 10-11.

[761] Sean Collins & Stephen McCombie, "Stuxnet: The Emergence of A New Cyber Weapon and Its Implications", *Journal of Policing, Intelligence and Counter Terrorism*, Cilt 7, Sayı 1, Nisan 2012, s. 88.

[762] Chris Demchak, "Evolutions In Asymmetric Cyberpower", *World Politics Review*, Cyberwar: Real and Imagined, Feature Report, 19 Nisan 2011, s. 6.

Son olarak, uluslararası hukuk açısından değerlendirme yapılırsa, onarılabilir hasara neden olan ancak insanları yaralamayan siber saldırıların kuvvet kullanımı veya silahlı saldırı olarak sınıflandırılmadığı, Stuxnet saldırısının uluslararası ilkeleri ihlal etse bile mevcut uluslararası hukukun siber savaşları düzenleme konusundaki yetersizliği ve ulusal güvenlik yasalarıyla ilgili uluslararası paradigmada bir değişime ihtiyaç olduğu görülmüştür. Siber saldırıların dağınık ve anonim doğasının ise devletlerin kendilerini savunmadaki kuvvet kullanma yeteneklerini sınırladığını ve caydırıcılığı zayıflattığını göstermiştir.[763] Ayrıca Stuxnet saldırısı, yeni teknolojilerle birlikte savaşın doğasının ve şeklinin değiştiğini göstermiştir. Bu nedenle yaşanan gelişme ve dönüşüme uygun ve eşit yanıtların uluslararası hukuk alanında geliştirilmesinin gerekliliği, gelecekteki Stuxnet benzeri saldırıların önlenebilmesi adına üzerinde fikir birliği elde edilmesi oldukça zor olsa da yeni hükümetler arası anlaşmaların geliştirilmesinin mecburiyetini bir kez daha ortaya koymuştur.[764]

4.5. WikiLeaks (2010)

Siber olayların doğasındaki karmaşıklığın ve etki boyutu büyüklüğünün görüldüğü en etkileyici gelişmelerden biri olarak "*WikiLeaks*" isimli oluşumun başta ABD diplomatik belgeleri olmak üzere dünya çapında çeşitli ülkelere ait "çok gizli" olarak tasniflendirilmiş çeşitli belgeleri kamuoyuna sızdırma eylemleri gösterilmektedir. Danielle M. Logue ile Stewart R. Clegg'in *WikiLeaks*'i konu alan disiplinlerarası çeşitli bilimsel makalelerdeki kullanım çerçevesi ve söylem incelemelerine göre *WikiLeaks* çok çeşitli şekillerde tanımlanabilmektedir: Toplumsal bir hareket; Siyasi bir proje; Bir sivil toplum kuruluşu; Sanal işbirliği platformu; Devlet dışı ve kurumsal olmayan bir kuruluş; Gazetecilerin ya da bilgisayar korsanlarının etiketlerini çürüten ve şeffaflığı temsil eden bir organizasyon; Bilgi girişimciliğinin bir örneği; Bir tür güç yapısı; Bir çeşit yönetişim tarzı; Siber alanda faaliyet gösteren uluslararası bir kuruluş; Sanal bir proje; İçerik

[763] Jordan Peagler, "The Stuxnet Attack: A New Form of Warfare and The (In)Applicability of Current International Law", *Arizona Journal of International & Comparative Law*, Cilt 31, Sayı 2, 2014, s. 433.
[764] Chris Masciotra, *a.g.m.*, s. 119.

sağlayıcı; Veri sızıntı kanalı.[765] Şüphesiz bu kadar fazla etiket çeşitliliğinin bulunması, *WikiLeaks*'in sınıflandırılmasını belirsiz kılmakla birlikte oluşumun yetkili çevrimiçi kanalında "2006 yılında Julian Assange tarafından kurulan, savaş, casusluk ve yolsuzluk içeren sansürlenmiş veya çeşitli kısıtlamalara tabi tutulan resmi materyallerin ve büyük veri kümelerinin analizi ve yayınlanmasında uzman çok uluslu bir medya organizasyonu" olarak tanımlanmaktadır.[766] *WikiLeaks*'in 2006-2010 yılları arasındaki dönemine bakıldığında bir evrilme süreci yaşandığı görülmektedir. Bu süreçte *WikiLeaks* aktif bir anonim aktör olarak kalırken, materyal seçimi ve düzenlemeleriyle birlikte muhbirlerin belgelerini yayınlamalarına ya da ifşa etmelerine olanak tanıyan aracı pozisyonundan evrilmiştir. Bu dönemin temel amacını ise bilgilerin anonim olarak gönderilebilmesi için hızlı ve güvenli bir mekanizma oluşturulması ve söz konusu bilgilerin küresel anlamda kitlelere erişilebilir kılınabilmesi adına İnternetin hızından, etkileşiminden ve küresel erişiminden yararlanılması oluşturmuştur. Bu bağlamda *WikiLeaks*'in kuruluşunun ilk yıllarında karışık medya etkileri yaratan bir dizi dosya elektronik ortamda yayınlanmıştır. 2007 yılının Kasım ayında Küba Adası'ndaki ABD kontrollü gözaltı merkezindeki günlük operasyonların ayrıntılı şekilde ana hatlarıyla belirtildiği "Camp Delta Standart İşletim Prosedürleri" (*Camp Delta Standard Operating Procedures*) adlı Guantanamo Körfezi askeri el kitabını sızdırarak küresel anlamda ilk defa dikkatleri üzerine çekmiştir.[767] Sonrasında ise *Scientology* Kilisesi'ne ait gizli metinler, eski Kenya Devlet Başkanı Daniel Arap Moi'nin ailesinin yolsuzluklarını belgleyen raporlar, İngiliz şirketi *Trafigura*'nın yasadışı olarak Fildişi Sahili'ne zehirli atık bıraktığının kanıtları, İzlanda'daki ekonomik çöküşe yol açan bankaların mali anlaşmaları, Cumhuriyetçi Parti'nin 2008 yılındaki ABD Başkanlık

---

[765] Danielle M. Logue & Stewart R. Clegg, "Wikileaks and The News of the World: The Political Circuitry of Labeling", *Journal of Management Inquiry*, Cilt 24, Sayı 4, 2015, s. 397.

[766] WikiLeaks, "What is WikiLeaks", 3 Kasım 2015, *https://wikileaks.org/What-is-WikiLeaks.html*, (Erişim Tarihi: 20 Mayıs 2020).

[767] Bart Cammaerts, "Networked Resistance: The Case of WikiLeaks", *Journal of Computer-Mediated Communication*, Cilt 18, Sayı 4, Temmuz 2013, s. 420.; WikiLeaks, "Camp Delta Standard Operating Procedure", 7 Kasım 2007, *https://wikileaks.org/wiki/Camp_Delta_Standard_Operating_Procedure*, (Erişim Tarihi: 20 Mayıs 2020).; Andy Greenberg, "WikiLeaks Announces 'The Detainee Policies': A History Of U.S. Post-9/11 Military Prisoners In Leaked Documents", Forbes, 25 Ekim 2012, *https://www.forbes.com/sites/andygreenberg/2012/10/25/wikileaks-announces-the-detainee-policies-a-history-of-american-military-detainees-in-leaked-documents/#3778d3841455*, (Erişim Tarihi: 20 Mayıs 2020).

Seçimleri'ndeki Başkan Yardımcısı adayı Sarah Palin'in kişisel e-postaları, aşırı sağcı İngiliz Ulusal Partisi'nin (*British National Party*, BNP) üyelik listeleri, İsviçre bankası *Julius Baer Group*'un vergi kaçırdığı ve kara para akladığına dair belgeler, çeşitli ülkelerin İnternet filtre listeleri ve daha çok sayıda kamuoyundan saklanan bilgiler servis edilmiştir.[768]

2006-2009 arasındaki bu dönem, *WikiLeaks*'in ana akım medya unsurlarıyla çok az etkileşim ve işbirliği içerisinde olduğu, servis ettiği bilgilerin medyada nispeten daha az yer kapladığı ve alternatif bir bilgi kaynağı olarak kabul edildiği süreçtir. 2010 ve 2011 yılları itibariyle ise hem uluslararası kamuoyunda hem medyada hem de akademik dünyadaki etkisinde büyük değişiklik yaşanmaya başlamıştır. Öyle ki, Christian Christensen'in tespitine göre; *Google Scholar* üzerinde "*WikiLeaks*" kelimesi aratıldığında 2009 yılında 614, 2010 yılında 1450 ve 2011 yılında ise 5720 sonuç çıkmıştır.[769] Bunun nedeni olarak ise kamuoyuna

---

[768] Benedetta Brevini, Arne Hintz & Patrick McCurdy, "Introduction", Editörler: Benedetta Brevini, Arne Hintz & Patrick McCurdy, *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, 1. Basım, Palgrave Macmillan, Hampshire 2013, s. 2.; WikiLeaks, "Church of Scientology's 'Operating Thetan' documents leaked online", 26 Mart 2008, *https://wikileaks.org/wiki/Church_of_Scientology%27s_%27Operating_Thetan%27_documents_leaked_online*, (Erişim Tarihi: 20 Mayıs 2020).; WikiLEaks, "The looting of Kenya under President Moi", 30 Ağustos 2007, *https://wikileaks.org/wiki/The_looting_of_Kenya_under_President_Moi*, (Erişim Tarihi: 20 Mayıs 2020).; WikiLeaks, "Côte d'Ivoire: Toxic Waste Scandal Unfolds", 8 Eylül 2006, *https://wikileaks.org/plusd/cables/06ABIDJAN1004_a.html*, (Erişim Tarihi: 20 Mayıs 2020).; WikiLeaks, "Financial collapse: Confidential exposure analysis of 205 companies each owing above EUR45M to Icelandic bank Kaupthing, 26 Sep 2008", 30 Temmuz 2009, *https://wikileaks.org/wiki/Financial_collapse:_Confidential_exposure_analysis_of_205_companies_each_owing_above_EUR45M_to_Icelandic_bank_Kaupthing,_26_Sep_2008*, (Erişim Tarihi: 20 Mayıs 2020).; WikiLeaks, "VP contender Sarah Palin hacked", 17 Eylül 2008, *https://wikileaks.org/wiki/VP_contender_Sarah_Palin_hacked*, (Erişim Tarihi: 20 Mayıs 2020).; WikiLeaks, "British National Party membership list and other information, 15 Apr 2009", 20Ekim 2009,*https://wikileaks.org/wiki/British_National_Party_membership_list_and_other_information,_15_Apr_2009*, (Erişim Tarihi: 20 Mayıs 2020).; WikiLeaks, "Bank Julius Baer USA tax evasion trusts", 16 Nisan 2008, *https://www.wikileaks.org/wiki/Bank_Julius_Baer_USA_tax_evasion_trusts*, (Erişim Tarihi: 20 Mayıs 2020).; Elena Schor, "Wikileaks posts a hack of Palin's e-mail account", The Guradian, 18 Eylül 2008, *https://www.theguardian.com/world/deadlineusa/2008/sep/17/uselections2008.sarahpalin*, (Erişim Tarihi: 20 Mayıs 2020).; James Kirkup & Christopher Hope, "BNP membership list leaked onto internet", The Telegraph, 18 Kasım 2008, *https://www.telegraph.co.uk/news/politics/3479612/BNP-membership-list-leaked-onto-internet.html*, (Erişim Tarihi: 20 Mayıs 2020).; BBC News, "Swiss banker linked to Wikileaks is found guilty", 19 Ocak 2011, *https://www.bbc.com/news/business-12231036*, (Erişim Tarihi: 20 Mayıs 2020).; Xan Rice, "The Looting of Kenya", The Guardian, 31 Ağustos 2007, *https://www.theguardian.com/world/2007/aug/31/kenya.topstories3*, (Erişim Tarihi: 20 Mayıs 2020).

[769] Christian Christensen, "A Decade of WikiLeaks: So What?", *International Journal of Media & Cultural Politics*, Cilt 10, Sayı 3, 2015, s. 275.

sızdırılan gizli bilgi ve belge miktarındaki artış kadar bilgi ve belgelerin konu olduğu dört temel olay gösterilmektedir:

(1) 2007 yılında Bağdat'ta gerçekleştirilen hava saldırısında iki *Reuters* çalışanı ile birlikte 10 sivilin Amerikan ordusuna ait bir *Apache* helikopteri tarafından vurulduğunu gösteren gizli bir videonun "Teminat Cinayeti" (*Collateral Murder*) başlıklı düzenlenmiş hali, 5 Nisan 2010 tarihinde *WikiLeaks* tarafından kamuoyuna sunulmuştur.[770]

(2) 25 Temmuz 2010 tarihinde 2004-2010 yılları arasındaki Afganistan'daki savaşı kapsayan 91.000'den fazla gizli belge ve rapor, "Afganistan Savaş Günlüğü" (*The Afghan War Diary*) başlığıyla kamuoyuna servis edilmiştir. Ana akım medyadan üç kurumla –*The New York Times, The Guardian, Der Spiegel*– oluşturulan bir konsorsiyumla işbirliği içerisinde sunulan bu belgelerde ABD ordusunun ölümcül askeri eylemlerinin içeriği, öldürülen, yaralanan ve alıkonulan kişilerin bilgileri, olayların gerçekleştiği yerlerin kesin coğrafi bilgileri, ilgili askeri birimler ile kullanılan büyük silah sistemleri detaylı olarak yer almıştır.[771]

(3) 22 Ekim 2010 tarihinde *WikiLeaks* ile ana akım medya konsorsiyumunun işbirliği doğrultusunda "Irak Savaş Günlükleri" (*The Iraq War Logs*) olarak adlandırılan tarihin en büyük askeri gizli bilgi sızıntısı yayınlanmıştır. 1 Ocak 2004 ile 31 Aralık 2009 arası dönemde Irak'taki savaş ve Amerikan işgalini belgeleyen toplamda 391.832 rapor ve belge servis edilmiştir. Söz konusu belge ve raporlarda, Irak'ta toplamda 109.302 kişinin hayatını kaybettiği, bunların 66.081'inin

---

[770] WikiLeaks, "Collateral Murder", 5 Nisan 2020, *https://collateralmurder.wikileaks.org/*, (Erişim Tarihi: 21 Mayıs 2020).; Bart Cammaerts, *a.g.m.*, ss. 420-421.; BBC News, "WikiLeaks posts video of 'US military killings' in Iraq", 6 Nisan 2010, *http://news.bbc.co.uk/2/hi/americas/8603938.stm*, (Erişim Tarihi: 21 Mayıs 2020).; Josh Stieber & Ethan Mccord, "US Soldiers from Wikileaks 'Collateral Murder' Video Apologize", Global Policy Forum, 19 Nisan 2010, *https://www.globalpolicy.org/invasion-and-war/atrocities-and-criminal-homicides-/48984-us-soldiers-from-wikileaks-collateral-murder-video-apologize.html*, (Erişim Tarihi: 21 Mayıs 2020).

[771] WikiLeaks, "The Afghan War Diary", 25 Temmuz 2010, *https://wikileaks.org/afg/*, (Erişim Tarihi: 21 Mayıs 2020).; Nick Davies & David Leigh, "Afghanistan war logs: Massive leak of secret files exposes truth of occupation", The Guardian, 25 Temmuz 2010, *https://www.theguardian.com/world/2010/jul/25/afghanistan-war-logs-military-leaks*, (Erişim Tarihi: 21 Mayıs 2020).; The New York Times, "View Is Bleaker Than Official Portrayal of War in Afghanistan", 25 Temmuz 2010, *https://www.nytimes.com/2010/07/26/world/asia/26warlogs.html*, (Erişim Tarihi: 21 Mayıs 2020).; Der Spiegel, "Explosive Leaks Provide Image of War from Those Fighting It", 25 Temmuz 2010, *https://www.spiegel.de/international/world/afghanistan-explosive-leaks-provide-image-of-war-a-708314.html*, (Erişim Tarihi: 21 Mayıs 2020).; Bart Cammaerts, *a.g.m.*, s. 421.

"sivillerden" oluştuğu, 23.984'ünün "isyancılar" olarak tanımlandığı, 15.196'sının "Irak hükümet güçlerinden" ve 3.771 kişinin ise "koalisyon güçlerinden" olduğu belgelenmiştir.[772]

(4) 28 Kasım 2010 tarihinde *WikiLeaks* tarafından 2003-2010 yılları arasındaki çoğu ABD elçiliklerinin gizli diplomatik yazışmalarını içeren 251.287 belge "*Cablegate*" adıyla sızdırılmıştır. Söz konusu belgelerin içeriğinde hükümetler arasında ve hükümetlerle şirketler arasındaki anlaşmaların arka planları, ABD'nin BM yetkililerine yönelik casusluk uygulamaları, Orta Doğu ve Kuzey Afrika'daki ABD Hükümetine ait yolsuzluklar, finans endüstrisinin gizli ilişkileri, üzeri kapatılan askeri saldırılar gibi çeşitli konulara dair detaylı bilgiler yer almıştır.[773]

Yukarıda sunulan dört gelişme neticesinde 2010 yılı sonuna gelindiğinde Julian Assange ve *WikiLeaks*, küresel anlamda geniş bir medya odağının merkezi haline gelmiştir. Sızıntıların ölçeği, hızı ve önemi dikkate alındığında, dünyanın yeni bir "radikal şeffaflık" çağına girdiği ve Uluslararası İlişkilerde Soğuk Savaş dönemindeki gibi eski tarz gizliliğin artık sona erdiğine dair çeşitli yorumları beraberinde getirmiştir.[774] Uluslararası anlamda siyasi depremler yaratan 2010 yılındaki *WikiLeaks* sızıntılarının muhbiri olarak tespit edilen Bradley Manning,

---

[772] WikiLeaks, "The Iraq War Logs", 22 Ekim 2010, *https://wikileaks.org/irq/*, (Erişim Tarihi: 21 Mayıs 2020).; Bart Cammaerts, *a.g.m.*, s. 421.; Der Spiegel, "Greatest Data Leak in US Military History", 22 Ekim 2010, *https://www.spiegel.de/international/world/the-wikileaks-iraq-war-logs-greatest-data-leak-in-us-military-history-a-724845.html*, (Erişim Tarihi: 21 Mayıs 2020).; Nick Davies, Jonathan Steele & David Leigh, "Iraq war logs: secret files show how US ignored torture", The Guardian, 22 Ekim 2010, *https://www.theguardian.com/world/2010/oct/22/iraq-war-logs-military-leaks*, (Erişim Tarihi: 21 Mayıs 2020).; The New York Times, "The Iraq Archive: The Strands of a War", 22 Ekim 2010, *https://www.nytimes.com/2010/10/23/world/middleeast/23intro.html*, (Erişim Tarihi: 21 Mayıs 2020).; BBC News, "Wikileaks: Iraq war logs 'reveal truth about conflict'", 23 Ekim 2010, *https://www.bbc.com/news/world-middle-east-11612731*, (Erişim Tarihi: 21 Mayıs 2020).

[773] WikiLeaks, "Cablegate: 250,000 US Embassy Diplomatic Cables", 28 Kasım 2010, *https://www.wikileaks.org/Cablegate-250-000-US-Embassy.html*, (Erişim Tarihi: 21 Mayıs 2020).; Bart Cammaerts, *a.g.m.*, s. 421.; The Guardian, "WikiLeaks embassy cables: the key points at a glance", 7 Kasım 2010, *https://www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points*, (Erişim Tarihi: 21 Mayıs 2020).; Scott Shane & Andrew W. Lehren, "Leaked Cables Offer Raw Look at U.S. Diplomacy", 28 Kasım 2010, *https://www.nytimes.com/2010/11/29/world/29cables.html*, (Erişim Tarihi: 21 Mayıs 2020).; BBC News, "Wikileaks US diplomatic cables: Key issues", 3 Aralık 2010, *https://www.bbc.com/news/world-us-canada-11858990*, (Erişim Tarihi: 21 Mayıs 2020).; Der Spiegel, "How America Views the World", 29 Kasım 2010, *https://www.spiegel.de/international/world/state-department-secrets-revealed-how-america-views-the-world-a-732819.html*, (Erişim Tarihi: 21 Mayıs 2020).

[774] Alasdair Roberts, "WikiLeaks: The Illusion of Transparency", *International Review of Administrative Sciences*, Cilt 78, Sayı 1, 2012, s. 117.

Irak'taki ABD ordusunda istihbarat analisti olarak görev yaparken yakalanarak tutuklanmış ve bir yıl boyunca hiç yargılama yapılmaksızın oldukça kötü koşullarda ve işkence yapılarak tutulmuştur.[775] Ardından başlayan yargı süreci neticesinde 2013 yılının Temmuz ayında ABD Casusluk Yasası'nı ihlal ettiği gerekçesiyle ise bu konuda Amerikan tarihinin en uzun süreli hapis cezasına –35 yıl– çarptırılmıştır.[776] Cezasının ardından cinsiyet değişikliği talebinde bulunmuş, adını Chelsea Manning olarak değiştirmiş ve 2017 yılında da dönemin ABD Başkanı Barack Obama tarafından affedilerek serbest bırakılmıştır.[777] Diğer taraftan Julian Assange ise *Cablegate* sızıntıları sonrasında İsveçli yetkililer tarafından 2006 yılında İsveç'te iki kadına cinsel saldırıda bulunduğu suçlamasıyla çıkarılan uluslararası yakalama kararı doğrultusunda İngiliz polisi tarafından tutuklanmıştır. Suçlamaları reddeden ve siyasi olarak motive edildiğini belirten Assange, 2010 yılı sonunda kefaletle hapishaneden çıkarak ev hapsine alınmıştır. 2011 yılında İsveç'e iade kararı onanan Assange, 2012 yılında temyiz mahkemesine yapmış olduğu başvuru da reddedilince Londra'daki Ekvator Büyükelçiliği'ne sığınmış ve kendisine 16 Ağustos 2012 tarihinde resmen siyasi sığınma hakkı tanınmıştır.[778] Yedi yıl boyunca Londra'daki Ekvator Büyükelçiliği'nde kalan Assange'ın sığınma hakkı, Ekvator'da yaşanan hükümet değişikliğinin ardından 11 Nisan 2019'da kaldırılmış ve İngiliz polisi tarafından tutuklanmıştır. Ardından ABD tarafından resmen iadesi istenmiş ve aynı zamanda

---

[775] Arne Hintz, "Challenges to Freedom of Expression in the Digital World: Lessons from WikiLeaks and the Arab Spring", *ESSACHESS - Journal for Communication Studies*, Cilt 5, Sayı 1(9), 2012, s. 94.

[776] Cherie Blair & Ema Vidak Gojkovic, "WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence", *ICSID Review,* Cilt 33, Sayı 1, 2018, s. 236.

[777] Harriet Alexander, "Who is Chelsea Manning and why is she being released from prison?", 17 Mayıs 2017, *https://www.telegraph.co.uk/news/2017/05/17/chelsea-manning-released-prison/*, (Erişim Tarihi: 22 Mayıs 2020).; BBC News, "Chelsea Manning: Wikileaks source celebrates 'first steps of freedom'", 17 Mayıs 2017, *https://www.bbc.com/news/world-us-canada-39947602*, (Erişim Tarihi: 22 Mayıs 2020).

[778] Iveta Imre, Ivanka Pjesivac & Catherine A. Luther, "Governmental Control of the Internet and WikiLeaks: How does the Press in Four Countries Discuss Freedom of Expression?", *the International Communication Gazette*, Cilt 78, Sayı 5, 2016, ss. 386-387.; BBC News, "Julian Assange: A timeline of Wikileaks founder's case", 19 Kasım 2019, *https://www.bbc.com/news/world-europe-11949341*, (Erişim Tarihi: 22 Mayıs 2020).; Nesrine Malik, "Why is the left blinkered to claims about Assange and sexual assault?", The Guardian, 15 Nisan 2019, *https://www.theguardian.com/commentisfree/2019/apr/15/left-blinkered-claims-julian-assange-sexual-assault*, (Erişim Tarihi: 22 Mayıs 2020).; Anna North, "The rape allegation against Julian Assange, explained", 13 Mayıs 2019, *https://www.vox.com/identities/2019/4/12/18306901/julian-assange-arrest-wikileaks-rape-sweden-embassy*, (Erişim Tarihi: 22 Mayıs 2020).

İsveç Savcılığı tarafından cinsel saldırı soruşturması tekrardan başlatılmıştır. 2020 yılının bahar aylarında dünyada ortaya çıkan yeni tip corona virüs (COVID-19) pandemisi sebebiyle ABD'ye iade davası ertelenen Assange, halen İngiltere'deki Belmarsh Cezaevi'nde yatmaktadır.[779]

WikiLeaks sızıntılarının Uluslararası İlişkilere olan yansımalarına bakıldığında, 21. yüzyıldaki küresel ilişkilerin birbirine olan bağlılığının devletlerin içsel endişelerini aştığının görülmesine vesile olmuştur. Ülkeler arası ve ülkeler içi güç dengelerinin tek bir web sitesi üzerinden nasıl etkilenebileceği ve hatta tersine çevrilebileceğinin ispatı olarak da yorumlanmaktadır.[780] *WikiLeaks*, daha önce örneği görülmemiş ve insanlık tarafından bilinmeyen bir fenomeni, hükümetler ve insanlar tarafından toplu olarak fark etmeye zorlamış ve uluslararası toplum tarafından siber uzayın açtığı yeni enformasyon ve bilgi sınırlarının insanlıkça algılanmasına meydan okumasını öngöremediğini gözler önüne sermiştir. Dolayısıyla *WikiLeaks*, gerçekleşme süreci devam eden ancak henüz tamamlanmamış bir fenomen olarak okunabilmektedir. Dahası, içinde bulunulan bu siber çağda bilginin güç üzerindeki belirleyiciliği ve yoğunluğu giderek artmaktadır. Bilginin erişimi, dağıtımı ve paylaşımı, artık sadece güçlü ve etkili olanın münhasır koruması altında değildir ve uluslararası toplumun ortak zenginliği haline evrilmiştir. Yani, İnternet erişimi olan herkes, daha önceleri seçkin elitlerin alanında kabul edilen bilgi ve belgelere ulaşabilir ve hatta katkı sağlayabilir pozisyona gelmiştir.[781] Bilginin yeni sınırlarındaki çelişkiler, İran, Suriye gibi siyasi açıdan göreceli "doğru" olarak

---

[779] Jacob Jarvis, "Julian Assange's Extradition Hearing Delayed to at Least September, WikiLeaks Announces", Newsweek, 5 Nisan 2020, *https://www.newsweek.com/julian-assange-extradition-delayed-september-wikileaks-1501780*, (Erişim Tarihi: 22 Mayıs 2020).; Jedidajah Otte, "Release Julian Assange, says woman who had two children with him while in embassy", The Guardian, 12 Nisan 2020, *https://www.theguardian.com/media/2020/apr/12/release-julian-assange-says-woman-who-had-two-children-with-him-while-in-embassy*, (Erişim Tarihi: 22 Mayıs 2020).; Reuters, "Coronavirus forces delay in U.S. extradition case against Assange", 27 Nisan 2020, *https://www.reuters.com/article/us-britain-assange/coronavirus-forces-delay-in-us-extradition-case-against-assange-idUSKCN22913S*, (Erişim Tarihi: 22 Mayıs 2020).; Ellen Milligan, "Julian Assange's Extradition Trial Delayed by Coronavirus", Bloomberg, 27 Nisan 2020, *https://www.bloomberg.com/news/articles/2020-04-27/wikileak-s-assange-extradition-trial-delayed-by-coronavirus*, (Erişim Tarihi: 22 Mayıs 2020).

[780] Hannes Steen-Thornhammar, "VIEWPOINT: Combating Censorship Should be a Foreign Policy Goal", Editörler: Sean S. Costigan & Jake Perry, *Cyberspaces and Global Affairs, Ashgate Publishing*, Farnham 2012, s. 229.

[781] Karamatullah K. Ghori, "The Global Challenge of WikiLeaks", *Pakistan Horizon*, Cilt 64, Sayı 1, Ocak 2011, s. 5.

addedilen hedeflerin teşhir edilmesinin, hegemon aktör olarak ABD'nin teşhir edilmesinden çok daha farklı standartlara sahip olduğunu ortaya koymuştur. ABD'nin istihbarat toplamak ve BM diplomatlarının biyometrik bilgilerini ele geçirmek için dünya çapındaki İnternet, cep telefonu ve akıllı telefon ağlarını izlediği, veriler topladığı ve manipüle ettiğine dair ispatların *WikiLeaks* gibi devlet-dışı bir aktör ve yepyeni bir siber fenomen tarafından kamuoyuna servis edilmesi, ABD tarafından söz konusu bilgi sızıntılarının siber terörizm, siber hırsızlık, siber casusluk ve vandalizm olarak tanımlanmasına neden olmuştur.[782] Dahası, söz konusu saldırıların sadece Amerikan iç işlerine yönelik olmadığı, küresel güvenliği koruyan ve ekonomik refahı ilerleten uluslararası topluma, ittifaklara, ortaklıklara, görüşmelere ve müzakerelere yönelik olduğu vurgulanmış ve siber alanda bilgi kontrolü ve güvenliğine yönelik devlet aktörlerinin daha sert önlemler alması gerektiği belirtilmiştir.[783]

Diğer taraftan 21. yüzyılın bu karşılıklı hiper bağlantı ortamında ortaya çıkan *WikiLeaks*'in medya ve siyasetteki şeffaflık ve hesap verebilirliğe katkı sağlayıp sağlamadığına dair tartışmalar ortaya çıkmıştır. Buna göre vatandaşlar ile siyasi iktidar temsilcileri arasındaki giderek soyutlaşan ve zayıflayan iletişim halinin değiştirilebilmesi adına kamusal alanda büyük umutlar ve geniş kapsamlı beklentilerin oluşmasına katkı sağlandığı görülmektedir. Hatta kamuoyuna sızıdırılan bilgi ve belge içeriklerine bağlı olarak halkın siyasi, ekonomik ve toplumsal hesap verilebilirlikteki algılanan başarısızlıklara karşı koymasına teşvik edici etkiler yaratması söz konusu olabilmektedir. Bu bağlamda *WikiLeaks*, ağlara bağlı dijital çağın vaatleri ile bunların güç, siyaset ve hesap verilebilirlik üzerindeki dönüşümsel etkisini enkarne eden, gizlilik ve bilginin biriktirilmesini sona erdirip, açıklığı, şeffaflığı ve bilgi paylaşımını mecbur kılan, açık bir toplumun gelişebilmesi ve büyüyebilmesi için değişim ve dönüşüm sürecini başlatan bir fenomen olarak

---

[782] Jan Nederveen Pieterse, "Leaking Superpower: WikiLeaks and the Contradictions of Democracy", *Third World Quarterly*, Cilt 33, Sayı 10, 2012, s. 1912.

[783] Cherie Blair & Ema Vidak Gojkovic, *a.g.m.*, ss. 236-237.; Ewen MacAskill, "Hillary Clinton Attacks Release of US Embassy Cables", The Guardian, 29 Kasım 2010, *https://www.theguardian.com/world/2010/nov/29/clinton-reacts-us-embassy-cables*, (Erişim Tarihi: 23 Mayıs 2020).; BBC News, "Wikileaks Diplomatic Cables Release 'Attack on World'", 29 Kasım 2010, *https://www.bbc.com/news/world-us-canada-11868838*, (Erişim Tarihi: 23 Mayıs 2020).

yorumlanmaktadır.[784] Öte yandan ise *WikiLeaks*, siber uzay alanında devlet aktörlerinin baskı ve kontrollerini arttıracağı ve İnternet'in ifade özgürlüğünün geleceğini olumsuz olarak etkileyeceğini savunan görüşler de bulunmaktadır. 2010 yılındaki bu büyük sızıntılara dek İnternet özgürlüğünün en güçlü destekçisi olan ABD'nin, 2010 yılı sonrasında *WikiLeaks*'i kınaması, siteye erişimin engellenmesi ve saldırılar gerçekleştirilmesi, kurucusu ve çalışanlarına soruşturma başlatılması, *Visa, MasterCard, PayPal, Bank of America* ve *Western Union*'ın finansal blokaj uygulaması gibi gelişmeler, İnternet'in özgürlüğünün geleceği hakkındaki endişeleri destekler niteliktedir.[785] Diğer taraftan ise ulusal ve uluslararası düzeyde şeffaflık ve hesap verilebilirlik kadar güven duygusunun da hala çok önemli bir değer olmaya devam ettiği, gizliliğin ise güven için ön koşul oluşturduğunu düşünenler bulunmaktadır. Buna göre uluslararası politikadaki çıkarların korunabilmesi adına özellikle diplomatik yazışmaların kabul edilebilir bir düzeyde gizlilik gerektirdiği ancak devlet-dışı bir aktör olarak *WikiLeaks*'in bu ilkeyi ihlal ettiği belirtilmektedir.[786] *WikiLeaks* sızıntılarındaki ulusal güvenlik bilgilerinin açıklanabilmesi için kurumsal çerçevede değişimler yarattığı ve uluslararası düzeyde beklenen zararların gerçekleşmediği görüşü de savunulmaktadır.[787] Son olarak ülke içerisindeki müspet etkilerine bakıldığında ise 2016 yılındaki ABD Başkanlık Seçimleri öncesinde Demokratik Ulusal Komite'ye (*Democratic National Committee*) ve Hillary Clinton'ın seçim kampanyasını yöneten John Podesta'ya ait toplamda 70.000'den fazla e-posta yayınlanmıştır.[788] Sızdırılan yazışmalar ve belgelerin kamuoyunu etkileyerek Hillary Clinton'un seçimlerde Donald Trump'a

---

[784] James W. Davis & Miriam Meckel, "Political Power and the Requirements of Accountability in the Age of WikiLeaks", *ZPol Zeitschrift für Politikwissenschaft*, Cilt 22, Sayı 4, 2012, ss. 478-479.

[785] Iveta Imre, Ivanka Pjesivac & Catherine A. Luther, *a.g.m.*, s. 387.; Jane Wakefield, "Wikileaks' Struggle to Stay Online", BBC News, 7 Aralık 2010, *https://www.bbc.com/news/technology-11928899*, (Erişim Tarihi: 23 Mayıs 2020).; Andy Greenberg, "Visa, MasterCard Move To Choke WikiLeaks", Forbes, 7 Aralık 2010, *https://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/#7821c00f2cad*, (Erişim Tarihi: 23 Mayıs 2020).; Ewen MacAskill, "WikiLeaks website pulled by Amazon after US political pressure", The Guardian, 2 Aralık 2010, *https://www.theguardian.com/media/2010/dec/01/wikileaks-website-cables-servers-amazon*, (Erişim Tarihi: 23 Mayıs 2020).

[786] Ondřej Horký, "The Future of Diplomacy: European and Global Challenges", *Institute of International Relations*, Policy Paper, Prag, Şubat 2011, s. 4.

[787] Patricia L. Bellia, "WikiLeaks and the Institutional Framework for National Security Disclosures", *The Yale Law Journal*, Cilt 121, Sayı 6, Nisan 2012, ss. 1503-1504. ((((1448-1526))))

[788] Laura Poitras, Yoni Golijov & Brenda Coughlin (Yapımcılar), Laura Poitras (Yönetmen), *Risk*, [Belgesel], Neon, ABD 2016.

kaybetmesinde etkili olduğu görüşleri hâkim olmakla birlikte söz konusu yazışmalara ulaşılması hususunda Rus kaynakların destek verdiği görüşleri de bulunmaktadır.[789] Nihayetinde *WikiLeaks*, hem ulusal hem de uluslararası bağlamlarda büyük etkiler yaratmış, aktörlerin siber uzay sahasının muazzam boyutlarını daha net şekilde tecrübe etmelerini sağlamış ve Siber Uluslararası İlişkilerde güç dengeleri, gizlilik, şeffaflık, hesap verilebilirlik, güven, ulusal, uluslararası ve siber çıkarlar gibi temel değerlerin yeniden değişim ve dönüşüm sürecine girmesine vesile olmuştur.

4.6. Snowden (2013)

21. yüzyıl modern toplumunun özünde olan özelliklerden biri olarak kabul edilen gözetim/gözetleme/izleme (*surveillance*) hali, sadece veri toplamayı değil, toplanan verilerin sosyal kontrol uygulamasında kullanılmasını da sağlamakta ve suçluları, siyasi aktivistleri ve kötü amaçlı aktörleri izleyen gizli servisler ve polis kuvvetleri gibi devlet kurumlarından işçileri, müşterileri ve piyasadaki rakiplerini izleyen özel şirketlere kadar çeşitlilik arz edebilmektedir. 20. yüzyılda tüketici kültürü ve bilgi işleminde yaşanan artış, 21. yüzyılda daha fazla ağa bağlı, her yerde bulunabilen ve gerçek zamanlı organize edilmesini sağlayan bazı niteliksel gözetim değişikliklerinin ortaya çıkmasını sağlamıştır.[790] *WikiLeaks* sızıntıları sonrasında uluslararası ortamda oluşan sosyo-politik sarsıntı ve şaşkınlık hali, eski bir CIA ve

---

[789] Tom Spender, "Wikileaks: Is Julian Assange interfering in US election?", BBC News, 19 Ekim 2016, *https://www.bbc.com/news/uk-37704393*, (Erişim Tarihi: 23 Mayıs 2020).; Al Jazeera, "WikiLeaks, political hacks and the US election", 23 Ekim 2016, *https://www.aljazeera.com/programmes/listeningpost/2016/10/wikileaks-political-hacks-election-161023102730794.html*, (Erişim Tarihi: 23 Mayıs 2020).; David Smith, "WikiLeaks emails: what they revealed about the Clinton campaign's mechanics", The Guardian, 6 Kasım 2016, *https://www.theguardian.com/us-news/2016/nov/06/wikileaks-emails-hillary-clinton-campaign-john-podesta*, (Erişim Tarihi: 23 Mayıs 2020).; Zack Beauchamp, "WikiLeaks just tried to justify its behavior this year in a bizarre Election Day statement", 8 Kasım 2016, *https://www.vox.com/world/2016/11/8/13563750/wikileaks-2016-election-statement*, (Erişim Tarihi: 23 Mayıs 2020).; John Muth, "WikiLeaks and The 2016 Presidential Election", Towson University Journal of International Affairs, 8 Kasım 2016, *https://wp.towson.edu/iajournal/2016/11/08/wikileaks-and-the-2016-presidential-election/*, (Erişim Tarihi: 23 Mayıs 2020).; Mark Hosenball, "WikiLeaks faces U.S. probes into its 2016 election role and CIA leaks: sources", Reuters, 7 Aralık 2017, *https://www.reuters.com/article/us-usa-trump-russia-wikileaks/wikileaks-faces-u-s-probes-into-its-2016-election-role-and-cia-leaks-sources-idUSKBN1E12J2*, (Erişim Tarihi: 23 Mayıs 2020).

[790] Christian Fuchs & Daniel Trottier, "Internet Surveillance After Snowden: A Critical Empirical Study of Computer Experts' Attitudes on Commercial and State Surveillance of the Internet and Social Media Post-Edward Snowden", *Journal of Information, Communication and Ethics in Society*, Cilt 15, Sayı 4, 2017, ss. 412-413.

NSA çalışanı olan Edward Snowden tarafından gerçekleştirilen yeni sızıntılarla birlikte gölgede bırakılmış ve 21. yüzyılın tartışmalı kavramları olan "Büyük Veri" (*Big Data*) ve "gözetleme/gözetim/izleme"nin (*surveillance*) etki boyutlarının ve tekniklerinin ciddiyetini yeniden gözler önüne sermiş ve Büyük Verinin gözetleme ile destekleyici ilişkiler kurulmasının yollarını net olarak göstermiştir.[791] "Büyük Veri" (*Big Data*), çok büyük veri kümelerini, bunların araştırılması, analizi ve manipüle edilmesi için kullanılan araç ve prosedürlerle birlikte aynı zamanda da düşünce ve araştırmadaki sayısal dönüşümü ifade etmektedir. Tıpkı Ford'un araba yapma şeklini değiştirmesi sonrasında sektördeki işleyişin kendisini dönüştürmesi gibi, Büyük Veri de zaten bilgi nesnelerini değiştiren bir bilgi sistemi ortaya çıkarken, aynı zamanda da insan ağlarının ve toplumların nasıl anlaşıldığını bildirme gücüne sahip olmuştur.[792] "Gözetim" (*surveillance*) ise bilgiye erişmek veya Büyük Veri analizleri ve grafik-teorik uygulamalar aracılığıyla iletişim kuranların sosyal ağları hakkında bilgi edinme girişimlerini kapsamaktadır.[793] Çeşitli fikirleri, uygulamaları, metaforları, yazılımları ve teknikleri içeren Büyük Verinin, etkileme, yönetme ya da yetkilendirme gibi belirli bir amaç için kişisel detaylara yönelik sistematik ve yoğun bir odaklanma ve dikkat yaratması, Snowden'ın sızıntılarıyla birlikte 21. yüzyıldaki muazzam veri yığınlarının ve teknik izlemelerin sosyo-teknik karakterinin analizi açısından önemli fırsatlar sağlamıştır.[794]

Eski bir CIA ve NSA çalışanı olan Edward Joseph Snowden, 2013 yılında ABD Ulusal Güvenlik Dairesi'nin (NSA) küresel gözetim/izleme programlarının operasyonel yöntemlerini ortaya koyan yüksek dereceli gizli belgelerin kamuoyuna sızdırılmasını sağlamış ve yaşanan gelişmeler hem ABD'de hem de uluslararası arenada "Snowden Etkisi" (*Snowden Impact*) ya da "Snowden İhlali" (*Snowden*

---

[791] Petros Iosifidis & Mark Wheeler, Public Spheres and Mediated Social Networks in the Western Context and Beyond, *Palgrave Macmillan*, Londra 2016, s. 139.
[792] Danah Boyd & Kate Crawford, "Critical Questions For Big Data: Provocations For A Cultural, Technological, and Scholarly Phenomenon", *Information, Communication & Society*, Cilt 15, Sayı 5, 2012, s. 665.
[793] Florian Sprenger, *The Politics of Micro-Decisions: Edward Snowden, Net Neutrality, and the Architectures of the Internet*, Meson Press, Lüneburg 2015, s. 24.
[794] David Lyon, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique", *Big Data & Society*, Cilt 1, Sayı 2, Temmuz 2014, ss. 1-2.

Breach) şeklinde adlandırılmıştır.[795] 2013 yılının Mayıs ayında Hawaii'den Hong Kong'a geçen Snowden, 1 Haziran 2013 tarihinde İngiliz gazetesi *The Guardian*'ın muhabirleri Glenn Greenwald ile Ewen MacAskill ve belgesel yapımcısı Laura Poitras'la Hong Kong'taki The Mira Hotel'de bir haftalık röportajlara ve belgesel kaydına başlamıştır.[796] 6 Haziran 2013 tarihinde *The Guardian*, ABD Hükümeti'nin telekom devi *Verizon*'u, milyonlarca Amerikan vatandaşının telefon kayıtlarını teslim etmeye zorladığına dair gizli bir mahkeme emrini yayınlamıştır.[797] 7 ve 8 Haziran 2013 tarihlerinde ise NSA'e ait olan küresel teknik gizli izleme programı "PRISM" (*Planning Tool for Resource Integration, Synchronization, and Management* / *Personal Record Information System Methodology*) açıklanmış, başta *Microsoft, Yahoo, Google, Facebook, YouTube* ve *Apple* olmak üzere çeşitli İnternet devleri tarafından tutulan verilere doğrudan erişim sağlanabilmesi için sistemlerine arka kapı erişimi kurulduğu ifşa edilmiştir.[798] Tablo 38'de sunulan tabloda hangi İnternet şirketinin hangi tarihlerde PRISM programına dâhil olduğu net olarak görülmekle beraber yıllık maliyetinin 20 Milyon Doların üzerinde olduğu belirtilmiş ve bu program sayesinde şifreleme ve gizlilik protokolleri söz konusu şirketlerin yardımıyla atlatılmıştır. NSA tarafından Utah'ta inşa edilen ve ilk "İstihbarat Topluluğu Kapsamlı Ulusal Siber Güvenlik Girişimi" (*Intelligence Community Comprehensive National Cyber-security Initiative*, IC-CNCI) olarak tanımlanan devasa boyutlardaki "*Bumblehive*" kod isimli veri merkezi olan "Utah Veri Merkezi" (*The Utah Data Center*), PRISM tarzı gerçek zamanlı İnternet gözetimi ve veri madenciliği (*data mining*) olarak da adlandırılan küresel ağın dijital verilerinin

---

[795] Hasan T. Arslan & Joyren Quarcoo, "Political, Economical and Social Impacts of Snowden Breach", *Pakistan Journal of Criminology*, Cilt 7, Sayı 2, Nisan 2015, s. 29.

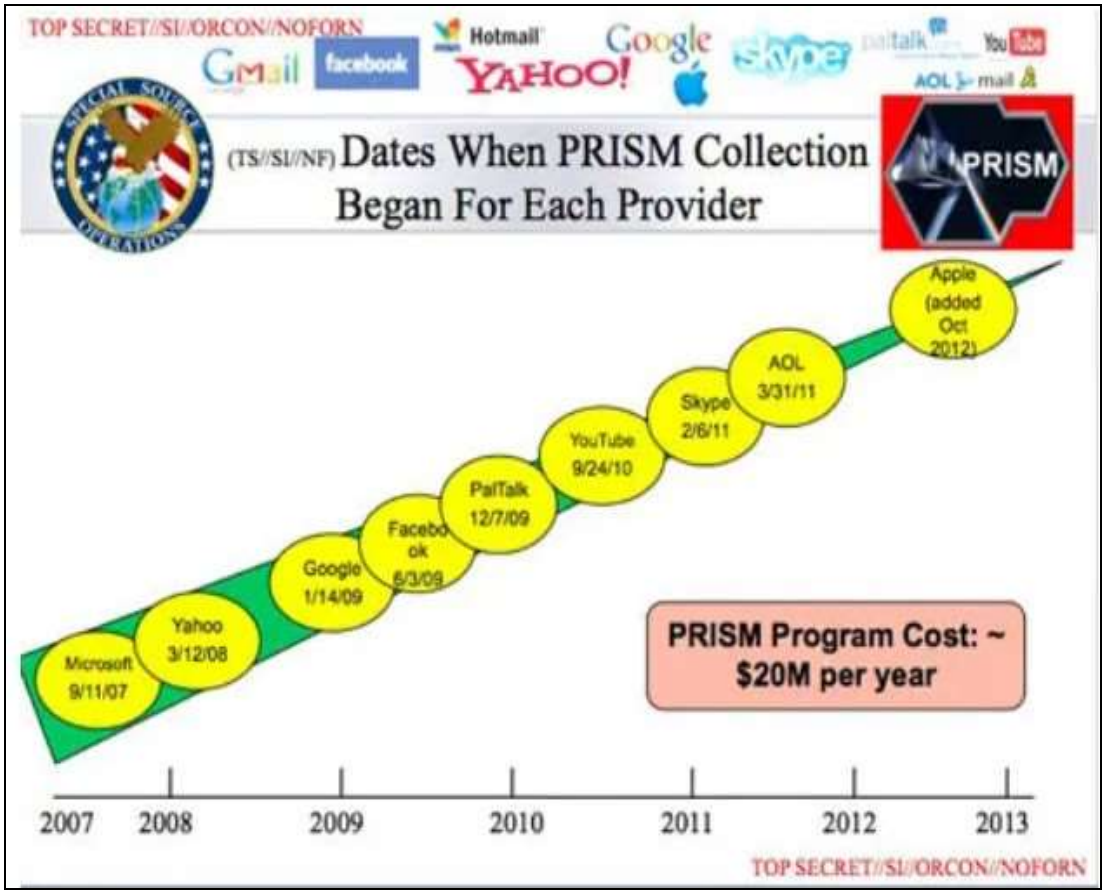
[796] Laura Poitras, Mathide Bonnefoy & Dirk Wilutzky (Yapımcılar), Laura Poitras (Yönetmen), *Citizenfour* [Belgesel], Radius-TWC, ABD 2014.

[797] Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily", The Guardian, 6 Haziran, *https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order*, (Erişim Tarihi: 25 Mayıs 2020).; Mahkeme kararına ulaşmak için bkz.: The Guardian, "The NSA Files: Verizon Forced to Hand Over Telephone Data – Full Court Ruling", 6 Haziran 2013, *https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order*, (Erişim Tarihi: 25 Mayıs 2020).

[798] Glenn Greenwald & Ewen MacAskill, "NSA Prism Program Taps In To User Data of Apple, Google and Others", The Guardian, 7 Haziran 2013, *https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data*, (Erişim Tarihi: 25 Mayıs 2020).; James Ball, "NSA's Prism Surveillance Program: How It Works and What It Can Do", The Guardian, 8 Haziran 2013, *https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google*, (Erişim Tarihi: 25 Mayıs 2020).

izlendiği, toplandığı, analiz ve kontrol edildiği uygulamaların genişletilmesini ve ilerletilmesini sağlamıştır.[799]

Tablo 38: PRISM Programına Veri Sağlayan İnternet Şirketleri



***Kaynak*:** Edward Snowden tarafından sızdırılan belgelerdeki "PRISM/US-984XN Overview or *The SIGAD Used Most in NSA Reporting Overview*" başlıklı sunum içerisinden alınmıştır. Detaylı bilgi için bkz.: Glenn Greenwald & Ewen MacAskill, "NSA Prism Program Taps In To User Data of Apple, Google and Others", The Guardian, 7 Haziran 2013, *https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data*, (Erişim Tarihi: 25 Mayıs 2020).

[799] NSA, Domestic Surveillance Directorate, "Utah Data Center", *https://nsa.gov1.info/utah-data-center/index.html*, (Erişim Tarihi: 25 Mayıs 2020).; David Lyon, a.g.m., s. 8.; Lydia Warren, "Inside America's $1.9 Billion Data Mine: How All Your Pivate Details Will Soon Be Stored In This Vast NSA Nerve Center In Utah Valley", Daily Mail, 7 Haziran 2013, *https://www.dailymail.co.uk/news/article-2337420/Utah-Data-Center-The-million-square-foot-Utah-data-mining-facility-built-NSA.html*, (Erişim Tarihi: 25 Mayıs 2020).; Rory Carroll, "Welcome to Utah, the NSA's Desert Home For Eavesdropping On America", The Guardian, 14 Haziran 2013, *https://www.theguardian.com/world/2013/jun/14/nsa-utah-data-facility*, (Erişim Tarihi: 25 Mayıs 2020).; John Brandon, "Inside the NSA's Secret Utah Data Center", Fox News, 11 Haziran 2013, *https://www.foxnews.com/tech/inside-the-nsas-secret-utah-data-center*, (Erişim Tarihi: 25 Mayıs 2020).

Bununla birlikte yine NSA'ye ait olan *Xkeyscore*, *Upstream*, *Quantuminsert*, *Bullrun* ve *Dishfire* gibi diğer Amerikan gözetim/izleme programlarıyla birlikte Birleşik Krallık Hükümet İletişim Merkezi'ne (*UK Government Communications Headquarters*, UK-GCHQ)[800] ait olan ve Snowden tarafından dünyanın ilk tam kapsamlı şebeke takip programı olarak tanımlanan "TEMPORA"ya ait bilgiler de servis edilmiştir.[801] TEMPORA programı, dünyanın su altı fiber optik kablolarından gelen iletişim verilerinin toplu olarak ele alınmasını ve GCHQ'nun veri madenciliği süreçlerinde toplanan verilerin analiz edilebilmesi için 30 güne kadar verilerin kullanılabilmesini ve saklanabilmesini sağlayan, muazzam miktarlarda iletişime erişebilen ve bunları işleyebilen çok gelişmiş bir program olarak tanımlanmaktadır.[802] Netice olarak Snowden, sızdırmış olduğu program bilgileriyle NSA ile GCHQ'nun dünya çapında kurdukları altyapıya ve diğer hükümetlerle ve çok uluslu şirketlerle yaptıkları işbirliğine bağlı olarak insanlar ile bilgisayarlar ve cihazlar arası iletişimleri yani insanlar arasındaki tüm ilişkileri hedef gözetmeksizin otomatik olarak kaydedebildiklerini ortaya koymuştur. Böylelikle bireylerin geriye dönük olarak üçüncü kişilerin izni olmadan kişisel iletişimlerinin soruşturulmasına olanak sağlanmaktadır. Dünya çapındaki iletişim ağlarındaki pasif bilgilerden e-posta adreslerine, IP adreslerine, telefon numaraları ve kredi kartı bilgilerine ve hatta kimsenin kullanmadığı kişiye özgü parolalara kadar her veri kaydedilmektedir.[803]

Diğer taraftan, sadece NSA programları ve teknikleri ifşa edilmemiş, 2009 yılından beri NSA tarafından Hong Kong ve Çin bilgisayar ağlarına siber saldırıların gerçekleştirildiği, 2009 yılındaki G20 Zirvesi'nde yabancı politikacıların iletişiminin GCHQ tarafından engellendiği, Almanya Şansölyesi Angela Merkel'in telefonun

---

[800] UK-GCHQ, siber tehditlerin tanımlanmasını, analiz edilmesini ve bozulmasını misyon edinen, İngiliz Hükümetine bağlı siber istihbarat ve güvenlik kurumudur. Detaylı bilgi için bkz.: GCHQ, " Mission Overview", *https://www.gchq.gov.uk/section/mission/overview*, (Erişim Tarihi: 25 Mayıs 2020).

[801] Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon & R. B. J. Walker, "After Snowden: Rethinking the Impact of Surveillance", *International Political Sociology*, Cilt 8, Sayı 2, Haziran 2014, s. 122.

[802] Glenn Greenwald, *No Place To Hide: Edward Snowden, the NSA and the Surveillance State*, Penguin Group, Londra 2014, s. 117.; Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies & James Ball, "GCHQ Taps Fibre-Optic Cables For Secret Access To World's Communications", The Guardian, 21 Haziran 2013, *https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa*, (Erişim Tarihi: 25 Mayıs 2020).

[803] Laura Poitras, Mathide Bonnefoy & Dirk Wilutzky (Yapımcılar), Laura Poitras (Yönetmen), *Citizenfour* [Belgesel], Radius-TWC, ABD 2014.

2009 yılından beri dinlediğine dair bilgiler de kamuoyu ile paylaşılmıştır.[804] Almanya dışında Fransa, Brezilya, Meksika, İspanya ve AB ile BM'ye ait çeşitli ofislerde de dinlemelerin yapıldığı belirtilmiştir. Ek olarak ise ABD'nin sadece düşman gördüğü ülkeleri değil, müttefiklerine yönelik de siber ekonomik casusluk operasyonları gerçekleştirdiği ortaya çıkarılmıştır.[805]

Tüm zamanların en büyük vatandaşlık hakları ihlali olarak yorumlanan Snowden sızıntıları sonrası kamuoyu tarafından Snowden'ı kahraman olarak gören kesimin yanı sıra onu vatan haini olarak gören bir başka kesim de söz konusu olmuştur.[806] Onu destekleyen kesimin tespitine göre Snowden, muazzam boyutlarda kişisel fedakârlıklar yaparak demokrasi ve 21. yüzyılın özgürlük anlayışı olarak ele alınan kişisel yaşamın gizliliği ve mahremiyet savunucusu bir kahraman olarak öne çıkarılmaktadır. Onu eleştiren kesime göre ise Snowden, ülkesinin gizli bilgilerini başka bir ülkenin –Rusya– casusu olarak para karşılığında ifşa eden bir vatan haini olarak tanımlanmaktadır.[807] Nitekim Amerikan halkının çoğunluğunun ikinci görüşü benimsediği ve sızdırılan NSA belgelerindeki programlar hakkında bilgi sahibi olmamalarına rağmen Snowden'ın yasadışı davrandığı ve yargılanması gerektiğine dair inancı 2013 yılında ABD içerisinde yapılan çeşitli kamuoyu yoklamalarında görülmüştür.[808] 21 Haziran 2013 tarihinde ABD Hükümeti tarafından Casusluk Yasası'nın (*The Espionage Act*) iki defa ihlali ve hırsızlık suçlamalarıyla itham

---

[804] James Pomfret, "Ex-CIA man's snooping claims raise alarm bells in Hong Kong", Reuters, 13 Haziran 2013, *https://www.reuters.com/article/us-usa-security-hongkong/ex-cia-mans-snooping-claims-raise-alarm-bells-in-hong-kong-idUSBRE95C08920130613*, (Erişim Tarihi: 25 Mayıs 2020).; Lee Ferran & Akiko Fujita, "Edward Snowden Claims NSA Documents Show U.S. Hacks China: Report", ABC News, 12 Haziran 2013, *https://abcnews.go.com/Blotter/edward-snowden-claims-evidence-shows-us-hacks-china/story?id=19384436*, (Erişim Tarihi: 25 Mayıs 2020).; Te-Ping Chen, "Snowden Alleges U.S. Hacking in China", The Wall Street Journal, 23 Haziran 2013, *https://www.wsj.com/articles/SB10001424127887324577904578562483284884530*, (Erişim Tarihi: 25 Mayıs 2020).; Nicholas Watt & Rowena Mason, "Angela Merkel phone-bugging claims are result of Snowden leaks, MP claims", The Guardian, 24 Ekim 2013, *https://www.theguardian.com/world/2013/oct/24/angela-merkel-bugging-snowden-leaks-mp*, (Erişim Tarihi: 25 Mayıs 2020).; BBC News, "Snowden NSA: Germany drops Merkel phone-tapping probe", 12 Haziran 2015, *https://www.bbc.com/news/world-europe-33106044*, (Erişim Tarihi: 25 Mayıs 2020).

[805] Ioannis L. Konstantopoulos, "Democracy and Ethics vs. Intelligence and Security: From WikiLeaks to Snowden", Editörler: George C. Bitros & Nicholas C. Kyriazis, *Democracy and an Open-Economy World Order*, Springer International Publishing AG, Cham 2017, ss. 14-15.

[806] Jeff Jarvis, "The Debate Continues On Edward Snowden: Hero or Traitor", The Guardian, 26 Kasım 2013, *https://www.theguardian.com/commentisfree/2013/nov/26/edward-snowden-hero-traitor-debate*, (Erişim Tarihi: 26 Mayıs 2020).

[807] Ioannis L. Konstantopoulos, *a.g.m.*, s. 15.

[808] Melissa Higgins, *Edward Snowden: NSA Whistle-Blower*, Abdo Publishing, Minnesota 2017, s. 67.

edilerek pasaportu iptal edilen ve Hong Kong'tan iade talebinde bulunulan Snowden, *WikiLeaks*'in de desteğiyle Moskova'ya geçmiş ve Rusya'ya sığınma talebinde bulunmuştur. 1 Ağustos 2013 tarihinde Rusya tarafından sığınma hakkı tanınan Snowden, halen Rusya'da bulunmaktadır.[809]

Snowden tarafından sızdırılan belgelerin yaratmış olduğu etkilere bakıldığında çeşitli sonuçlar görülmektedir. Siyasal açıdan ele alındığında, 9/11 Terör Saldırıları sonrasındaki yeni Uluslararası İlişkilerin siber boyuttaki yansımaları Snowden sayesinde çok daha net görülmüştür. Bilindiği üzere 9/11 Terör Saldırıları sonrasında tehdit algısı değişimi hızlanmış, şiddetin ulusal sınırlara bakılmaksızın küçük bir aşırılık yanlısı grup ya da bireyler tarafından gerçekleştirilebileceği tecrübe edilmiş ve makro ölçekte çok yönlü güvenlik anlayışı geliştirilmiştir. Laura Poitras'ın *Citizenfour* isimli belgeselinin başlangıcında eski NSA kripto-matematikçilerinden Willian Binney'in de belirttiği üzere 9/11 Terör Saldırıları'ndan sadece birkaç gün sonra NSA ABD'deki herkesi aktif olarak izlemeye karar vermiş, mahkeme kararlarıyla telekomünikasyon verileri alınarak izlemenin kapsamı ve altyapısı hızla genişletilmiştir.[810] Sonrasında hızla kolluk kuvvetleri ve istihbarat teşkilatlarının erişimini önemli ölçüde arttıran yeni yasalar –örneğin ABD Vatanseverlik Yasası (*The Patriot Act*), 2001– getirilmiş ve siber uzay sahasındaki özel sektöre devlet baskısı mahkeme kararları, ulusal güvenlik mektupları, işletme ruhsatlarının alıkonulması gibi çeşitli resmi ve gayri resmi yollar üzerinden giderek artmıştır. İnternet devi şirketlerin altyapılarının çoğunun ABD'de olması ve ABD Hükümetinin bu şirketlere yönelik artan baskıları, siber uzay sahasının fiziksel coğrafyasının önemini gözler önüne sermektedir.[811] Dolayısıyla devlet aktörlerinden bağımsız bir gelişme süreci yaşan siber uzay alanı, 9/11 Terör saldırıları sonrasında ABD baskınlığının artmasıyla birlikte devlet aktörlerinin rolünü arttığı bir sahaya

---

[809] Laura Poitras, Mathide Bonnefoy & Dirk Wilutzky (Yapımcılar), Laura Poitras (Yönetmen), *Citizenfour* [Belgesel], Radius-TWC, ABD 2014.; Mary Ilyushina, "Edward Snowden Requests A Three-Year Extension of Russian Residency", CNN, 17 Nisan 2020, *https://edition.cnn.com/2020/04/16/europe/edward-snowden-russian-residency-intl/index.html*, (Erişim Tarihi: 26 Mayıs 2020).; Sputnik Türkiye, "Snowden Rusya'dan Oturma İzninin Uzatılmasını Talep Etti", 17 Nisan 2020, *https://tr.sputniknews.com/politika/202004171041850401-edward-snowden-rusyadan-oturma-izninin-uzatilmasini-talep-etti/*, (Erişim Tarihi: 26 Mayıs 2020).

[810] Laura Poitras, Mathide Bonnefoy & Dirk Wilutzky (Yapımcılar), Laura Poitras (Yönetmen), *Citizenfour* [Belgesel], Radius-TWC, ABD 2014.

[811] Ron Deibert, "The Geopolitics of Cyberspace After Snowden", *Current History*, Cilt 114, Sayı 768, Ocak 2015, ss. 10-11.

evrilmiştir. Hukuki yansımalara bakıldığında ise BM, Uluslararası Adalet Divanı (UAD), Avrupa İnsan Hakları Mahkemesi (AHİM), Avrupa içindeki çeşitli yerel mahkemelerin kararları ve hatta ABD'deki iç politika değişiklikleri, gizlilik hakkının daha iyi korunmasına yönelik baskıları arttırmıştır. Mahkeme kararlarının bağlayıcılığı sayesinde devletlerin yabancı gözetleme uygulamalarında şekil değişikliği için doğrudan gereklilikler yaratılmakta ve insan hakları kurumlarının eylemleriyle devletler, vatandaşların gizlilik ve güvenlik dengesinin gizlilik tarafına daha fazla ağırlık vermeye zorlanmaktadır.[812] Ekonomik açıdan ise sadece Amerikan ekonomisi değil, küresel teknoloji endüstrisi de önemli bir darbe almıştır. Müşteri gizliliği koruma zaafiyeti belgelenen *Google, Facebook, Apple* gibi teknoloji devlerinin 35 Milyar Doları bulan pazar payı ve kar marjı azalmaları ile müşteri güven kayıpları yaşanmıştır.[813] Öte yandan Brezilya, daha öncesinde Amerikan firması *Boeing* ile yapmış olduğu savaş uçağı alım sözleşmesini iptal ederek İsveçli *Saab* şirketiyle 36 savaş uçağı karşılığında 4.5 Milyar Dolarlık sözleşme imzalamıştır.[814] Dahası, Almanya ve Brezilya, liderlerinin dinlenmesine yönelik sadece soruşturma başlatmakla kalmamış, İnternet trafiğinin ABD üzerinden geçmesine gerek kalmayacak şekilde yeni İnternet altyapıları inşa edilmesi taahhüdünü ve ABD ticari çıkarlarına zarar verebilecek ve Amerikan şirketlerinin yüksek uyum maliyetleri nedeniyle yeni pazarlara girmesini engelleyebilecek veri yerelleştirmesi önerilerini dile getirmiştir.[815] Yine Almanya ve Brezilya tarafından BM Genel Kurulu'na sunulan "Dijital Çağda Gizlilik Hakkı" (*The Right to Privacy in the Digital Age*) tasarısı 18 Aralık 2013 tarihinde BM Genel Kurulu'nda kabul edilerek, çevrimdışı kişilerin sahip oldukları hakların çevrimiçi ortamda da korunması gerektiği teyit edilmiş ve tüm devletler iletişim gözetimi, müdahalesi ve

---

[812] Ashley Deeks, éAn International Legal Framework for Surveillance", *Virginia Journal of International Law*, Cilt 55, Sayı 2, Bahar 2015, s. 333.

[813] Rob Lever, "Snowden Revelations Costly For US Tech Firms, Study Says", 9 Haziran 2015, *https://phys.org/news/2015-06-snowden-revelations-costly-tech-firms.html*, (Erişim Tarihi: 26 Mayıs 2020).

[814] Matthew Cowley, "Saab Gets $4.5 Billion Contract From Brazil for 36 Fighter Jets", The Wall Street Journal, 18 Aralık 2013, *https://www.wsj.com/articles/brazil-to-announce-fighter-jet-contract-results-1387388061*, (Erişim Tarihi: 26 Mayıs 2020).; BBC News, "Saab Wins $4.5bn Brazil Fighter Jet Contract", 19 Aralık 2013, *https://www.bbc.com/news/business-25441231*, (Erişim Tarihi: 26 Mayıs 2020).

[815] Danielle Kehl, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*, New America's Open Technology Institute, Policy Paper, Temmuz 2014, s. 11.

kişisel verilerin toplanması hususlarında mevcut prosedür, uygulama ve mevzuatları gözden geçirmeye çağrılmıştır.[816] Sızıntıların bir diğer sonucu olarak ise *Google, Yahoo, Microsoft* ve diğer teknoloji şirketleri, veri trafiğinin yığın şeklinde toplanmasını durdurmak için fiber optik hatları boyunca yüksek maliyetli şifreleme yazılımları kurmaya başlamışlardır. Bazı İnternet şirketleri ise gizli izleme ve dinlemeleri azaltmak için İnternet trafiğini diğer şirketlerin sunucuları üzerinden yönlendirmeye başlamıştır.[817]

Netice olarak Snowden sızıntıları, ABD'nin müttefikleriyle olan politik ve diplomatik ilişkilerine zarar vermekle kalmamış, ABD'nin yumuşak gücünün ve istihbarat yeteneklerinin darbe almasına neden olmuştur. NSA'in ifşa edilen gizli faaliyetleri, bir taraftan ABD'ye stratejik bir avantaj kaybı yaşatırken, diğer taraftan ise siber alanda hem güven hem de güvenlik anlayışını zedelemiştir. Devletlere ve istihbarat aygıtlarına olan güvenin yanı sıra teknoloji sağlayıcılarına yönelik kamusal güven azalmıştır. İnternet özgürlüğü hususundaki en büyük savunucu imajını kaybeden ABD, uluslararası alanda ciddi anlamda itibar kaybetmiştir. Küresel teknoloji endüstrisi ekonomik olarak büyük zarar görmüş, bununla birlikte teknoloji şirketlerine yönelik devlet baskıları ortaya çıkmıştır. Diğer taraftan ise söz konusu sızıntılar sayesinde kamuoyunda demokrasinin ve insan haklarının korunmasına ve şeffaflığın güçlendirilerek kişisel gizliliğin arttırılmasına yönelik tartışmaların önemli seviyelerde artması sağlanmıştır. Siber alandaki devlet aktörlerinin yapılanmaları ve uygulamaları ise modernizasyona tabi olmuştur.[818] Son olarak Snowden'ın NSA'ye ait elindeki tüm bilgileri açıklamadığına dair spekülasyonlar bulunmaktadır. Snowden'ın yakalanması ya da fiziksel olarak zarar görmesi durumunda yeni çok gizli bilgi sızıntılarının yaşanması olasılığının, ABD'nin azalan İnternet kontrolü denetleme güvenine çok daha büyük ve kalıcı hasarlar doğurabileceği düşünülmektedir.[819]

---

[816] United Nations, "The Right To Privacy In The Digital Age", A/RES/68/167, 18 Aralık 2013, *https://undocs.org/en/A/RES/68/167*, (Erişim Tarihi: 26 Mayıs 2020).
[817] Melissa Higgins, *a.g.e.*, s. 84.
[818] Ioannis L. Konstantopoulos, *a.g.m.*, ss. 16-17.
[819] Suné von Solms & Renier van Heerden, "The Consequences of Edward Snowden NSA Related Information Disclosures", *Proceedings of The 10th International Conference on Cyber Warfare and Security ICCWS-2015*, University of Venda & The Council for Scientific and Industrial Research, Kruger National Park, Güney Afrika, 24-25 Mart 2015, s. 366.

4.7. Ukrayna Saldırıları (2017)

2017 yılının Haziran ayında gerçekleşen Ukrayna saldırılarının iyi idrak edilebilmesi açısından tarihsel arka planının ve yaşanan gelişmelerin kronolojik olarak incelenmesi son derece önem taşımaktadır. SSCB'nin dağılmasıyla bağımsızlığını kazanan Ukrayna ile Rusya Federasyonu arasındaki ilişkiler inişli çıkışlı bir karaktere sahiptir. Ruslar, her daim eski Sovyet Cumhuriyetleri üzerinde belirli bir kontrol sağlama ve etki alanı oluşturma gayesi gütmüşlerdir. Nüfuz mücadelesinin yanı sıra 2004 yılındaki Ukrayna seçimlerinde yaşanan "Turuncu Devrim"[820] ve doğal gaz kaynakları konusundaki anlaşmazlıklar, genel olarak Ukrayna-Rusya ilişkilerinin temel odağını oluşturmuştur.[821] 2007 yılında Ukrayna'nın AB ile ortaklık ve serbest ticaret anlaşmaları üzerine müzakerelere başlamasıyla birlikte artan Batı'yla yakınlaşma durumu, Ukrayna ile derin siyasi ve ekonomik bağlantılara sahip olan Rusya'yı rahatsız etmiş ve Batı'nın Ukrayna'nın geleceği üzerindeki etkisinin ve belirleyiciliğinin giderek arttığı algısını yaratmıştır. 2004 yılındaki Turuncu Devrim'de Cumhurbaşkanlığını kaybeden Rus yanlısı Viktor Yanukoviç, 2006 yılında Başbakan, 2010 yılında ise Cumhurbaşkanı olmuş, 21 Kasım 2013 tarihinde ise AB ile Ortaklık Anlaşması'nı (*Association Agreement*) imzalama hazırlıklarını askıya aldığını duyurmuştur. Ukrayna'nın AB ile işbirliğindeki bu geri dönüşünün nedenleri arasında yaklaşan 2015 seçimleri, Rus baskısı, giderek bozulan Ukrayna ekonomisinin dengelenebilmesi adına Ukrayna mallarının Rusya pazarına sürekli erişiminin sağlanabilmesi, Rusya ile kredi ve gaz sözleşmelerinin yeniden müzakere edilmesi umutları gibi çeşitli faktörler

[820] Turuncu Devrim: 21 Kasım 2004 tarihindeki Ukrayna Cumhurbaşkanlığı seçimlerinde Viktor Yuşçenko ile Viktor Yanukoviç aday olmuşlar, Viktor Yanukoviç'in seçimleri kazandığının ilan edilmesi üzerine 22 Kasım 2004 tarihinden itibaren Kiev Bağımsızlık Meydanı'nda Viktor Yuşçenko taraftarları toplanmışlardır. Yuşçenko'nun seçim kampanyası boyunca kullandığı renk olan turuncuya ithafen göstericiler turuncu giyinmişler ve ülke çapında seçime hile karıştırıldığına yönelik şiddet içermeyen protesto gösterileri düzenlemişlerdir. Neticede seçimler geçersiz sayılmış ve Aralık ayında yapılan yeni seçimleri Viktor Yuşçenko kazanmıştır. Turuncu Devrim olarak adlandırılan bu süreç, komünizm sonrası Doğu Avrupa jeopolitiğinde Batı'ya dönüşümün yeni bir dönüm noktası olarak yorumlanmıştır. Detaylı bilgi için bkz.: Adrian Karatnycky, "Ukraine's Orange Revolution", *Foreign Affairs*, Cilt 84, Sayı 2, Mart-Nisan 2005, ss. 35-52.

[821] Marie Baezner, *Cyber and Information Warfare In The Ukrainian Conflict*, Center for Security Studies (CSS) Cyber Defense Project Report, Zürih, Ekim 2018, s. 7.

gösterilmiştir.[822] Viktor Yanukoviç'in bu kararı, Ukrayna'daki iç siyasi durumun daha istikrarsızlaşmasına neden olarak siyasi gerginliğin kaynama noktasına ulaşmasına neden olmuştur. Sonrasında ise AB yanlısı Ukraynalılar tarafından "*Euromaidan*" olarak adlandırılan çeşitli protestolar yine Kiev Bağımsızlık Meydanı'nda (*Maidan Nezalezhnosti*) başlamış ve ülkenin çeşitli yerlerinde meydana gelen çatışmalar Ukrayna'yı iç savaşın eşiğine getirmiştir. 100'den fazla kişinin hayatını kaybettiği olaylar, Cumhurbaşkanı Viktor Yanukoviç'in 21 Şubat 2014 tarihinde Ukrayna'da siyasi krizin çözümüne ilişkin anlaşmayı imzalamasıyla son bulmuştur. Cumhurbaşkanı Viktor Yanukoviç ise bir gün sonrasında Rusya'nın yardımıyla Ukrayna'dan kaçmıştır.[823] Ardından 27-28 Şubat 2014 tarihlerinde Rus yanlısı silahlı kişilerin Kırım'ın kilit kurumlarıyla birlikte etnik çoğunluğunu Rusların oluşturduğu Kırım Yarımadası'nın kontrolünü ele geçirmesi gelişmesi yaşanmıştır. 16 Mart 2014 tarihinde Ukrayna ve Batı tarafından yasadışı kabul edilen bir referandum gerçekleştirilmiş ve Kırım'ın bağımsızlığı ilan edilmiştir. İki gün sonrasında ise Rus ve Kırım liderleri Moskova'da biraraya gelerek Kırım Yarımadası'nı Rusya'ya bağlayan bir anlaşma imzalamışlardır. Böylelikle Kırım'ın Rusya tarafından ilhakı gerçekleşmiş ve bölgeden çok sayıda Ukraynalı ve Kırım Tatarı vatandaş kaçmak zorunda bırakılmıştır.[824]

---

[822] Wojciech Konończuk, "Ukraine Withdraws From Signing The Association Agreement in Vilnius: The Motives and Implications", Centre For Eastern Studies (OSW), 27 Kasım 2013, *https://www.osw.waw.pl/en/publikacje/analyses/2013-11-27/ukraine-withdraws-signing-association-agreement-vilnius-motives-and*, (Erişim Tarihi: 12 Mayıs 2020).; Ian Traynor & Oksana Grytsenko, "Ukraine Suspends Talks On EU Trade Pact As Putin Wins Tug of War", The Guardian, 21 Kasım 2013, *https://www.theguardian.com/world/2013/nov/21/ukraine-suspends-preparations-eu-trade-pact*, (Erişim Tarihi: 12 Mayıs 2020).

[823] BBC News, "Ukraine Protests After Yanukovych EU Deal Rejection", 30 Kasım 2013, *https://www.bbc.com/news/world-europe-25162563*, (Erişim Tarihi: 12 Mayıs 2020).; Oksana Grytsenko, "Ukrainian Protesters Flood Kiev After President Pulls Out of EU Deal", 24 Kasım 2013, *https://www.theguardian.com/world/2013/nov/24/ukraine-protesters-yanukovych-aborts-eu-deal-russia*, (Erişim Tarihi: 12 Mayıs 2020).; BBC News, "Putin: Russia Helped Yanukovych to Flee Ukraine", 24 Ekim 2014, *https://www.bbc.com/news/world-europe-29761799*, (Erişim Tarihi: 12 Mayıs 2020).; CBS News, "Opposition Signs Deal Aiming to End Ukraine's Deadly Crisis", 21 Şubat 2014, *https://www.cbsnews.com/news/ukraine-protest-leaders-sign-deal-to-end-crisis-in-kiev/*, (Erişim Tarihi: 12 Mayıs 2020).

[824] John Simpson, "Russia's Crimea Plan Detailed, Secret and Successful", BBC News, 19 Mart 2014, *https://www.bbc.com/news/world-europe-26644082*, (Erişim Tarihi: 12 Mayıs 2020).; Alan Yuhas, "Russian Propaganda Over Crimea and the Ukraine: How Does It Work?", The Guardian, 17 Mart 2014, *https://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media*, (Erişim Tarihi: 12 Mayıs 2020).; Andrew E. Kramer & Michael R. Gordon, "Ukraine Reports Russian Invasion on a New Front", The New York Times, 27 Ağustos 2014,

Kırım'ın ilhakı sonrasındaki gelişmeler, çeşitli çatışmaların yaşandığı, sıcak çatışmalar kadar siber saldırıların da ağırlık kazandığı ve değişik etkilerin gözlemlendiği bir süreç olarak dikkat çekmektedir. Öyle ki Ukrayna Hükümeti Rusya'yı 2016 yılının son iki ayında altyapısına ve kamu kurumlarına gerçekleşen 6500'den fazla siber saldırıyı organize etmekle suçlamıştır ancak söz konusu suçlamalar defalarca Rus yetkililer tarafından reddedilmiştir.[825] 23 Aralık 2015 tarihinde Ukrayna'da gerçekleşen meşhur elektrik kesintisinden birkaç gün öncesinde Ukrayna yanlısı aktivistler, Kırım'a elektrik sağlayan trafo merkezlerine fiziksel olarak saldırmış ve yaklaşık iki milyonluk Kırım nüfusunun geçici süreyle elektriksiz kalmasına neden olmuştur. Bu saldırıya müteakip Ukrayna'da gerçekleşen elektrik kesintilerinin Kırım trafo merkezlerine yönelik gerçekleştirilen fiziksel saldırılara misilleme olduğu yönünde spekülasyonlar yaygın olmakla birlikte Ukrayna enerji şirketlerine yönelik siber operasyonların en az altı ay öncesinden başladığı tespit edilmiştir. Dolayısıyla Kırım'daki saldırıların orijinal motivasyon olmamakla beraber katalizör etkisinde bulunduğu iddia edilmiştir. 2015 yılı Aralık ayında Ukrayna'da gerçekleşen son derece organize ve planlı siber saldırılar neticesinde Ukrayna'nın batısındaki Ivano-Frankvisk bölgesinde yaklaşık 700.000'den fazla kişinin saatlerce elektriksiz kalması sağlanmıştır. Çok sayıda trafoyu devre dışı bırakan, çağrı merkezlerini kitleyen ve bilgisayarların önemli sistem dosyalarını silerek çökmesine neden olan bu saldırılar, siber silahların nasıl modern bir savaş aracı haline geldiğine dair ciddi anlamda bir uyarı sunulması şeklinde yorumlanmıştır.[826] Bir yıl sonrasında, 17 Aralık 2016 tarihinde, Ukrayna'nın elektrik şebekesi tekrardan büyük bir siber saldırı yaşamış ve yaklaşık 225.000 kullanıcının elektriği kesilmiştir. 2015 yılındaki saldırıya benzer şekilde

---

https://www.nytimes.com/2014/08/28/world/europe/ukraine-russia-novoazovsk-crimea.html?auth=login-google, (Erişim Tarihi: 12 Mayıs 2020).; Open Society Foundations, "Understanding Ukraine's Euromaidan Protests", Mayıs 2019, *https://www.opensocietyfoundations.org/explainers/understanding-ukraines-euromaidan-protests*, (Erişim Tarihi: 12 Mayıs 2020).

[825] Julia E. Sullivana & Dmitriy Kamensky, "How Cyber-Attacks In Ukraine Show The Vulnerability of the U.S. Power Grid", *The Electric Journal*, Cilt 30, Sayı 3, Nisan 2017, s. 31.

[826] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", Wired, 3 Mart 2016, *https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/*, (Erişim Tarihi: 13 Mayıs 2020).; Elias Groll, "Did Russia Knock Out Ukraine's Power Grid?", Foreign Policy, 8 Ocak 2016, *https://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/*, (Erişim Tarihi: 13 Mayıs 2020).; BBC News, "Ukraine Power Cut 'Was Cyber-Attack'", 11 Ocak 2017, *https://www.bbc.com/news/technology-38573074*, (Erişim Tarihi: 13 Mayıs 2020).

yapılan saldırı, ilk saldırıdan daha karmaşık özellikler sergilemesine rağmen işçilerin trafo merkezlerine gelerek manuel olarak kesicileri kapatmasıyla birkaç saat içerisinde çözülmüştür. Bu saldırıda kullanılan ve siber güvenlik uzmanlarınca "*CrashOverride*" olarak isimlendirilen kötü amaçlı yazılım, fiziksel endüstriyel süreçleri bozmak için tasarlanan, kullanılan ve tespit edilen –Stuxnet'ten sonraki– ikinci kötü amaçlı yazılım, elektrik şebekelerine saldırmak için tasarlanan ise ilk kötü amaçlı yazılım olarak tanımlanmıştır. Söz konusu yazılımın işlevselliğinin casusluğu kapsamadığı, sadece geçici olarak elektrik kesintilerine yol açmak için hazırlandığı tespit edilmiştir.[827]

Son yıllarda Rusya ile Ukrayna arasında yaşanan çatışma ve yüksek gerginlik hali, Rus siber savaş teknikleri ve araçları için Ukrayna'yı bir çeşit test sahası haline getirmiştir. 2015-2016 yıllarında "*Fancy Bear*" olarak bilinen Rusya sponsorlu bilgisayar korsanları grubu, Amerikan sunucularına saldırılar düzenlerken, "*Sandworm*" isimli bir başka grup ise Ukrayna hükümetine ait kurumlara ve özel sektördeki şirketlere çok sayıda siber saldırı gerçekleştirmiştir. Her yıl mevsimsel bir ritimle Ukrayna'ya gerçekleştirilen bu saldırılar, 2017 yılına gelindiğinde dijital tarihin en yıkıcı ve küresel çaplı yoğun etkiler doğuran saldırılarından birine dönüşmüştür: *NotPetya*.[828] Küçük bir Ukraynalı yazılım firması olan *Linkos Group*'un sunucularından başlayan saldırı, neredeyse ülke genelinde kullanılan bir muhasebe yazılımıyla ilgili sözleşmelerden biri olan *M.E.Doc* üzerinden dünya çapındaki binlerce sunucuya gizli arka kapı erişimleri kurmuş ve bunlar, *NotPetya* isimli kötü amaçlı yazılımın yayılması için kullanılmıştır. 2017 yılının Haziran ayında Ukrayna'da ortaya çıkmasından saatler sonra dünyaya yayılmış ve o zamana kadar görülen en hızlı yayılan kötü amaçlı yazılım parçası olarak tanımlanmıştır.[829] Bir ay öncesinde 12 Mayıs 2017 tarihinde ortaya çıkan "*WannaCry*" –*WannaCrypt0r., WannaCrypt*– isimli fidye yazılımı, enerji dağıtım şirketleri,

---

[827] Kevin E. Hemsley & Ronald E. Fisher, *History of Industrial Control System Cyber Incidents*, U.S. Department of Energy, Office of Nuclear Energy, DOE Idaho National Laboratory, Report, INL/CON-18-44411-Revision-2, Aralık 2018, ss. 18-19.

[828] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, 22 Ağustos 2018, *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*, (Erişim Tarihi: 13 Mayıs 2020).

[829] Louis Léonet, *Contextual Cyber Securitisation: A Case Study of Russian Cyberattacks against Ukraine*, Danışman: Matthew Frear, Master Tezi, International Relations, Universiteit Leiden, Leiden, Hollanda, Temmuz 2019, s. 16.

demiryolları, otomobil endüstrileri ve hükümetler dahil olmak üzere 150'den fazla ülkede 200.000'den fazla kurumu doğrudan etkilemiş ve dünya çapında yaklaşık 4 ila 8 Milyar Dolar arası hasar yaratarak o zamana kadarki en pahalı siber saldırı olarak kabul edilmiştir.[830] Mart 2016'da ilk olarak tanıklık edilen "*Petya*" isimli fidye yazılımının varyasyonlarından biri olan *NotPetya* ise, benzer özellikler taşımakla birlikte önemli farklılıklar da barındırmaktadır: Buna göre *Petya* fidye yazılımı, bir kullanıcının bilmeden etkinleştirmesini isterken, *NotPetya* kendi kendine yayılmakta ve daha fazla bileşeni şifrelemektedir. *NotPetya* tarafından enfekte edilen makineler *Windows*'a erişim sunma yeteneğini kaybetmekte ve kullanıcıların makineleri kullanmasını engelleyebilmektedir. *Petya*'nın aksine *NotPetya*, özellikle yıkıcı olarak tasarlanmış kötü amaçlı bir yazılımdır ve küresel çapta etkiler yaratmasına rağmen birincil hedefi Ukrayna olmuştur.[831] Ukrayna bankaları, enerji şirketleri, devlete ait İnternet kaynakları ve yerel ağlar, Ukrayna medyası ve özel sektöre ait büyük firmalar, doğrudan zarar görmüştür. *NotPetya*'nın dünya çapında gerçekleştirdiği saldırıların %75,24'ünün Ukrayna'ya yönelik olduğu belirtilmiştir.[832] *NotPetya* yazılımı, özel olarak enerji şebekelerini veya kritik altyapıları hedeflememekle birlikte kapsam ve etki boyutu açısından çok çeşitli sektörlere doğrudan etkiler yaratmıştır ve dünya çapında oluşturduğu zararın ise 10 Milyar Doları aştığı tahmin edilmektedir.[833]

Netice olarak 2017 yılından itibaren Ukrayna'nın dâhil olduğu siber uzay sahasında çeşitli araçlar, teknikler, hedefler ve aktörler konusundan bir dizi izlerleme yaşanmıştır. Özellikle geliştirilen yeni kötü amaçlı yazılımların ve siber silahların, Ukrayna hedeflerine yönelik oldukça etkili olduğu görülmüş ve siber alandaki aktörler açısından önemli bilgiler ortaya çıkmıştır. 2015 ve 2016 yıllarında elektrik şebekelerine yönelik gerçekleştirilen organize siber saldırılar, 2017 yılında *NotPetya*

---

[830] Marcelo Ayres Branquinho, "Ransomware In Industrial Control Systems: What Comes After WannaCry and Petya Global Attack?", Editörler: C. A. Brebbia, F. Garzia & M. Lombardi, *WIT Transactions on The Built Environment*, Safety and Security Engineering VII, WIT Press, Cilt 174, Southampton 2017, s. 332.

[831] Jagmeet Singh Aidan, Harsh Kumar Verma & Lalit Kumar Awasthi, "Comprehensive Survey on Petya Ransomware Attack", *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, Aralık 2017, s. 124.

[832] Myroslav Komar, Vitaliy Dorosh, Grygoriy Hladiy & Anatoliy Sachenko, "Deep Neural Network for Detection of Cyber Attacks", *2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC)*, Kiev, 8-12 Ekim 2018, s. 1.

[833] Kevin E. Hemsley & Ronald E. Fisher, *a.g.e.*, s. 21.

yazılımının hastanelerden ATM'lere, demiryollarından fabrikalara, nakliye ve inşaat firmalarından çok uluslu şirketlere ve devlet kurumlarına kadar yaşamın her alanında yarattığı doğrudan yıkıcı etkiler, Kırım'ın Ruslar tarafından ilhak edilmesinden beri devamlı ve düşük şiddetli olarak devam eden binlerce DDoS saldırısı ve çevrimiçi sayfa kusurları, 2018 yılından itibaren Ukrayna'nın siber güvenlik konusunda yeni yatırımlar geliştirmesine, siber güvenliğe verdiği önemin ve ayırdığı bütçenin artmasına ve başta ABD'den olmak üzere çeşitli ülkelerden yeni siber güvenlik projelerinin tesisi için uluslararası ekonomik yardım ve proje desteği görmesine vesile olmuştur.[834] Son olarak; Ukrayna'da yaşanan siber gelişmeler, ulusal ve uluslararası ilişkilerin dijitalizasyonunun hangi boyutlara ulaştığını sadece gözler önüne sermekle kalmamış, aynı zamanda da Siber Uluslararası İlişkilerde güvenlik inşası adına uluslararası işbirliği çabalarının arttırılması gerekliliğini bir kez daha net şekilde ortaya koymuştur.

[834] Marie Baezner, *a.g.e.*, ss. 35-36.; U.S. Department of State, "The United States and Ukraine Hold Third Cyber Dialogue", Media Note, Office of the Spokesperson, 3 Mart 2020, *https://www.state.gov/the-united-states-and-ukraine-hold-third-cyber-dialogue/*, (Erişim Tarihi: 13 Mayıs 2020).; Pavel Polityuk, "Ukraine Power Distributor Plans Cyber Defense System for $20 Million", Reuters, 6 Şubat 2018, *https://www.reuters.com/article/us-ukraine-cyber-ukrenergo/ukraine-power-distributor-plans-cyber-defense-system-for-20-million-idUSKBN1FQ1TD*, (Erişim Tarihi: 13 Mayıs 2020).

SONUÇ

21. yüzyıl, yaşanan bilimsel ve teknolojik gelişmelerin yarattığı ulusal ve uluslararası geniş kapsamlı, son derece hızlı ve çok yönlü değişimler ve dönüşümler açısından son derece dikkat çekici bir süreç olmaktadır. Bilim ve teknoloji tabanlı küresel başkalaşımın öne çıktığı bu dijitalizasyon döneminde ortaya çıkan ve etki boyutu giderek artan yapısal belirsizlik ve karmaşıklık halini eş zamanlı olarak aktörel çeşitlilik artışı desteklemektedir. Bilimsel bilginin uygulanabilirliğinin genişlemesi ve teknolojik ilerlemeler neticesinde üretim seçeneklerinden iletişim ve ulaşım teknolojilerine kadar yaşanan kapsamlı değişim ve dönüşümler, ulusal ve uluslararası boyutlarda ekonomik, siyasi, askeri, hukuki ve kültürel etkiler yaratmıştır. Söz konusu dönemin öne çıkan en belirgin iki özelliği olarak "hız" ve "dönüşüm", insanların yaşamını bir yandan kolaylaştırmakta ve pratiklik sağlamaktayken, diğer yandan ise yıkıcılığın arttığı çatışma ve savaşlarla beraber küresel iklim değişikliği ya da biyoçeşitliliğin azalması gibi doğrudan insan yaşamını etkileyen olumsuz yan etkiler ve riskler de göstermektedir.

Uluslararası sistem açısından yaklaşıldığında ise Uluslararası İlişkilerin baskın aktörleri olan devletlerin, nükleer teknoloji yetkinliği tabanlı güç anlayışının belirleyicilik ve caydırıcılık avantajlarının yanı sıra uluslararası sistem içerisindeki aksiyonların değişkeni olarak sistem dâhilinde sunulan imkânlar ve artan aktörel çeşitlilik durumu gibi dezavantajların da öne çıktığı görülmektedir. Uluslararası İlişkiler aktörlerinin bu yeni dijital dünya içerisinde rekabet edebilir konumda olabilmesinin temel dayanağının bilimsel ve teknolojik bilgiye dayalı yeni yetenekler üretebilmesinde ve ürettiği bu yeni yetenekleri koruyarak hızlı şekilde geliştirebilmesinde olduğu görülmektedir. Dolayısıyla bilim, teknoloji ve Uluslararası İlişkiler arasındaki işteş bağ, 21. yüzyıl itibariyle daha öncesinde hiç olmadığı kadar derin ve geniş boyutlara ulaşmıştır. Öyle ki, bilimsel ilerlemeler teknolojik gelişmeleri hızlandırmış, teknolojik gelişmeler neticesinde elde edilen yeni bilgiler ise bilimsel anlamda yeni perspektifler oluşturmuştur. Söz konusu yeni perspektiflerle beraber yepyeni fenomenler ve konular, Uluslararası İlişkiler aktörlerinin sadece gündemine girmekle kalmamış, aynı zamanda da ulusal önceliklerin ve çıkarların bu doğrultuda yeniden yapılandırılmasına vesile olmuştur.

Günümüz küresel ilişkilerindeki bilimsel bilgi ve teknolojik ilerlemelerin belirleyiciliğinin kökenine bakıldığında ise zamanın ve mekânın erişilebilirliğini arttıran, bilgiyi kaydederek geleceğe aktaran, iletişimi çeşitlendirerek hızlandıran ve demokratikleştiren "Bilgi ve İletişim Devrimi"nin yer aldığı tespit edilmiştir. Bilgi ve İletişim Devrimi, uzun soluklu teknolojik bilgi ve iletişim süreci olup odak noktasını matbaa oluşturmaktadır. Matbaa sayesinde bilginin depolanabilmesi, yeniden üretilebilmesi ve kopyalanabilmesi söz konusu olmuş, bilginin maliyeti azalarak temin süresi hızlanmış ve miktarında son derece önemli artışlar yaşanmıştır. Dünya üzerindeki farklı görüşlerin yayılmasının kolaylaştığı ve dil hegemonyalarının kırıldığı bu süreçte benzeri görülmemiş siyasi ve sosyal etkiler yaratılmıştır. Ardından optik (semafor) telgraf ve elektrikli telgrafın icadıyla birlikte iletişimdeki mesafe engeli ortadan kalkmaya başlamıştır. Bilim ve teknolojinin işteş etkisinin en iyi gözlemlendiği gelişmelerden biri olarak elektrik bilgisinin iletişime uygulanması ve elektrikli telgrafın keşfi gösterilebilmektedir. İnsan ve yük taşımacılığında kullanılan demiryolu ağları ile bilgi ve iletişim aktarımında kullanılan telgraf ağların eklektik hale gelmesi, sadece modernite ve ilerlemenin sembolü olarak yorumlanmamış, aynı zamanda da ulusal ve uluslararası ticaretin bu yönde ilerlemesine vesile olarak yeni yasaların, siyasal düzenlemelerin ve yönetim tekniklerinin geliştirilmesi ihtiyacını ortaya çıkarmıştır. Sonrasında ses iletim teknolojisi olarak geliştirilen telefon, karmaşık yapısı ve yüksek maliyetinden dolayı küresel boyutta oldukça yavaş yayılmıştır. 1970'lerden itibaren Avrupa, ABD ile rekabet edebilir hale gelmiş, ticari boyutun yanı sıra askeri ve siyasi olarak bu teknolojinin kullanılması söz konusu olmuş ve Uluslararası İlişkilerde istihbaratın yeni enstrümanlarından biri haline evrilmiştir. Gerçek zamanlı iletişim hali, devletler arası rekabetin hızlanmasını ve karar vericilerin tepki sürelerinin kısalmasını sağlayarak devletler ararası askeri ve ticari rekabeti derinleştirmiştir. Ardından radyo ve televizyonun geliştirilme çalışmaları ve radyo ve televizyon yayıncılığının ortaya çıkmasıyla beraber bilim ve teknolojinin insanlık tarafından en dinamik şekilde tecrübe edilmesi söz konusu olmuştur. Uluslararası İlişkilerde radyo ve televizyon yayıncılığı, ticari ve askeri istihbarat boyutunun yanı sıra en etkili propaganda yöntemlerinden biri olmuş ve bununla birlikte devletler tarafından toplumsal istikrar ve moral inşa enstrümanı, siyasi elitler tarafından ise kitle manipülasyonu şeklinde

kullanılmıştır. Medyanın ve kitle iletişiminin ortaya çıkmasıyla birlikte ise siyaset, diplomasi ve küresel iletişim açısından belirleyici unsur boyutuna evrilmiştir. Son olarak keşif, gözlem ve iletişim amaçlı geliştirilen uydu teknolojileri, Bilgi ve İletişim Devriminin devletler arası güç ve egemenlik mücadelelerindeki rolünü zirveye taşımıştır. Uluslararası rekabetin kara, hava ve deniz boyutlarına dış uzay sahasını dördüncü boyut olarak eklemiştir. Dolayısıyla dış uzay sahasının da siyasileşmesi ve askerileşmesi söz konusu olmuştur. Uydu sistemleri teknolojisinin küresel boyutta devasa iletişim ve gözlem kapasitesi yaratması, bir taraftan Uluslararası İlişkiler aktörlerinin ulusal ve uluslararası güvenlik tehdit unsurlarının saptanmasını kolaylaştırırken, diğer taraftan ise çok daha yıkıcı etkiler yaratabilecek yepyeni tehdit unsurlarının yaratılabilmesi potansiyelini arttırmıştır. Uydu sistemi teknolojileri, bilimsel bilgi birikimi ve teknolojik devinimin tahayyül edilemeyecek boyutlarda hızlandırarak, yeniden değişim ve dönüşüm yaşanarak mevcut kara, hava, deniz ve dış uzay sahasını birbirine bağlayan sanal bir alanın beşinci boyut olarak oluşmasını sağlamıştır. Bilhassa devletlerin kritik altyapılarını ortaya çıkan bu yeni alana hızla adapte etmeleri, devletler arası güç dengelerine yeni yaklaşımlar getirmekle birlikte Uluslararası İlişkilerdeki güvenlik, çıkar, tehdit, diplomasi gibi temel unsurların belirsizliklerle dolu bu karmaşık alanın içerisinde yeniden tanımlanma arayışlarını ortaya çıkarmıştır.

Bilim ve teknolojinin küresel ilişkilerdeki evriminin teknik sürecini Bilgi ve İletişim Devrimi oluştururken, ticari ve endüstriyel sürecini ise Sanayi Devrimleri oluşturmaktadır. Politik devrimlerin aksine Bilgi ve İletişim Devrimi ya da Sanayi Devrimleri anlık olaylardan ziyade yavaş yavaş ve kademeli olarak gerçekleşen süreçlerdir. Zaman ve mekân sınırlarını bulanıklaştırarak bilgi ve iletişimin hızlanmasını sağlayan Bilgi ve İletişim Devrimi, güç parametrelerini dönüştürerek fiziksel bağlamda doğal kaynaklara erişimi vurgulayarak Uluslararası İlişkileri ve ekonomiyi belirleyen Sanayi Devrimleri ile tamamlayacı etkileşime sahiptir. Endüstri 1.0 ile başlayan süreçte buhar makinesinin icadı ve üretime fonksiyonel olarak dâhil edilmesiyle el emeğinin makineleşme aşaması başlamıştır. Su ve buhar enerjisine dayanan mekanik üretim anlayışıyla yaşanan bu endüstriyel değişimin sosyal yapılara, demografik davranışlara ve tasarruf alışkanlıklarına doğrudan etkisi olmuştur. Endüstri 2.0 ile birlikte ise petrol türevlerine ve elektriğe dayanan yeni

üretim teknolojileri geliştirilmiş ve sanayileşmenin yayılması Batı'nın ötesine ulaşmıştır. Mühendislik, tıp ve tarım alanlarında önemli gelişmeler yaşanmakla birlikte iş bölümüne dayalı seri üretim bu dönemde başlamıştır. Endüstriyel ihtiyaçların karşılanması adına ulaşıma yatırımlar yapılmış ve demiryolu ağları genişletilmiştir. Endüstriyel devrim süreci, yaşanan iki büyük savaş ve küresel ekonomik kriz neticesinde sekteye uğramıştır. 1970'lerle birlikte bilgi ve iletişim teknolojilerinin otomasyona dâhil olması, inovasyon ve Ar-Ge çalışmalarına ağırlık verilmesi, yeni teknolojilerin sanayi ekonomilerinde benimsenmesi, mikro bilgisayarların ve programlanabilir mantık devrelerinin endüstriyel bağlamda uygulanabilir hale getirilmesi ve 1990 itibariyle İnternet ağının küresel boyutta derinleşmeye başlamasıyla beraber kişisel üretimlerin dijital üretimlerle birleşmesi yaşanmıştır. Öte yandan Endüstri 3.0 sürecinin, kıt kaynak olma özelliğine sahip fosil yakıtlara dayanan endüstriyel çağın yenilenebilir enerjilere geçiş aşaması olarak nitelendirildiği görülmüştür. 2000'lerden günümüze dek uzanan Endüstri 4.0 sürecinde ise siber-fiziksel sistemlere dayalı üretim devreye alınmış, yapay zeka teknolojileri ve akıllı üretim ön plana çıkarılmıştır. Ağ oluşturma, mekanizasyon ve dijitalleşmede yaşanan gelişmeler, fiziksel temel sistemlerin siber altyapılarının oluşturulmasına ve ağ bağlantılı standardizasyon ve entegrasyon yaratılmasını sağlamıştır. Endüstri 4.0 süreci, küresel ilişkileri hiper seviyede bağlantılı hale getirirken, aynı zamanda da güvenlik algısının ve tehdit unsurlarının karakterini değiştirmektedir. Özellikle siber alanda artan devlet dışı aktörel çeşitlilik hali, beraberinde getirdiği çeşitli meydan okumalarla birlikte önemli uluslararası güvenlik konuları etrafında uluslararası işbirliği ihtiyacını daha da kritik hale getirmiştir.

Bilgi ve İletişim Devrimi ile Sanayi Devrimleri süreçleri, rekabet alanlarının coğrafyaları aşarak elektronik ortama ulaştığını, bilgiye dayalı teknolojilerin yeni bilgi ekonomileri ve bilgi toplumları inşa ettiğini ve nihayetinde dönüşerek oluşan bu yepyeni uluslararası yapının nedensel ve ereksel tartışmalar üzerinden anlaşılabilme tartışmalarını doğurduğunu gözler önüne sermektedir. Bilimsel ve teknolojik ilerlemelerin sosyal dünyayı şekillendirebilir seviyelere ulaşmasıyla beraber bilim ve teknolojiye yönelik deterministik yaklaşımlar ile sosyal dünyaya yönelik ereksel yaklaşımların yeniden ele alınması ve tespit edilmesi gerekli olmuştur. Uluslararası İlişkilerin omurgasını oluşturan Büyük Tartışmalardaki metodoloji, kavrayış,

açıklama ve uzlaşı arayışları, algılanan karmaşık gerçekliğin daha geniş farkındalığı adına farklı teorik algıların ontolojik ve epistemolojik argümanlarını geliştirmişlerdir. Bu bağlamda "Beşinci Büyük Tartışma" olarak Prof. Dr. Emilian Kavalski tarafından geliştirilen yaklaşımda; indirgemeci yöntemler üzerinden düzen ve öngörülebilirlik esaslı doğrusal modellemeleri içeren diğer Büyük Tartışmaların aksine çeşitli fenomenlerin çeşitli biçimlerde ve çeşitli zaman formlarında var olabileceği iddia edilmiştir. Karmaşık yapılı özelliklere sahip bireylerden oluşan toplumların ve ulusların içinde ve arasındaki etkileşimlerin doğrusal yönlü fonksiyonel ilişkilerden ziyade çok değişkenli ve karmaşık sistemler olduğu vurgulanmıştır. Dolayısıyla yaşanan ulusal ve uluslararası her türlü değişim ve dönüşümün doğrusal olmayan dinamikler üzerine temellendirilen yaklaşımlar sayesinde "çeşitlilik" esaslı olduğu öne çıkarılmakta ve dünyanın yapısına yönelik öngörülebilirliğin ve kontrolün sınırlılığına dikkat çekilmektedir. Doğrusal olmayan dinamiklerin doğrusal dinamiklere kıyasla üstünlüğü ve karmaşıklığın basitliğe nazaran gerçekliği göz önünde bulundurulduğunda aslında var olan karmaşa halinin normal ve sağlıklı olduğu şeklinde yorumlanmaktadır. Buna göre; kendi kendini yapılandırma anlamına gelen "otopoez", karmaşık uluslararası sistemin istikrarlı görünen karakterinde değişimler yaratabilmekte ve Geleneksel Uluslararası İlişkiler yaklaşımlarının doğrusal perspektifleri ani, süreksiz ve beklenmedik olayları öngörme ve anlama konusunda başarısız ve yetersiz kalabilmektedir. Bu doğrultuda da Uluslararası İlişkiler disiplininin küresel politikada öne çıkan değişim, dönüşüm ve karmaşıklık olgularını açıklayan kavramsal çerçeveler oluşturma hususunda gerçekten zorlandığı görülmektedir. Bilimsel bilgi ve teknolojik ilerlemelerin oluşturduğu yapay, karmaşık ve anonim özellikli Beşinci Stratejik Alanın mevcut Uluslararası İlişkilere yansıması ve eklemlenmesi dikkate alındığında ise disiplin içerisindeki Beşinci Büyük Tartışmanın çerçevesi mahiyetinde geliştirilmeye çalışılan Karmaşık Uluslararası İlişkiler Teorisi yaklaşımının insani ve insan dışı (siber-fiziksel) sistemler arası etkileşimi anlamlandırabilme, kavramsal çerçeveler oluşturabilme ve Siber Uluslararası İlişkiler içerisinde daha büyük bilgi yüküne sahip bileşen çeşitliliğinin asimetrik ilişkilerinin karşılıklı bağımlılık modellemesinin yapılabilmesi ve tecrübe edilebilmesi adına son derece önemli olduğu düşünülmektedir.

Diğer taraftan siber uzay sahası, 21. yüzyılın öne çıkan en temel gerçekliği olarak dikkat çekmektedir. Aslına bakılırsa 20. yüzyılın ikinci yarısı itibariyle insanlığın dış uzay sahasına ulaşması ve Uluslararası İlişkilerde Uzay Çağı olarak nitelendirilen dönemin başlamasıyla birlikte uzay kavramının katmanlı yapısı ortaya çıkmıştır. Dış uzay sahasına yönelik artan bilimsel bilgi ve teknolojik yeniliklerin büyük etkisiyle birlikte ise dünyadaki tüm rekabet sahalarını doğrudan ve dolaylı olarak birbirine bağlayan, tamamıyla insan yapımı ve yapay nitelikte olan yepyeni bir sanal ortam yaratılmıştır. Diğer stratejik alanlara -hava, kara, deniz, dış uzay- kıyasla siber uzayın yapısının değiştirilebilir olması ve teknolojinin karma karakterinin bu alana en iyi şekilde yansıtılabilmesi, gerek 21. yüzyıl insan ilişkileri gerekse küresel ilişkiler üzerinde belirleyici olmuştur. Söz konusu Beşinci Stratejik Sahanın kapsamına; bilgisayarlar, İnternet, telekomünikasyon, bilgi ve iletişim teknolojileri, altyapı ağları, siber-fiziksel ve akıllı sistemler dahil olmak üzere her türlü dijital, elektronik ve sayısal unsur girmektedir. İnsanlığın gündelik hayatını doğrudan etkileyen her türlü organizasyon ve sistem -tıbbi teknolojiler, trafik ışıkları, hava trafik kontrol sistemleri, güç şebekeleri, telekomünikasyon operatörleri, İnternet sağlayıcıları, endüstriyel üretim tesisleri vs.- siber uzay alanından yönlendirilebilmekte, manipüle edilebilmekte ve üzerlerinde kontrol sağlanabilmektedir. Bundan dolayı da siber uzay, 21. yüzyıl itibariyle Uluslararası İlişkilerin baskın aktörleri olan devletlerin ulusal ve uluslararası güvenliklerini doğrudan etkileyebilen yüksek politika meselesi haline gelmiştir. Öyle ki günümüzde her ülkenin kendisine ait Siber Güvenlik Strateji Belgesi bulunmaktadır. Siber alanın hız, zaman, geçirgenlik, çoklu katılım, anonimlik, hesap verilebilirlik, ara bağlantısallık gibi çeşitli özelliklerinin sağladığı avantajlar ve dezavantajlar dikkate alındığında ise Geleneksel ve Çağdaş Uluslararası İlişkilere dair güç politikaları, teorik yaklaşımlar ve güvenlik uygulamaları gibi temel unsurların sorgulandığı ve yeniden şekillendirildiği görülmüştür. Örneğin; kara, hava, deniz ve dış uzay sahalarına kıyasla siber alanda belirleyici ve caydırıcı olabilmenin daha hızlı ve kolay olabilmesinin özünde diğer stratejik alanlardaki sınırlayıcı ve engelleyici faktörlerin siber alanda yeterince bulunmaması ve söz konusu alanın herkese açık olması gibi etkenlerin bulunduğu ve dolayısıyla da siber alana tam anlamıyla hakim olma olasılığının oldukça düşük kaldığı tespit edilmiştir.

Belirsizliklerle dolu bu yeni siber uluslararası etkileşim sahası, bir yandan mevcut Uluslararası İlişkiler sözlüğünü siber alana uyarlarken, diğer taraftan ise yepyeni kavramlar ve olgular türetmektedir. Şüphesiz bu yeni kavram ve olguların başında İnternet gelmektedir. 20. yüzyılın ikinci yarısında, olası bir nükleer saldırı durumunda iletişimi devam ettirebilecek teknoloji arayışı temeline dayanan İnternet, 21. yüzyılın başına gelindiğinde dünya üzerindeki tüm bilgisayar ve ağları birbirine bağlayan ve hizmet çeşitliliği sunan ağların ağı haline gelmiştir. Günümüzde dünyanın nüfusunun yarıdan fazlasının doğrudan İnternet bağlantısı bulunmakla birlikte bu oran her geçen gün hızla artmakta ve sosyo-kültürel bir olgu olarak İnternetin belirleyiciliği ve etki sahası giderek derinleşmektedir. Bu durum, siber tehditlerin ve siber saldırıların artmasına vesile olmaktadır. Siber tehditler; suç çetelerinden teröristlere, bilgisayar korsanlarından hasmane devletlere kadar siber alandaki kötü niyetli aktörlerin oluşturdukları eylem algıları olarak tanımlanmaktadır. Siber saldırılar, siber saha içerisinde meydana gelen her türlü zararlı faaliyetin genel adıdır. Daha önce de belirtildiği üzere güç şebekeleri ve endüstriyel sistemler gibi kritik altyapılar, siber saldırılarda birincil hedefleri oluşturmaktadır. Öte yandan siber saldırılarda hedef sistemlerin ya da ağların kullanılamaz ya da daha az yararlı hale getirilmesi gibi yıkıcı amaçlar söz konusuyken, siber casusluk faaliyetlerinde genellikle gizli bilgilere dikkat çekmeyecek küçük müdahaleler üzerinde ulaşmak ve tahribat yaratmamak durumu söz konusudur. Siber alandaki unsurlar aracılığıyla gerçekleştirilen her türlü yasadışı faaliyet ise siber suç kapsamındadır. Siber terörizm ise siber suç faaliyetlerinden motivasyon ve eylem şekilleri açısından ayrılmaktadır. Spesifik -sosyal, politik, dini- bir gündemle ve ekonomik amaçlar doğrultusunda ulusal güvenlik ve kamu güvenliğine yönelik zarar verilmesi ya da hizmetlerin sonlandırılması faaliyetlerine siber terörizm adı verilmektedir. İnternetin düşük maliyetle dünya çapında etkileşim sağlayabilmesi, büyük hasarlar yaratabilme potansiyeli, anonimliği, psikolojik etkisi ve medya cazibesi de dikkate alındığında teröristler açısından siber alan son derece cezbedici bulunmaktadır. Son olarak siber savaşa bakıldığında ise askeri uzmanların kinetik etki vurgusunun öne çıktığı tespit edilmiştir. Buna göre siber alanda devlet sponsorluğunda gerçekleştiği tespit edilen ve fiziksel dünyaya doğrudan, dolaylı ve sonuçsal etkiler yaratan eylemler siber savaş kapsamında değerlendirilmektedir.

Herhangi bir siber saldırının siber savaşın bir parçası olup olmadığının tespit edilebilmesi adına örgütsel kaynağı, coğrafi kökeni, sonuçları ve karmaşıklık düzeyinin incelenmesi gerekmektedir. Siber savaşlar, bilgisayar ağlarının sağladığı faydalara ya da kötüye kullanımın caydırılmasına bakılmaksızın devletler arasında ve devletler ile güçlü devlet-dışı siber aktörler arasında devam etmektedir. Karmaşık siber sistemlere bağımlılığın hızla artması, özellikle devletlerin güvenliğe dair endişelerinin de artmasına neden olmaktadır.

9/11 Terör Saldırıları sırasında ve sonrasında teknolojinin artık devlet-dışı aktörlerin yıkıcı amaçlarına hizmet edebilir hale geldiği ve mesafelerin etkisinin ortadan kalktığı en acı şekilde tecrübe edilmiştir. Ayrıca İnternetin önemli bir yaşam biçimi haline geldiği ve vatandaşların, şirketlerin, hükümetlerin dijital altyapılara olan bağlılığının daha da yoğunlaştığı görülmüştür. Böyle bir ortamda siber güvenlik, tüm siber alan paydaşları açısından birincil mesele haline gelmiştir. Bu bağlamda da siber güvenlik; siber ortamdaki her türlü varlığın -bilgi işlem aygıtları, personeller, altyapılar, veriler, hizmetler, sistemler- korunabilmesi adına kullanılabilecek araçların, politikaların, yaklaşımların, eylemlerin, eğitimlerin ve uygulamaların tamamı olarak tanımlanmaktadır. Başta teknik, idari, politik ve yasal olmak üzere tüm önlem çeşitleri, siber güvenlik kapsamında ele alınmaktadır. Ek olarak siber güvenlik, kişi, kurum ya da devlet bilgilerinin ve sistem altyapılarının korunmasından daha fazlasıyla ilgili olup siber uzay sahasında kaynak kullanan tüm aktörlerin ve topluma ait olan tüm varlıkların korunmasını da içermektedir. Devletlerin kendi kritik altyapıları üzerinde daha güçlü kontrol alanları yaratarak kendi güvenlik seviyelerini yükseltmeleri ve daha güçlü siber yetenekler yaratmaları olağan bir durum olarak görülmekle birlikte kimi durumlarda söz konusu siber yeteneklerin düşman unsurlara karşı güvenliği sağlamak yerine sivillere yönelik casusluk ve gözetleme faaliyetlerinde kullanabildiği de görülmektedir. Bilgi ve iletişim teknolojilerine artan bağımlılık halinin siber tehdit ve siber saldırı yelpazesini çeşitlendirmesi ve potansiyeli arttırması hesaba katıldığında ise politika yapıcıların sürekli yenilenen siber tehditler ve siber saldırılar karşısında doğru aksiyonları zamanında alabilmesi konusunda sıkıntı yaşamalarına neden olabilmektedir. Bu nedenle Siber Uluslararası İlişkilerde küresel siber güvenlik anlayışının ve işbirliğinin verimli bir şekilde geliştirilmesi elzem görünmektedir.

Siber Uluslararası İlişkiler, 20. yüzyılın sonundan günümüze değin siber uzay sahasında yaşanan büyümeyle birlikte geleneksel uluslararası sistemde meydana yenilikleri, değişimleri ve dönüşümleri belirtmektedir. Devletler hala baskın aktör konumunda olmalarına rağmen siber uzay alanında devlet-dışı aktörlerin baskılarına ve sınırlandırmalarına maruz kalmaktadırlar. Siber Uluslararası İlişkiler ortamının belirsizliği, alanın yeniliğinden ziyade anonim, karmaşık ve hassas yapısına atfedilmektedir. Yeni uluslararası etkileşim sahası olarak siber uzaydaki özel sektör baskınlığı, devlet aktörleri tarafından tam anlamıyla kontrol edilemez olması, artan siber tehditlerin ve siber saldırıların siber uzayı siyallaştırması, yeni tür simetriler ve asimetriler oluşturması, yeni aktörlerin geleneksel uluslararası karar verici mekanizmaları etkileme gücü gibi çeşitli tespitler göstermektedir ki siber uzay, artık küresel çıkar rekabetlerinin yaşandığı karmaşık bir güç rekabet sahasıdır. Bu bağlamda, siber alandaki imkanlar doğrultusunda gerçekleştirilen eylemlerle kimlerin, neyi, ne zaman ve ne şekilde elde ettiklerini belirleyen etkileşimlerin birleşimi anlamına gelen siberpolitik, dünya çapında yeni çıkarlarla beraber yeni Uluslararası İlişkiler kalıplarının oluşturulmasına ve yepyeni küresel tepki biçimlerinin ortaya çıkmasına vesile olmaktadır. Öyle ki; siber alana yönelik ulusal çıkarların güvence altına alınabilmesi adına diplomatik kaynakların ve işlevlerin bu doğrultuda kullanılması söz konusu olmakta ve dijital diplomasi oluşturulmaktadır. Buna karşın, dijital teknolojinin uluslararası sistemdeki güç dengesini hiyerarşik devlet tabanlı yapılardan merkezi olmayan ağlara kaydırdığı gerçeği göz önünde bulundurulduğunda, diplomasinin dijital alanda var oluşsal sıkıntılarla karşılaşabileceği düşünülmektedir; çünkü dijital teknolojiler, bir taraftan sistem içerisindeki aktörlerin daha güçlü hale gelmesine katkı sağlarken, diğer taraftan ise yeni tehdit türevleri oluşturarak mevcut yapıyı daha kırılgan hale getirebilmektedir. Dolayısıyla günümüz Uluslararası İlişkilerinde olmazsa olmaz bir dış politika şartı haline gelen dijital diplomasi, rasyonel ve efektif kullanılması halinde devletlerin dış politika hedeflerini ilerletebilmelerine önemli katkılar sağlayabilecek bir tamamlayıcı pozisyonundadır. Diğer taraftan ise siber alan içerisindeki aktörlerin sahip oldukları siber bilgi ve beceriyle doğru orantılı olarak farklı siber güç formlarına eş zamanlı ve çoklu olarak sahip olabilmelerinden bahsedilebilmektedir. Fakat hangi kategorizasyon ve modellemeye tabi olursa olsun siber güç, siber alanın dinamik,

değişken, belirsiz ve karmaşık doğası sayesinde en üst düzeyde ve çok yönlü olarak gerçekleşebilmektedir.

Siber alanda hukukun ve işbirliğinin uygulanabilirliği ele alındığında, diğer stratejik alanlara kıyasla tamamen yapay ve teknolojik dinamizmi yüksek bir saha olmasından kaynaklı, her türlü düzenleme ve girişimin sürekli bir yetersizlik hali içerisinde olduğu gözlenmiştir. Uluslararası hukuk açısından siber uzaya yaklaşıldığında söz konusu alanın uluslararası hukukta nasıl temsil edildiğine dair anlayışlardan etkilendiği görülmektedir. Bu bağlamda bir taraftan devletlerin klasik egemenlik alanlarının ötesinde ve insan faaliyetlerinin diğer alanlarıyla benzer düzenlemeler içermeyen yeni bir boyut olarak kabul edenler bulunmakta, diğer taraftan ise siber uzayın yapay ve gidilemez bir alan olmasından kaynaklı onu beşinci alan olarak kabul etmeyen ve mevcut uluslararası hukuk ilkelerinin uygulanabileceğini iddia eden görüşler bulunmaktadır. Yapay nitelikte olan siber uzayın operasyonel boyutları ve fiziksel dünyaya yansımaları dikkate alındığında küresel bir müşterek olarak siber ortam faaliyetlerin uluslararası hukuk ilkeleri ve normları doğrultusunda düzenlenmesinin en mantıklı yol olduğu devlet aktörlerince uygun görülmüştür ancak bu doğrultudaki girişimlerin ne kadar başarılı olduğu tartışmalıdır. Siber suçlara yönelik bağlayıcı uluslararası hukuk anlaşmalarına bakıldığında, Budapeşte Sözleşmesi olarak da bilinen Avrupa Konseyi Siber Suçlar Sözleşmesi, uluslararası düzeyde soruşturma prosedürlerinin standartlaştırılması, devletler arasında siber suçlara yönelik yasaların daha uyumlu ve tutarlı getirilmesi gibi sağladığı net faydalar sebebiyle en başarılı uluslararası hukuk düzenlemesi olarak kabul edilmektedir. Siber savaşlara yönelik bağlayıcı bir uluslararası hukuk düzenlemesi olmamakla beraber Siber Savaşa Uygulanacak Uluslararası Hukuk Hakkında Tallinn El Kitabı'nın en fazla öne çıkan yönlendirici kaynak olduğu görülmektedir. Siber alana yönelik uluslararası hukuk düzenleme girişimlerine nazaran uluslararası işbirliği girişimlerinin daha fazla gerçekleştirildiği tespit edilmiştir. Siber alan içi etkileşimlerin, mücadelelerin, tehditlerin ve niyetlerin belirsizliğinden ve karmaşıklığından kaynaklanan endişe hali, güçlü siber aktörleri siber alanda küresel düzeyde işbirliğine mecbur kılmaktadır. Siber alanda güven ortamının ve işleyişin sağlanabilmesi adına norm ve standartların uluslararası çok paydaşlı kurumlar tarafından inşa edilme çabasında olduğu görülmüştür. Bu

bağlamda siber uzaya yönelik bölgesel ve küresel nitelikte çok sayıda işbirliği girişimi yapılmakla beraber ITU, ICANN ve IGF'nin en fazla öne çıkan organizasyonlar olduğu tespit edilmiştir. Siber uzayın temel ilke, kural, protokol, standart ve uygulamalarının oluşturulması girişiminde bulunan bu tür organizasyonların temel hedeflerini; siber ortamda güven inşası, özgürlüğün güvence altına alınması, işbirliklerinin verimli hale getirilmesi ve siber uzayın karmaşık ve dinamik yapısı içerisinde meydana gelebilecek her türlü sorunun saptanan yönetişim ilkeleri doğrultusunda çözümü olduğu belirtilmektedir.

Diğer taraftan siber ortamdaki operasyonların karakterize edilebilmesi her geçen gün zorlaşmaktadır. Bunun nedeni olarak ise siber uzay sahasının belirsiz ve karmaşık yapısı, öngörülemez olayların yaşanabilme olasılığının oldukça yüksek olması, saliseler içerisinde çoklu kaynaktan çoklu aktörler tarafından çoklu eylemlerin gerçekleştirilebilmesi ve aktörel fazlalık gibi çeşitli gerekçeler gösterilmektedir. Başta devletler olmak üzere çok uluslu şirketler, kurumlar, organizasyonlar, kar amacı gütmeyen kuruluşlar, amatör oluşumlar, bireyler ve hatta yapay zekâ vb. teknoloji türevlerine sahip sistemler, araçlar ve enstrümanlar gibi pek çok aktörün, sürekli genişlemekte ve değişmekte olan siber uzay sahasında ne gibi zorluklarla karşılaşacağı ve onlarla nasıl mücadele edeceğini, sahip oldukları siber yeteneklere ne ölçüde yatırım yaptıkları ve geliştirdikleri gerçeği belirleyecektir. Siber uzaydaki operasyonlar ele alındığında, potansiyel siber operasyonların neredeyse tespit edilemez seviyelerde olduğu görülürken, siber operasyonların saldırganlığı ve yıkıcılığı arttıkça fark edilebilirliğinin de yükseldiği gözlemlenmiştir. Dünya nüfusunun İnternete ve teknolojik araçlara erişebilirliğinin son hızla arttığı gerçeği akıllara getirildiğinde ise siber uzay operasyonları spektrumu üzerinde yer alan operasyon sayısının muazzam boyutlarda olduğu düşünülmektedir. Öyle ki siber alandaki güvenlik açıkları salt büyük ve güçlü aktörlerin işleyişlerine zarar getirmekle kalmamakta, aynı zamanda bireylerin gündelik yaşamlarına da doğrudan ulaşabilmekte ve işlerini sekteye uğratabilmektedir. Dolayısıyla siber ortamın artan aktör çeşitliliği, yeni güvenlik açıklarını oluşturmakta, oluşan güvenlik açıkları ise siber ortamdaki güvensizlik ve tehdit algılarını arttırmakta ve nihayetinde de güçlü siber aktörlerin kendilerini savunabilmeleri adına daha saldırgan siber yeteneklere yönelmelerine vesile olmaktadır.

Siber alandaki her türlü elektronik varlığa veya sisteme yönelik zarar verme veya müdahalede bulunma amacıyla çok sayıda ve değişik özelliklerde kötü amaçlı yazılımlar tasarlanmıştır. Bu tarz yazılımlar, siber alanın en tehlikeli silahları olarak tanımlanmakta ve siber aktörlere büyük zararlar verebilmektedirler. Öyle ki; 21. yüzyılda oldukça iyi organize olmuş ve devasa bir pazar haline gelen kötü amaçlı yazılım endüstrisi bulunmakta ve her geçen yıl çok daha büyük yatırımlar almaktadır. Kötü amaçlı yazılımların davranış biçimleri, nasıl tetiklendikleri ve yayıldıkları, nasıl tespit edilebildikleri veya gizlendikleri gibi karakteristiklerine bağlı olarak çok sayıda çeşitli formları bulunmaktadır. Örneğin virüsler, kendi kodlarını yürütebilmek için makro unsurları destekleyen programlara ihtiyaç duyarlar ve hedeflenen bilgisayar sisteminin operatörünün bilgisi olmaksızın kendilerini çoğaltarak yayılabilmektedirler. Diğer taraftan bilgisayar solucanları, bir bilgisayardan kaynaklanan ve yerel ağ ya da İnternet üzerinden diğer bilgisayarlara süresiz veya bir zamanlama mekanizmasına tabi olarak bulaşabilir ve çoğalabilirler. Virüslerden farklı olarak bağımsız yazılımlardır ve yayılabilmek için sunucu program ya da operatöre ihtiyaç duymazlar. Ağ kitlenmeleri, web kaynağı erişim hızının düşmesi veya e-posta sunucularına aşırı yüklenmeler gibi sorunlar yaratabilirler. Öte yandan truva atlarına bakıldığında, verilere ya da ağlara zarar vermek, bozmak, çalmak, kontrolü ele geçirmek gibi çeşitli kötü niyetli amaçlarla tasarlanmış yazılımlar oldukları görülmektedir. Virüslerin ve bilgisayar solucanlarının aksine truva atları kendi kendilerini çoğaltamamakta, bilgisayar kullanıcılarının farklı yöntemlerde ikna edilmesi üzerine sisteme yüklenerek etkinleştirilebilmektedirler. Çok zor tanımlanabilen truva atları, siber suçlular tarafından hedef bilgisayar ya da ağdaki hassas bilgilerin gözlenmesi, ele geçirilmesi, kopyalanabilmesi ve bozulabilmesi gibi eylemlerde kullanılabilirler. Bir diğer dikkat çeken kötü amaçlı yazılım formu ise İnternet robotu anlamına gelen botlardır. Bilgisayar çalıştırıldığında botların bilgisayar kaynaklarına erişimi, tıpkı bilgisayar operatörününki gibi olmakta ve e-postalardan kamera uygulamalarına, sistem dosyalarından belgelere kadar her türlü eylemi gerçekleştirebilirler. Birden fazla bilgisayara yayılan botların birbirine bağlanmasıyla da botnet adı verilen bot ağları oluşturulabilmekte ve eş zamanlı olarak güç şebekelerini, hava trafik kontrol sistemlerini, endüstriyel tesisleri veya iletişim ağlarını doğrudan hedef alarak büyük

zararlar verebilmektedirler. Son olarak casus yazılımlara bakıldığında ise kullanıcıların şifreleri, parolaları, kredi kartı bilgileri, telefon rehberleri, ziyaret ettikleri çevrimiçi sayfaların listesi vb. kişisel ve gizli bilgilerin, kullanıcıların haberi olmaksızın ele geçirme amacıyla tasarlandıkları görülmektedir. Diğer kötü amaçlı yazılımlar genellikle işletim sistemlerine veya fonksiyonel süreçlere zararlar verirken, casus yazılımlar kullanıcıların kariyerlerine ve ekonomik durumlarına büyük hasarlar yaratabilmektedir.

Siber olay süreçlerinin daha iyi anlaşılabilmesi adına çeşitli sınıflandırmalar yapıldığı ancak siber gelişmelerin birçok değişkene dayanan dinamik altyapılarından dolayı ideal bir sınıflandırma üzerinde fikir birliğine varılamadığı gözlenmiştir. Geliştirilen çeşitli pratik kategoriler içerisinde amaca dayalı siber saldırı sınıflandırması en fazla öne çıktığından, bu çalışmada söz konusu kategorizasyon tercih edilmiştir. Siber olayların ve saldırıların doğru şekilde tanımlanabilmesi ve değerlendirilebilmesi, risklerin ve tehditlerin azaltılabilmesi adına doğru kararların alınabilmesi açısından son derece önem arz etmektedir. Bu bağlamda amaçsal olarak üç farklı şekilde siber olayların sınıflandırılması mümkündür: Hedeflenen cihazların ya da ağların en zayıf olduğu ve hatta savunmasız kaldığı noktaların belirlenmesi amacıyla gerçekleştirilen "keşif saldırıları"; bilgisayar kaynaklarına yetkisiz erişimin her türlü biçimini kapsayan "erişim saldırıları"; ve siber suçlular ya da saldırganlar tarafından bilgi sistemlerine, cihazlara veya diğer ağ kaynaklarına erişim engeli getiren ve "DoS saldırıları" olarak da bilinen "hizmet engelleme saldırıları". Böylelikle planlanan amaçlar ve hazırlanan süreçler doğrultusunda öncelikle hedef unsurun savunmasız noktaları tespit edilmiş, sonrasında erişim bilgileri ele geçirilmiş ve nihayetinde de erişime çeşitli şekillerde engeller getirilmiş olmaktadır. Diğer yandan, DoS saldırılarında bir hedefe yönelik bir kaynaktan saldırı gerçekleştirilirken, "DDoS saldırıları" olarak da bilinen "dağıtılmış hizmet engelleme saldırıları"nda ise bir hedefe yönelik birden fazla farklı kaynaktan saldırı gerçekleştirilmektedir. DDoS saldırılarında ana kaynak tespitinin daha zor olması ve başarı oranının DoS saldırılarına kıyasla daha yüksek olması sebebiyle de daha fazla tercih edilmektedirler. Bu saldırılar neticesinde sistemin ağ trafiği kitlenerek hizmet vermesi engellenebilmekte ve hizmet akışında ciddi aksamalar yaşanabilmektedir.

Günümüze dek yaşanan ve bir şekilde kayıtlara geçen siber olayların tarihine bakıldığında ise olayların tarihsel olarak fazlara ayrılmasının mümkün olduğu tespit edilmiştir. Geçmişte yaşanan her türlü siber saldırı eyleminin, gelecekteki muhtemel siber zorlukların somutlaştırılması ve muhtemel yeni güvenlik açıklarının tespit edilmesine yönelik uyarı niteliği taşıdığı düşünülmektedir. Bu nedenle yaşanan her türlü siber olay, siber uzay sahasının kurumsal evrimi açısından katalizör etkisinde bulunmaktadır ve siber alanın yeni boyutlarının keşfedilmesine olanak sağlamaktadır. Bir diğer husus ise yaşanan her siber olayın etki ölçeği fark etmeksizin teknoloji bağımlılığını arttırıcı etkide bulunmasıdır. Ortaya çıkan güvenlik zafiyetleri ve muhtemel etkileri bağlamında alınacak her türlü önlem, teknolojik yetkinliğin daha da yoğunlaştırılmasını gerekli kılmakta ve dolayısıyla da teknolojik bağımlılığı derinleştirmektedir. Bu argümanın doğruluğu ise siber olaylar tarihinin aşamalarının tespitinde test edilmiştir. Buna göre 1980-1998 arasındaki İnternetin erken dönem olaylarını kapsayan süreç "gerçekleşme aşaması" olarak tanımlanmıştır. Bu dönemde birbirine bağlanan bilgisayar ağlarının açıklarının oluşturduğu potansiyel tehlikeler ortaya çıkmaya başlamış ve siber alanın altyapısındaki savunmasızlık halinin farkına varılmıştır. 1998-2003 arasındaki dönemde ise siber yeteneklere sahip aktör sayısında ve dolayısıyla kayıtlara geçen siber saldırı sayısında önemli bir artış yaşandığı için bu sürece "yükseliş aşaması" adı verilmiştir. Gerçekleşme aşamasındaki olaylara yönelik oluşturulan devlet politikaları ve doktrinlerindeki istihbarat savaşı anlayışının aksine yükseliş döneminde operasyonel tutumlar ve önlemler ağır basmıştır. 2003'ten günümüze kadar uzan sürece ise "militarizasyon aşaması" denilmiş ve siber alandaki devlet aktörlerinin gücü, çeşitliliği ve rekabet boyutları siber savaş seviyelerine ulaşmıştır. Bu dönemde siber alan, kötü amaçlı yazılımların ve saldırgan yeteneklerin artışıyla beraber fiziksel alanda yıkıcı etkiler yaratabilecek pek çok olayı tecrübe etmiştir. Devletlerin bu süreç içerisinde bir taraftan siber güvenlik strateji belgeleri yayınlamaya başladıkları görülürken, diğer taraftan da siber alanda gerek devletler arası gerekse de devlet-özel sektör işbirlikleri geliştirilmiştir. Asimetrik tehditlerin giderek artması ve öngörülemez siber olayların daha sık yaşanır hale gelmesi, tabiatıyla siber ortamın daha güvensiz olarak algılanmasına neden olmuştur. Daha da

önemlisi ise siber alandaki anlaşmazlıkların ya da çatışmaların etki boyutları siber alan sınırlarını aşarak fiziksel alanlara kadar uzanmıştır.

21. yüzyılda gerçekleşen çok sayıdaki Siber Uluslararası İlişkiler olaylarından nitelik ve etki bakımından en fazla öne çıkanlar şu şekilde tespit edilmiştir: Titan Rain Operasyonu (2003), Estonya Saldırıları (2007), Gürcistan Saldırıları (2008), Stuxnet Saldırısı (2010), WikiLeaks (2010), Snowden (2013) ve Ukrayna Saldırıları (2017). Titan Rain Operasyonu, ABD ile ÇHC'nin siber alandaki saldırgan rekabetinin başlangıcının kayıtlar geçmesi şeklinde yorumlanabilmektedir. Buna göre ÇHC tarafından ABD Hükümeti ve askeri sistemlerinde yer alan gizli bilgilere yönelik çok sayıda siber casusluk erişim saldırıları gerçekleştirilmiştir. Ek olarak bu saldırılar ABD ile sınırlı kalmamış ve Avrupa'nın çeşitli ülkelerinde de Çin kaynaklı siber saldırılar tespit edilmiştir. ABD hedefli Çin siber operasyonları halen devam etmekte olup söz konusu iki büyük siber gücün arasındaki siber rekabetin boyutları ve kapsamı giderek derinleşmektedir. Estonya, Gürcistan ve Ukrayna Saldırılarına bakıldığında ise Rusya Federasyonu'nun anonim devlet sponsorluğunda çeşitli formlarda ve büyük etkilere sahip saldırılar gerçekleştirdiği görülmüştür. Avrupa'nın teknolojik bağımlılığı en yüksek ülkelerinden olan Estonya, teknolojiye olan bağımlılığının neticesi olan güvenlik açıklarının etki boyutunu çok sert şekilde tecrübe etmiştir. RF kaynaklı yoğun DDoS saldırıları neticesinde bankacılık hizmetleri sekteye uğramış ve bunun ülkeye yansıması 1 Milyon Dolardan fazla olmuştur. Ayrıca Estonya Saldırıları, bir ulus-devletin kararlarının başka bir devletin anonim sponsorluğunda siber silahlar kullanılarak etkilenmeye çalışıldığı ilk siber savaş örneği olarak kayıtlara geçmiştir. Gürcistan Saldırıları ise Güney Osetya Savaşı esnasında Gürcistan İnternet ağının büyük bir kısmını kullanılamaz hale getirmiştir. Bu bağlamda ilk defa bir ulus-devlet, uluslararası bir siyasi ve askeri çatışmayla eşgüdümlü olarak siber saldırılara maruz kalmıştır. Ukrayna Saldırıları ise Kırım'ın ilhak edilmesi sürecinde ve sonrasında binlerce siber saldırının elektrik şebekelerine gerçekleştirilmesi neticesinde yaşanan elektrik kesintileriyle meşhurdur. Ayrıca *WannaCry, Petya* ve *NotPetya* isimli kötü amaçlı yazılımların Ukrayna merkezli olarak dünya çapında milyarlarca dolar hasar yaratarak, tarihin en pahalı siber saldırıları şeklinde kayıtlara geçtiği tespit edilmiştir. Stuxnet Saldırısı ise ABD-İsrail ortaklığında İran'daki nükleer tesise yönelik gerçekleştirilen son derece yıkıcı

potansiyele sahip bir operasyondur. Bu saldırıyla birlikte saldırgan bir siber yeteneğin, uzak bir sistemi uluslararası sınırlarda fiziksel hasara neden olabilecek şekilde hedefleyebileceği görülmüş ve siber savaş tartışmalarında bir dönüm noktası olarak kayıtlara geçmiştir. WikiLeaks ve Snowden sızıntıları ise siber operasyonların Uluslararası İlişkilerdeki etki boyutunun çok farklı seviyelere ulaştığının kanıtı olarak yorumlanmaktadır. WikiLeaks tarafından içerisinde Irak ve Afganistan savaş kayıtlarının olduğu çok gizli belgelerle birlikte ABD elçiliklerinin gizli yazışmaları ve ABD Hükümetine ait çeşitli yolsuzlukların belgeleri kamuoyuna servis edilmiştir. Edward Snowden ise tüm zamanların en büyük vatandaşlık hakları ihlali olarak tanımlanan ve İnternet kullanıcıların tüm bilgilerinin kayıt altına alındığı ve izlendiği projeleri kamuoyuna ifşa etmiştir. Söz konusu sızıntılar sadece maddi ve siyasi hasarlar yaratmakla kalmamış, teknoloji bağımlılığının ve yetersiz güvenlik önlemlerinin etkilerinin ne boyutlara ulaşabileceğini gözler önüne sermiş, Siber Uluslararası İlişkilerin karmaşık yapısının derinliğini ortaya koymuş ve devlet aktörlerini şeffaflık, hesap verilebilirlik ve gizlilik üzerinden yoğun kamuoyu eleştirilerine maruz bırakmıştır.

Tüm bu anlatılanlar doğrultusunda çalışmanın hipotezi -“Soğuk Savaş dönemi Uluslararası İlişkilerinde ortaya çıkan uzay çalışmaları rekabeti ve geliştirilen yeni teknolojiler, 21. yüzyıl Uluslararası İlişkiler bilgisinde ‘teknolojik dönüşüm’ yaratarak siber uzayı Uluslararası İlişkilerin karmaşık çerçevesi içerisinde yeni güç rekabet sahalarından biri haline getirmiştir.”- saptanan sorular bağlamında test edilmiş ve elde edilen veriler ışığında doğrulanmıştır. Siber uzay sahası, 21. yüzyılın Beşinci Stratejik Alanı olmakla birlikte Uluslararası İlişkiler aktörlerinin güç mücadelelerini yansıttığı ve yaşadığı rekabet sahası haline gelmiştir. Bilimsel bilgi ve teknolojik ilerlemelerin neticesi olarak teknoloji bağımlılığının daha da derinleşeceği öngörülmektedir. Dolayısıyla ortaya çıkacak yepyeni güvenlik açıklarına bağlı olarak, aktörel çeşitlilik de hesaba katıldığında artan güvensizlik ve tehdit algılarının saldırgan siber yetenekler geliştirilerek kapatılmaya çalışılması olası görülmektedir. Ekonomi, sağlık, eğitim, üretim gibi alanlar başta olmak üzere fiziksel dünyanın tüm boyutları siber ortama entegre olmaya devam etmektedir. Artan saldırgan siber yetenekler ve artan siber-fiziksel bağımlılık göz önünde bulundurulduğunda, gelecek bugünden daha da karmaşık olacaktır.

KAYNAKÇA

Kitaplar / Raporlar:

ACEMOĞLU, Daron & James A. ROBINSON, *Ulusların Düşüşü: Güç, Zenginlik ve Yoksulluğun Kökenleri*, Çeviren: Faruk Rasim Velioğlu, 45. Basım, Doğan Kitap, İstanbul 2019.

AMAYA, Daniel Gómez, *The Theory of Complexity Adapted To International Relations: The Behaviour Of The Visegrad-Ukraine Complex Adaptive System Since November 2013*, (Universidad del Rosario, School of International Relations, Basılmamış Doktora Tezi), Bogotá 2016.

ANDERSON, Benedict, *Hayali Cemaatler: Milliyetçiliğin Kökenleri ve Yayılması*, Çeviren: İskender Savaşır, 1. Basım, Metis Yayınları, İstanbul 1993.

ANDERSON, Bella, *Cybercrime: Criminal Threats from Cyberspace*, White Press Academic, Los Angeles 2018.

ANDERSON, Chris, *Makers: The New Industrial Revolution*, Crown Business, New York 2012.

ARMAOĞLU, Fahir H., *Siyasi Tarih (1789-1960)*, Sevinç Matbaası, Ankara 1964.

BAEZNER, Marie, *Cyber and Information Warfare In The Ukrainian Conflict*, Center for Security Studies (CSS) Cyber Defense Project Report, Zürih, Ekim 2018.

BAK, Per, *How Nature Works: The Science of Self-Organized Criticality*, 1. Basım, Springer-Verlag, New York 1996.

BAYUK, Jennifer L., Jason HEALEY, Paul ROHMEYER, Marcus H. SACHS, Jeffrey SCHMIDT & Joseph WEISS, *Cyber Security Policy Guidebook*, 1. Basım, John Wiley & Sons, Inc., New Jersey 2012.

BEEHNER, Lionel, Liam COLLINS, Steve FERENZI, Robert PERSON & Aaron BRANTLY, *Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia*, Modern War Institute, United States Military Academy, Report, 2018.

BETZ, David J. & Tim STEVENS, *Cyberspace and The State: Toward A Strategy For Cyber-Power,* 1. Basım, Routledge, New York 2011.

BOOTH, Ken (Editör), *Critical Security Studies and World Politics*, 1. Basım, Lynne Rienner Publishers, Colorado 2005.

BOOTH, Ken, *Theory of World Security*, 1. Basım, Cambridge University Press, New York 2007.

BOUSQUET, Antoine, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, 2. Basım, Columbia University Press, New York 2009.

BROWN, Bruce C., *How To Stop E-Mail Spam, Spyware, Malware, Computer Viruses, and Hackers From Ruining Your Computer or Network: The Complete Guide For Your Home and Work*, Atlantic Publishing Group, Florida 2011.

BRUNTON, Finn, *Spam: A shadow History of the Internet*, 1. Basım, The Massachusetts Institute of Technology Press, Massachusetts 2013.

BUZAN, Barry & Lene HANSEN, *The Evolution of Internationsal Security Studies*, 1. Basım, Cambridge University Press, New York 2009.

CAPRA, Fritjof, *The Web of Life: A New Scientific Understanding of Living Systems*,1. Basım, Anchor Books, Doubleday, New York 1996.

CAPRA, Fritjof, *The Hidden Connections: Integrating The Biological, Cognitive, and Social Dimensions of Life Into A Science of Sustainability*, 1. Basım, Doubleday, New York 2002.

CAREY, James W., *Communication as Culture: Essays on Media and Society*, Revised Edition, Routledge, New York 2008.

CARR, Edward Hallet, *The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations*, Macmillan & Co Ltd, Londra 1946.

CARR, Jeffrey, *Inside Cyber Warfare*, O'Reilly Media, Inc., California 2010.

CASTELLS, Manuel, *The Information Age: The Rise of Network Society (Volume 1)*, 2. Basım, Blackwell Publishers, Oxford 1996.

CASTELLS, Manuel, *The Rise of the Network Society*, 2. Baskı, Wiley-Blackwell, Singapur 2010.

CAVELTY DUNN, Myriam, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, 1. Basım, Routledge, New York 2008.

CHAPPLE, Mike & David SEIDL, *Cyberwarfare: Information Operations in a Connected World*, Jones & Barlett Learning, Massachusetts 2015.

CHOUCRI, Nazli, *Cyberpolitics in International Relations*, The Massachusetts Institute of Technology Press, Massachusetts 2012.

CHOUCRI, Nazli & David D. CLARK, *International Relations in the Cyber Age: The Co-Evolution Dilemma*, The Massachusetts Institute of Technology Press, Massachusetts 2018.

CLEMENS JR., Walter C., *Complexity Science and World Affairs*, 1. Basım, State University of New York Press, New York 2013.

COE, Lewis, *The Telephone and Its Several Inventors: A History*, 1. Basım, McFarland & Company, Inc., Publishers, North Carolina 1995.

COE, Lewis, *Wireless Radio: A History*, 2. Basım, McFarland & Company, Inc., Publishers, North Carolina Şubat 2006.

CORDESMAN, Anthony H. & Adam C. SEITZ, *Iranian Weapons of Mass Destruction, Iran's Nuclear Weapons Programs: Work In Progress?*, Center For Strategic & International Studies (CSIS), Working Draft for Review and Comments, Burke Chair in Strategy, 6 Kasım 2008.

CORNISH, Paul, David LIVINGSTONE, Dave CLEMENTE & Claire YORKE, *On Cyber Warfare: A Chatham House Report*, The Royal Institute of International Affairs, Londra Kasım 2010.

DENARDIS, Laura, *The Global War for Internet Governance*, Yale University Press, New Haven & London 2014.

DINNISS, Heather Harrison, *Cyber Warfare and the Laws of War*, 1. Basım, Cambridge University Press, Cambridge 2012.

DIZARD, Wilson, Jr., *Digital Diplomacy: U.S. Foreign Policy in the Information Age*, 1. Basım, Praeger Publishers, Connecticut 2001.

DUNHAM, Ken & Jim MELNICK, *Malicious Bots: An Inside Look Into The Cyber-Criminal Underground of The Internet*, CRC Press, Auerbach Publications, Florida 2009.

EATHER, Robert H., *Majestic Lights: The Aurora in Science, History, and the Arts*, American Geophysical Union, Washington D.C. 1980.

EDWARDS, Lee, *Mediapolitik: How the Mass Media Have Transformed World Politics*, 1. Basım, The Catholic University of America Press, Washington, D.C. 2001.

EISENSTEIN, Elizabeth L., *The Printing Press As An Agent Of Change: Communications and Cultural Transformations in Early-Modern Europe (Complete in One Volume)*, Cambridge University Press, New York 1980.

ERBSCHLOE, Michael, *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code*, Elsevier Butterworth–Heinemann, Massachusetts 2005.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Reference Incident Classification Taxonomy: Task Force Status and Way Forward*, Athens Office, Ocak 2018.

FISCHER, Claude S., *America Calling: A Social History of the Telephone to 1940*, University of California Press, California 1992.

FOSNOCK, Craig, *Computer Worms: Past, Present, and Future CISSP*, Technical Report 8, East Carolina University, 2005.

FRANDA, Marcus, *Governing The Internet: The Emergence of an International Regime*, 1. Basım, Lynne Rienner Publishers, Colorado 2001.

GAMERO-GARRIDO, Alexander, *Cyber Conflicts in International Relations: Framework and Case Studies*, Explorations in Cyber International Relations (ECIR) Working Paper, MIT & Harvard University, 2014.

GAZULA, Mohan B., *Cyber Warfare Conflict Analysis and Case Studies*, Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, Massachusetts Institute of Technology, Working Paper CISL# 2017-10, Massachusetts Mayıs 2017.

GELINAS, Ryan Richard, *Cyberdeterrence and The Problem of Attribution*, (Georgetown University, Faculty of the Graduate School of Arts and Sciences, Basılmamış Master Tezi), Washington, D.C. Nisan 2016.

GHERNAOUTI, Solange, *Cyber Power: Crime, Conflict and Security In Cyberspace*, EPFL Press, Lausanne 2013.

GIBSON, William, *Neuromancer*, (The Sprawl – 1), Ace Science Fiction Books, New York 1984.

GILCHRIST, Alasdair, *Industry 4.0: The Industrial Internet of Things*, Apress Media, New York 2016.

GOVERNMENT OF CANADA, *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*, Public Safety Canada, ISBN: 978-0-660-26553-7, 2018.

GREENWALD, Glenn, *No Place To Hide: Edward Snowden, the NSA and the Surveillance State*, Penguin Group, Londra 2014.

GULBENKIAN KOMİSYONU, *Sosyal Bilimleri Açın: Sosyal Bilimlerin Yeniden Yapılanması Üzerine Rapor*, Çeviren: Şirin Tekeli, 4. Basım, Metis Yayınları, İstanbul 2003.

HAMELINK, Cees J., *The Politics of Communication: A Human Rights Perspective*, SAGE Publlications, Londra 1994.

HANSON, Elizabeth C., *The Information Revolution and World Politics*, Rowman & Littlefield Publishers, Inc., Maryland 2008.

HARLEY, David, Robert Slade & Urs Gattiker, *Viruses Revealed*, McGraw-Hill/Osborne, New York 2001.

HART, Herbert Lionel Adolphus, *The Concept of Law*, 2. Basım, Oxford University Press, New York 1994.

HEADRICK, Daniel R., *The Tools of Empire: Technology and European Imperialism in the Nineteenth Century*, 1. Basım, Oxford University Press, Oxford & New York 1981.

HEALEY, Jason, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association (CCSA), Virginia 2013.

HEMSLEY, Kevin E. & Ronald E. FISHER, *History of Industrial Control System Cyber Incidents*, U.S. Department of Energy, Office of Nuclear Energy, DOE Idaho National Laboratory, Report, INL/CON-18-44411-Revision-2, Aralık 2018.

HIGGINS, Melissa, *Edward Snowden: NSA Whistle-Blower*, Abdo Publishing, Minnesota 2017.

HOBSBAWM, Eric John Ernest, *Devrim Çağı: Avrupa 1789-1848*, Çeviren: Bahadır Sina Şener, Dost Kitabevi, 3. Basım, Ankara 2003.

HOLLAND, John Henry, *Hidden Order: How Adaptation Builds Complexity*, Baci (Helix) Books, New York 1995.

HOLLIS, Martin & Steve SMITH, *Explaining and Understanding International Relations*, Oxford University Press, 1. Basım, New York 1990.

HOWARD, John D. & Thomas A. LONGSTAFF, *A Common Language for Computer Security Incidents*, Technical Report, SAND98-8667, Sandia National Laboratories, California Ekim 1998.

HUDSON, Pat, *The Industrial Revolution*, Hodder Arnold, New York 1992.

HUSSAIN, Alefiya, John HEIDEMANN & Christos PAPADOPOULOS, *A Framework for Classifying Denial of Service Attacks*, Technical Report ISI-TR-2003-569b, USC/Information Sciences Institute, Şubat 2003.

HUUDERMAN, Anton A., *The Worldwide History of Telecommunications*, Wiley-Interscience, New Jersey 2003.

INTERNATIONAL COURT OF JUSTICE, *Legality of the Threat or Use of Nuclear Weapons: Advisory Opinion of 8 July 1996*, Reports of Judgements, Advisory Opinions and Orders.

INTERNATIONAL TELECOMMUNICATION UNION, *Series X: Data Networks, Open System Communications and Security – Telecommunication Security; Overview of Cybersecurity*, ITU-T X.1205, 04/2008.

IOSIFIDIS, Petros & Mark WHEELER, *Public Spheres and Mediated Social Networks in the Western Context and Beyond*, Palgrave Macmillan, Londra 2016.

JACKSON, Robert & Georg SØRENSEN, *Introduction to International Relations: Theories and Approaches*, 5. Basım, Oxford University Press, Oxford 2013.

JERVIS, Robert, *System Effects: Complexity In Political and Social Life*, 10. Basım, Princeton University Press, New Jersey 1997.

JODOIN, Sébastien, "Terrorism as a War Crime", *International Criminal Law Review*, Cilt 7, Sayı 1, 2007, ss. 77-115.

KAPLAN, Fred, *Dark Territory: The Secret History of Cyber War*, 1. Basım, Simon & Schuster, New York 2016.

KEHL, Danielle, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*, New America's Open Technology Institute, Policy Paper, Temmuz 2014.

KELLO, Lucas, *The Virtual Weapon and International Order*, Yale University Press, New Haven & Londra 2017.

KENNEDY, Paul, *Büyük Güçlerin Yükseliş ve Çöküşleri: 16. Yüzyıldan Günümüze Ekonomik Değişim ve Askeri Çatışmalar*, Çeviren: Birtane Karanakçı, Türkiye İş Bankası Kültür Yayınları, 10. Basım, İstanbul 2005.

KIYUNA, A. & L. CONYERS, *Cyberwarfare Sourcebook*, Lulu.com, 2015.

KITTICHAISAREE Kriangsak, *Public International Law of Cyberspace*, Springer Nature, Law, Governance and Technology Series, Cilt 32, Cham 2017.

KOETSIER, Teun, *The Ascent of GIM, the Global Intelligent Mechine: A History of Production and Information Machines*, Springer, Cham 2019.

KOLODZIEJ, Edward A., "Security and International Relations", 1. Basım, *Cambridge University Press*, New York 2005.

KUHN, Thomas S., *The Structure of Scientific Revolutions: Volume II*, 2. Basım, The University of Chicago Press, Chicago 1970.

LARMOR, Joseph, *Aether and Matter: A Development of the Dynamical Relations of the Aether to Material Systems On The Basis of The Atomic Constitution of Matter*, Cambridge University Press, Cambridge 1900.

LASSWELL, Harold D., *Politics: Who Gets What, When, How*, McGraw Hill, New York 1936.

LEMCKE, Lukas, *Imperial Transportation and Communication from the Third to the Late Fourth Century: The Golden Age of the Cursus Publicus*, Collection Latomus 353, Edition Latomus, Bruxelles 2016.

LÉONET, Louis, *Contextual Cyber Securitisation: A Case Study of Russian Cyberattacks against Ukraine*, Danışman: Matthew Frear, Master Tezi, International Relations, Universiteit Leiden, Leiden, Hollanda, Temmuz 2019.

LISTER, Martin, Jon DOVEY, Seth GIDDINGS, Iain GRANT & Kieran KELLY, *New Media: A Critical Introduction*, 2. Basım, Routledge, 2009 New York.

LITTLE, William, H. W. FOWLER & J. COULSON, *The Oxford Universal Dictionary Illustrated: An Illustrated Edition of The Shorter Oxford English Dictionary*, Editör: C. T. Onions, 3. Basım, Oxford At The Clarendon Press, Londra 1965.

LORRAIN, Paul & Dale CORSON, *Electromagnetic Fields and Waves*, 2. Basım, W. H. Freeman and Company, San Fransico 1970.

LOUTH, Jonathon, *Imagining A Complex World: Science, Order and International Relations*, (Adelaide Üniversitesi, Tarih ve Politika Okulu, Basılmamış Doktora Tezi), Avusturalya, Kasım 2009.

LUBRANO, Annteresa, *The Telegraph: How Technology Innovation Caused Social Change*, 1. Basım, Routledge, New York 2012.

MATHIASON, John, *Internet Governance: The New Frontier of Global Institutions*, 1. Basım, Routledge, Oxon 2009.

MAZANEC, Brian M., *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*, University of Nebraska Press, Nebraska 2015.

MCLUHAN, Marshall & Bruce R. POWERS, *Global Köy: 21. Yüzyılda Yeryüzü Yaşamında ve Medyada Meydana Gelecek Dönüşümler*, Çeviren: Bahar Öcal Düzgören, 1. Basım, Scala Yayıncılık, İstanbul 2001.

MIDDLETON, Bruce, *A History of Cyber Security Attacks: 1980 to Present*, CRC Press, New York 2017.

MOKYR, Joel, *The Lever of Riches: Technological Creativity and Economic Progress*, 1. Basım, Oxford University Press, New York 1990.

MOKYR, Joel, *A Culture of Growth: The Origins of the Modern Economy*, Princeton University Press, New Jersey 2017.

MOLZ, Redmond Kathleen & Phyllis DAIN, *Civic Space / Cyberspace: The American Public Library in the Information Age*, The Massachusetts Institue of Technology Press, Cambridge, Massachusetts 1999.

MOWLANA, Hamid, *Global Information and World Communication: New Frontiers in International Relations*, 3. Basım, SAGE Publications, Londra 1998.

MUELLER, Milton L., *Ruling the Root: Internet Governance and the Taming of Cyberspace*, 1. Basım, Massachusetts Institute of Technology Press, Massachusetts 2004.

NEWBY, Julian, *Inside Broadcasting*, 1. Basım, Routledge, Londra 1997.

NIEMELÄ, Jarno, Mikko HYPPÖNEN & Santeri KANGAS, *Malware Protection*, U.S. Patent No. 9,501,644, 22 Kasım 2016.

NYE, Joseph S., Jr., *Cyber Power*, Harvard Kennedy School, Belfer Center for Science and International Affairs, Report, Massachusetts Mayıs 2010.

NYE, Joseph S., Jr. & David A. WELCH, *Understanding Global Conflict and Cooperation: An Introduction to Theory and History*, 10. Basım, Pearson, Boston 2017.

OECD, *OECD Factbook 2013: Economic, Environmental and Social Statistics*, OECD Publishing, Paris 2012.

ORWELL, George, *1984*, Çeviren: Celal Üster, 44. Basım, Can Sanat Yayınları, İstanbul 2014.

PAGE, Arthur W., *The Bell Telephone System*, Harper & Brothers Publishers, New York & Londra 1941.

PAZARCI, Hüseyin, *Uluslararası Hukuk*, Turhan Kitabevi Yayınları, Ankara 2003.

PITTS, Vanessa, *Cyber Crimes: History of World's Worst Cyber Attacks*, Alpha Editions, Vij Books, Darya Ganj 2017.

PUYVELDE, Damien Van & Aaron F. BRANTLY, *Cybersecurity: Politics, Governance and Conflict in Cyberspace*, 1. Basım, Polity Press, Cambridge 2019.

RIFKIN, Jeremy, *The Third Industrial Revolution: How Lateral Power is Transforming Energy, The Economy, and The World*, Palgrave Macmillian, New York 2013.

ROSCINI, Marco, *Cyber Operations and the Use of Force in International Law*, 1. Basım, Oxford University Press, Oxford 2014.

ROSECRANCE, Richard N., *The Rise of The Virtual State: Wealth and Power in the Coming Century*, 1. Basım, Basic Books, New York 1999.

ROSENZWEIG, Paul, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, ABC-CLIO, California 2013.

RUSSELL, Alison Lawlor, *Cyber Blockades*, Georgetown University Press, Washington, D. C. 2014.

SANDRE, Andreas, *Digital Diplomacy: Conversations on Innovation in Foreign Policy*, The Rowman & Littlefield Publishing, Maryland 2015.

SCHMITT, Michael N., *Tallinn Manual On The International Law Applicable To Cyber Warfare*, 1. Basım, Cambridge University Press, Cambridge 2013.

SCHMITT, Michael N., *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*, 1. Basım, Cambridge University Press, Cambridge 2017.

SCHWAB, Klaus, *The Fourth Industrial Revolution*, World Economic Forum, Cenevre 2016.

SHAKARIAN, Paulo, Jana SHAKARIAN & Andrew RUEF, *Introduction To Cyber-Warfare: A Multidisciplinary Approach*, Syngress Elsevier, Massachusetts 2013.

SKILTON, Mark & Felix HOVSEPIAN, *The 4th Industrial Revolution: Responding to the Impact of Artificial Intelligence on Business*, Palgrave Macmillan, Cham 2018.

SKOLNIKOFF, Eugene B., *The Elusive Transformation: Science, Technology, and the Evolution of International Relations*, 1. Basım, Princeton University Press, New Jersey 1993.

SMITH, John & Chris JENKS, *Qualitative Complexity: Ecology, Cognitive Processes and The Re-Emergence of Structures in Post-Humanist Social Theory*, 1. Basım, Routledge, New York 2006.

SPRENGER, Florian, *The Politics of Micro-Decisions: Edward Snowden, Net Neutrality, and the Architectures of the Internet*, Meson Press, Lüneburg 2015.

SPRINGER, Paul J., *Encyclopedia of Cyber Warfare*, ABC-CLIO, California 2017.

STEARNS, Peter N., *The Industrial Revolution in World History*, 4. Basım, Westview Press, Philadelphia 2013.

STOLL, Cliff, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, New York 1989.

TOURÉ, Hamadoun I., *Report of the Chairman of High-Level Experts Group (HLEG)*, ITU Global Cybersecurity Agenda (GCA), Mossi Norveç 2008.

TOYNBEE, Arnold Joseph, *A Study of History*, 4. Basım, Oxford University Press, New York 1947.

UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Comprehensive Study on Cybercrime*, Draft, New York Şubat 2013.

URRY, John, *Global Complexity*, 1. Basım, Polity Press, Cambridge 2003.

USHER, Oli & Lars Lindberg CHRISTENSEN, *The Universe Through the Eyes of Hubble*, Springer International Pubslihing AG, Cham 2014.

VIRILIO, Paul, *Speed and Politics*, Çeviren: Marc Polizzotti, Semiotext(e), Los Angeles 2007.

VIRILIO, Paul & Slyvere LOTRINGER, *Pure War: Twenty-Five Years Later*, Çeviren: Mark Polizzotti, Semiotext(e), Los Angeles 2007.

YAR, Majid & Kevin F. STEINMETZ, *Cyber Crime and Society*, 3. Basım, Sage Publications, Londra 2019.

WALDROP, M. Mitchell, *Complexity: The Emerging Science At The Edge Of Order And Chaos*, 1. Basım, Touchstone Book, Simon & Schuster, New York 1993.

WALLERSTEIN, Immanuel (Editör), *Open The Social Sciences: Report Of The Gulbenkian Commision On The Restructuring Of The Social Sciences*, Mestizo Spaces/Espaces Metisses, Stanford University Press, California Mart 1996.

WALTZ, Kenneth N., *Theory of International Politics*, 1. Basım, McGraw-Hill, Inc., New York 1979.

WEBB, Richard C., *Tele-Visionaries: The People Behind The Invention of Television*, John Wiley & Sons, Inc., New Jersey 2005.

WEEKS, Edythe E., Esq., *Outer Space Development, International Relations and Space Law: A Method for Elucidating Seeds*, Cambridge Scholars Publishing, Newcastle 2012.

WENDT, Alexander, *Social Theory of International Politics*, 1. Basım, (Virtual Publishing, 2003), Cambridge University Press, New York 1999.

WHITMAN, Jim, *The Limits of Global Governance*, 1. Basım, Routledge, New York 2005.

WIENER, Norbert, *Cybernetics: Or Control and Communication in the Animal and the Machine*, The Massachusetts Institute of Technology Press, 4. Basım, Massachusetts 1985.

WILLIAMS, John B., *The Electronics Revolution: Inventing the Future*, 1. Basım, Springer Praxis Publishing, Chichester Mayıs 2017.

WILLIAMS, Raymond, *Television: Technology and Cultural Form*, 1. Basım, Schocken Books, New York 1975.

WINSTON, Brian, *Media, Technology and Society - A History: From The Telegraph to The Internet*, 1. Basım, Routledge, Londra 1998.

WOLFRAM, Stephen, *A New Kind Of Science*,1. Basım, Wolfram Media, Illinois 2002.

ZALOGA, Steven J., *V-2 Ballistic Missiles 1942-52*, Osprey Publishing, Oxford 2003.

ZIMAN, John Michael, *Public Knowledge: An Essay Concerning The Social Dimension of Science*, 2. Basım, Cambridge University Press, Londra 1974.

Makaleler / Kitap Bölümleri:

AALBERTS, Tanja E. & Rens van MUNSTER, "From Wendt to Kuhn: Reviving the 'Third Debate' in International Relations", *International Politics*, Cilt 45, Sayı 6, Ağustos 2008, ss. 720-746.

ABRAMSON, Albert, "The Invention of Television", *Television: An International History*, Editör: Anthony Smith, 2. Basım, Oxford University Press, New York 1998, ss. 9-23.

ADESINA, Olubukola S., "Foreign Policy in An Era of Digital Diplomacy", *Cogent Social Sciences*, Cilt 3, Sayı 1, 2017, ss. 1-13.

ADKINS, Gary, "Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism", *Journal of Strategic Security*, Cilt 6, Sayı 3, Güz 2013, ss. 1-9.

AHMAD, Rabiah & Zahri YUNOS, "A Dynamic Cyber Terrorism Framework", *International Journal of Computer Science and Information Security*, Cilt 10, Sayı 2, 2012, ss. 149-158.

AIDAN, Jagmeet Singh, Harsh Kumar VERMA & Lalit Kumar AWASTHI, "Comprehensive Survey on Petya Ransomware Attack", *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, Aralık 2017, ss. 122-125.

ALBION, Robert G., "The Communication Revolution", *The American Historical Review*, Cilt 37, Sayı 4, Temmuz 1932, ss. 718-720.

ALDRICH, Richard W., "How Do You Know You Are At War In The Information Age?", *Houston Journal of International Law*, Cilt 22, Sayı 2, 1999, ss. 223-260.

ALENIUS, Kari, "Victory in Exceptional War: The Estonian Main Narrative of the Cyber Attacks" , Editörler: Jari Rantapelkonen & Mirva Salminen, *The Fog of Cyber Defence*, National Defence University, Department of Leadership and Military Pedagogy, Publication Series 2, Article Collection No 10, Helsinki 2013, ss. 78-89.

ALKER, Hayward R., "On Learning From Wendt", *Review of International Studies*, Cilt 26, Sayı 1, 2000, ss. 141-150.

ANSELL, Christopher & Robert R. GEYER, "'Pragmatic Complexity' A New Foundation for Moving Beyond 'Evidence-Based Policy Making'?", *Policy Studies*, Cilt 38, Sayı 2, ss. 149-167.

ARSLAN, Hasan T. & Joyren QUARCOO, "Political, Economical and Social Impacts of Snowden Breach", *Pakistan Journal of Criminology*, Cilt 7, Sayı 2, Nisan 2015, ss. 29-42.

ATKESON, Andrew & Patrick J. KEHOE, "Modeling the Transition to a New Economy: Lessons from Two Technological Revolutions", *The American Economic Review*, Cilt 97, Sayı 1, Mart 2007, ss. 64-88.

AWAN, Imran, "Cyber Threats and Cyber Terrorism: The Internet as a Tool for Extremism", Editörler: Brian Blakemore & Imran Awan, *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*, Routledge, New York 2016, ss. 21-38.

BALDWIN, David A., "Thinking About Threats", *The Journal of Conflict Resolution*, Cilt 15, Sayı 1, Mart 1971, ss. 71-78.

BALL, Ken, "How Programmable Emerged From", *Control Engineering*, Eylül 2008, ss. 66-70.

BARLETTA, William A., "Cyberwar or Cyber-Terrorism: The Attack On Estonia", *International Seminar on Nuclear War and Planetary Emergencies*, The

Science and Culture Series, Nuclear Strategy and Peace Technology, 38th Session, 19-24 Ağustos 2007, Erice, İtalya 2008, ss. 481-486.

BARRINHA, André & Thomas RENARD, "Cyber-Diplomacy: The Making of an International Society in the Digital Age", *Global Affairs*, Cilt 3, Sayı 4-5, 2017, ss. 353-364.

BARRY, Andrew, "The Translation Zone: Between Actor-Network Theory and International Relations", *Millennium: Journal International Studies*, Cilt 41, Sayı 3, 2013, ss. 413-429.

BARZASHKA, Ivanka, "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme", *The RUSI Journal*, Cilt 158, Sayı 2, 2013, ss. 48-56.

BAUMAN, Zygmunt, Didier BIGO, Paulo ESTEVES, Elspeth GUILD, Vivienne JABRI, David LYON & R. B. J. WALKER, "After Snowden: Rethinking the Impact of Surveillance", *International Political Sociology*, Cilt 8, Sayı 2, Haziran 2014, ss. 121-144.

BELL, Duncan, "Beware of False Prophets: Biology, Human Nature and the Future of International Relations Theory", *International Affairs (Royal Institute of International Affairs 1944-)*, Cilt 82, Sayı 3, Mayıs 2006, ss. 493-510.

BELLIA, Patricia L., "WikiLeaks and the Institutional Framework for National Security Disclosures", *The Yale Law Journal*, Cilt 121, Sayı 6, Nisan 2012, ss. 1448-1526.

BERKNER, Lloyd V., "Earth Satellites and Foreign Policy", *Foreign Policy*, Cilt 36, Sayı 2, Ocak 1958, ss. 221-231.

BERKOWITZ, Marc J., "Shaping the Outer Space and Cyberspace Environments", Editör: Scott Jasper, *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, Georgetown University Press, Washington, D.C. 2012.

BEKTAS, Yakup, "Displaying the American Genius: The Electromagnetic Telegraph in the Wider World", *The British Journal for the History of Science*, Cilt 34, Sayı 2, Haziran 2001, ss. 199-232.

BEN-JACOB, Marion G., "Global Perspectives on Internet Regulation", *GSTF Journal of Computing (JoC)*, Cilt 6, Sayı 1, 2018, ss. 1-8.

BERKOWITZ, Marc J., "Shaping the Outer Space and Cyberspace Environments", Editör: Scott Jasper, *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, Georgetown University Press, Washington, D.C. 2012, ss. 155-170.

BETZ, David J. & Tim STEVENS, "Chapter One: Power and Cyberspace", *Adelphi Series, Cyberspace and the State: Towards a Strategy for Cyber-power*, Cilt 51, Sayı 424, 2011, ss. 35-54.

BETZ, David J. & Tim STEVENS, "Chapter Three: Cyberspace and War", *Adelphi Series, Cyberspace and the State: Toward a Strategy for Cyber-power*, Cilt 51, Sayı 424, 2011, ss. 75-98.

BEZANSON, Anna, "The Early Use of the Term Industrial Revolution", *The Quarterly Journal of Economics*, Cilt 36, Sayı 2, Şubat 1922, ss. 343-349.

BING, Jon, "Building Cyberspace: A Brief History of Internet", Editörler: Lee A. Bygrave & Jon Bing, *Internet Governance: Infrastructure and Institutions*, 1. Basım, Oxford University Press, New York 2009, ss. 8-47.

BİLGİN, Mert, "The State of Future in International Relations", *Futures*, Cilt 82, Eylül 2016, ss. 52-62.

BJOLA, Corneliu, "Introduction: Making Sense of Digital Diplomacy", Editörler: Corneliu Bjola & Marcus Holmes, *Digital Diplomacy: Theory and Practice*, 1. Basım, Routledge, New York 2015, ss. 1-10.

BJOLA, Corneliu, "Digital Diplomacy – The State of the Art", *Global Affairs*, Cilt 2, Sayı 3, 2016, ss. 297-299.

BLAIR, Cherie & Ema Vidak GOJKOVIC, "WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence", *ICSID Review*, Cilt 33, Sayı 1, 2018, ss. 235-259.

BOUSQUET, Antoine, "Complexity Theory and the War on Terror: Understanding The Self-Organising Dynamics of Leaderless Jihad", *Journal of International Relations and Development*, Cilt 15, Sayı 3, 2012, ss. 345-369.

BOUSQUET, Antoine & Robert R. GEYER, "Introduction: Complexity and The International Arena", *Cambridge Review of International Affairs*, Cilt 24, Sayı 1, Mart 2011, ss. 1-3.

BOUSQUET, Antoine & Simon CURTIS, "Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations", *Cambridge Review of International Affairs*, Cilt 24, Sayı 1, Mart 2011, ss. 43-62.

BOYD, Danah & Kate CRAWFORD, "Critical Questions For Big Data: Provocations For A Cultural, Technological, and Scholarly Phenomenon", *Information, Communication & Society*, Cilt 15, Sayı 5, 2012, ss. 662-679.

BRAMAN, Sandra, "Cyber Security Ethics at the Boundaries: System Maintenance and the Tallinn Manual", Editörler: Ludovica Glorioso & Anna-Maria

Osula, *Proceedings: 1st Workshop on Ethics of Cyber Conflict*, Tallinn 2014, ss. 49-58.

BRANDAU, Daniel, "Demarcation in the Void: Early Satellites and the Making of Outer Space", *Historical Social Research/Historische Sozialforschung*, Special Issue: Law and Conventions from a Historical Perspective, Cilt 40, Sayı 1 (151), 2015, ss. 239-264.

BRANQUINHO, Marcelo Ayres, "Ransomware In Industrial Control Systems: What Comes After WannaCry and Petya Global Attack?", Editörler: C. A. Brebbia, F. Garzia & M. Lombardi, *WIT Transactions on The Built Environment, Safety and Security Engineering VII*, WIT Press, Cilt 174, Southampton 2017, ss. 329-334.

BRANTLY, Aaron Franklin, "The Cyber Losers", *Democracy and Security*, Cilt 10, Sayı 2, 2014, ss. 132-155.

BREVINI, Benedetta, Arne Hintz & Patrick McCurdy, "Introduction", Editörler: Benedetta Brevini, Arne Hintz & Patrick McCurdy, *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, 1. Basım, Palgrave Macmillan, Hampshire 2013, ss. 1-10.

BROOKS, Harvey, "Technology, Evolution, and Purpose", *Daedalus*, Cilt 109, Sayı 1, Kış 1980, ss. 65-81.

BROWAEYS, Marie-Joelle & Walter BAETS, "Cultural Complexity: A New Epistemological Perspective", *The Learning Organization*, Cilt 10, Sayı 6, 2003, ss. 332-339.

BROWN, Gary & Keira POELLET, "The Customary International Law of Cyberspace", *Strategic Studies Quarterly*, Cilt 6, Sayı 3, Cyber Special Edition, Güz 2012, ss. 126-145.

BUCHAN, Russell, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", *Journal of Conflict & Security Law*, Cilt 17, Sayı 2, 2012, ss. 211-227.

BULLEN, Keith E., "The International Geophysical Year", *The Australian Quarterly*, Cilt 29, Sayı 1, Mart 1957, ss. 16-25.

BUSCHER, Bram, Stasja KOOT & Ingrid L. NELSON, "Introduction. Nature 2.0: New Media, Online Activism and The Cyberpolitics of Environmental Conservation", *Geoforum*, Cilt 79, Sayı 100, 2017, ss. 111-113.

BUZAN, Barry & Richard LITTLE, "Why International Relations has Failed as an Intellectual Project and What to do About it", *Millennium: Journal of International Studies*, Cilt 30, Sayı 1, 2001, ss. 19-39.

BUZAN, Barry & George LAWSON, "The Global Transformation: The Nineteenth Century and the Making of Modern International Relations", *International Studies Quarterly*, Cilt 57, Sayı 3, 2013, ss. 620-634.

CAMMAERTS, Bart, "Networked Resistance: The Case of WikiLeaks", *Journal of Computer-Mediated Communication*, Cilt 18, Sayı 4, Temmuz 2013, ss. 420-436.

CHARALAMBIDES, Yiannos, "The Invisible Cyber War", *21st Century*, Cilt 13, Sayı 1, 2013, ss. 16-34.

CHECKEL, Jeffrey T., "Review: The Constructivist Turn in International Relations Theory", *World Politics*, Cilt 50, Sayı 2, Ocak 1998, ss. 324-348.

CHEN, Wenhong & Barry WELLMAN, "The Global Digital Divide – Within and Between Countries", *IT & Society*, Cilt 1, Sayı 7, Yaz 2004, ss. 18-25.

CHENOU, Jean-Marie & Roxana RADU, "Global Internet Policy: A Fifteen-Year Long Debate", Editörler: Roxana Radu, Jean-Marie Chenou & Rolf H. Weber, *The Evolution of Global Internet Governance: Principles and Policies in the Making*, Springer-Verlag, Berlin Heidelberg 2014, ss. 3-22.

CHICHILNISKY, Graciela, "The Knowledge Revolution", *Journal of International Trade & Economic Development*, Cilt 7, Sayı 1, 1998, ss. 39-54.

CHINEN, Mark, "Complexity Theory and The Horizontal and Vertical Dimensions of State Responsibility", *The European Journal of International Law*, Cilt 25, Sayı 3, 2014, ss. 703-732.

CHOUCRI, Nazli, "Introduction: CyberPolitics in International Relations", *International Political Science Review*, Cilt 21, Sayı 3, 2000, ss. 243-263.

CHOUCRI, Nazli, Stuart MADNICK & Jeremy FERWERDA, "Institutions for Cyber Security: International Responses and Global Imperatives", *Infromation Technology for Development*, Cilt 20, Sayı 2, 2014, ss. 96-121.

CHRISTENSEN, Christian, "A Decade of WikiLeaks: So What?", *International Journal of Media & Cultural Politics*, Cilt 10, Sayı 3, 2015, ss. 273-284.

CHRISTOU, George & Seamus SIMPSON, "Gaining a Stake in Global Internet Governance: The EU, ICANN and Strategic Norm Manipulation", *European Journal of Communication*, Cilt 22, Sayı 2, 2007, ss. 147-164.

CIMBALA, Stephen J. & Roger N. MCDERMOTT, "A New Cold War? Missile Defenses, Nuclear Arms Reductions, and Cyber War", *Comparative Strategy*, Cilt 34, Sayı 1, 2015, ss. 95-111.

CIOT, Melania-Gabriela, "Cyberspace and The New World Order", *Studia Universitatis Babes-Bolyai-Studia Europaea,* Cilt 62, Sayı 2, ss. 5-15.

CODDING, George A., Jr., "Evolution of the ITU", *Telecommunications Policy*, Cilt 15, Sayı 4, Ağustos 1991, ss. 271-285.

COLINO, Richard R., "INTELSAT: Facing the Challenge of Tomorrow", *Journal of International Affairs*, Cilt 39, Sayı 1, 1985, ss. 129-150.

COLLINS, Neil & Kristina BEKENOVA, "Digital Diplomacy: Success at Your Fingerprint", *Place Branding and Public Diplomacy,* Cilt 15, Sayı 1, Mart 2019, ss. 1-11.

COLLINS, Sean & Stephen MCCOMBIE, "Stuxnet: The Emergence of A New Cyber Weapon and Its Implications", *Journal of Policing, Intelligence and Counter Terrorism*, Cilt 7, Sayı 1, Nisan 2012, ss. 80-91.

CONGRESSIONAL DIGEST CORPORATION, "Internet History: From ARPANET to Broadband", *Congressional Digest*, Cilt 86, Sayı 2, Şubat 2007, ss. 35-39.

CORNISH, Paul, "Governing Cyberspace Through Constructive Ambiguity", *Survival: Global Politics and Strategy*, Cilt 57, Sayı 3, Haziran-Temmuz 2015, ss. 153-176.

COSTIGAN, Sean S. & Chris PALLARIS, "Knowledge Ecologies in International Affairs: A New Paradigm for Dialog and Collaboration", Editörler: Sean S. Costigan & Jake Perry, *Cyberspaces and Global Affairs,* Ashgate Publishing, Farnham 2012, ss. 283-292.

CRACKNELL, Arthur P. & Costas A. VAROTSOS, "Editorial and Cover: Fifty Years After The First Artifical Satellite: From Sputnik 1 to ENVISAT", *International Journal of Remote Sensing*, Cilt 28, Sayı 10, 2007, ss. 2071-2072.

CRAFTS, Nicholas & Charles Knickerbocker HARLEY, "Output Growth and the British Industrial Revolution: A Restatement of the Crafts-Harley View", *The Economic History Review*, Cilt 45, Sayı 4, Kasım 1992, ss. 703-730.

CRAFTS, Nicholas, "Forging Ahead and Falling Behind: The Rise and Relative Decline of the First Industrial Nation", *The Journal of Economic Perspectives*, Cilt 12, Sayı 2, Bahar 1998, ss. 193-210.

CRAFTS, Nicholas, "Explaining the First Industrial Revolution: Two Views", *European Review of Economic History*, Cilt 15, Sayı 1, Nisan 2011, ss.153-168.

CRAIG, Anthony & Brandon VALERIANO, "Conceptualising Cyber Arms Races", *2016 8th International Conference on Cyber Conflict (CyCon)*, 31 Mayıs-3 Haziran 2016, Tallinn, ss. 141-158.

CUDWORTH, Erika & Stephen HOBDEN, "The Foundations of Complexity, The Complexity of Foundations", *Philosophy of the Social Sciences*, Cilt 42, Sayı 2, 2012, ss. 163-187.

CURRENT SCIENCE ASSOCIATION, "Space Satellites and World Communications", *Current Science*, Cilt 31, Sayı 5, Mayıs 1962, ss. 177-178.

D'AMATO, Anthony, "International Law, Cybernetics, and Cyberspace", *International Law Studies*, Cilt 76, Sayı 1, 2002, ss. 59-71.

DAVIS, James W. & Miriam MECKEL, "Political Power and the Requirements of Accountability in the Age of WikiLeaks", *ZPol Zeitschrift für Politikwissenschaft*, Cilt 22, Sayı 4, 2012, ss. 463-491.

DEEKS, Ashley, éAn International Legal Framework for Surveillance", *Virginia Journal of International Law*, Cilt 55, Sayı 2, Bahar 2015, ss. 291-368.

DEIBERT, Ron, "The Geopolitics of Cyberspace After Snowden", *Current History*, Cilt 114, Sayı 768, Ocak 2015, ss. 9-15.

DEIBERT, Ronald J., "Black Code Redux: Censorship, Surveillance, and the Militarization of Cyberspace", Editör: Megan Boler, *Digital Media and Democracy: Tactics in Hard Times*, The Massachusetts Institute of Technology Press, Massachusetts 2008, ss. 137-163.

DEIBERT, Ronald J. & Masashi CRETE-NISHIHATA, "Global Governance and The Spread of Cyberspace Controls", *Global Governance*, Cilt 18, Sayı 3, 2012, ss. 339-361.

DEIBERT, Ronald J., Rafal ROHOZINSKI & Masashi CRETE-NISHIHATA, "Cyclones In Cyberspace: Information Shaping and Denial In the 2008 Russia–Georgia War", *Security Dialogue*, Cilt 43, Sayı 1, 2012, ss. 3-24.

DELERUE, François, "Reinterpretation or Contestation of International Law in Cyberspace?", *Israel Law Review*, Cilt 52, Sayı 3, 2019, ss. 295-326.

DEMCHAK, Chris, "Evolutions In Asymmetric Cyberpower", *World Politics Review*, Cyberwar: Real and Imagined, Feature Report, 19 Nisan 2011, ss. 5-8.

DENEMARK, Robert A., "World System History: From Traditional International Politics to the Study of Global Relations", *International Studies Review*, Cilt 1, Sayı 2, Yaz 1999, ss. 43-75.

DEUTSCH, Karl W., "The Impact of Science and Technology on International Politics", *Daedalus*, Cilt 88, Sayı 4, Güz 1959, ss. 669-685.

DITTMAR, Jeremiah E., "Information Technology and Economic Change: The Impact of the Printing Press", *The Quarterly Journal of Economics*, Cilt 126, Sayı 3, Ağustos 2011, ss. 1133-1172.

DOĞRUL, Murat, Adil ASLAN & Eyyüp ÇELİK, "Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism", *2011 3rd International Conference On Cyber Conflict*, Tallinn 2011, ss. 29-43.

DUNN, Myriam, "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)", *Internationl Journal of Critical Infrastructures*, Cilt 1, Sayı 2-3, 2005, ss. 258-268.

DUNN, Myriam A., "Securing The Digital Age: The Challenges of Complexity for Critical Infrastructure Protection and IR Theory", Editörler: Johan Eriksson & Giampiero Giacomello, *International Relations and Security in the Digital Age*, 1. Basım, Routledge, New York 2007, ss. 85-105.

DUNN CAVELTY, Myriam, "The Militarisation of Cyberspace: Why Less May Be Better", *2012 4th International Conference on Cyber Conflict (CYCON)*, 5-8 Haziran 2012, Tallinn, ss. 1-13.

DUNN CAVELTY, Myriam, "Europe's Cyber-Power", *European Politics and Society*, Cilt 19, Sayı 3, 2018, ss. 304-320.

EBERT, Hannes & Tim MAURER, "Contested Cyberspace and Rising Powers", *Third World Quarterly*, Cilt 34, Sayı 6, 2013, ss. 1054-1074.

EETEN, Michel JG van & Milton MULLER, "Where is the Governance in Internet Governance?", *New Media & Society*, Cilt 15, Sayı 5, 2012, ss. 720-736.

EGAN J. D., Brian J., "International Law and Stability in Cyberspace", *Berkeley Journal of International Law*, Cilt 35, Sayı 1, 2017, ss. 169-180.

EINSTEIN, Albert, "Ether and The Theory of Relativity", *The Collected Papers of Albert Einstein, Volume 7: The Berlin Years: Writings, 1918-1921 (English Translation Supplement by Alfred Engel),* Princeton University Press, New Jersey 2002, ss. 160-183.

ELHEFNAWY, Nader, "Societal Complexity and Diminishing Returns in Security", *International Security*, Cilt 29, Sayı 1, Yaz 2004, ss. 152-174.

EPSTEIN, Dmitry, "The Making of Institutions of Information Governance: The Case of the Internet Governance Forum", *Journal of Infromation Technology*, Cilt 28, Sayı 2, 2013, ss. 137-149.

ERALP, Atila, "Uluslararası İlişkiler Disiplininin Oluşumu: İdealizm-Realizm Tartışması", *Devlet, Sistem ve Kimlik: Uluslararası İlişkilerde Temel Yaklaşımlar*, Editör: Atila Eralp, 9. Basım, İletişim Yayınları, İstanbul 2007, ss. 57-89.

ERIKSSON, Johan & Giampiero GIACOMELLO, "Introduction: Closing the Gap Between International Relations Theory and Studies of Digital-Age Security", Editörler: Johan Eriksson & Giampiero Giacomello, *International Relations and Security in the Digital Age*, 1. Basım, Routledge, New York 2007, ss. 1-28.

ESLAHI, Meisam, Rosli SALLEH & Nor Badrul ANUAR, "Bots and Botnets: An Overview of Characteristics, Detection and Challenges", *2012 IEEE International Conference on Control System, Computing and Engineering,* 23-25 Kasım 2012, Penang, Malezya, ss. 349-354.

EWING, Ann, "Man's First Satellites", *The Science News Letter*, Cilt 72, Sayı 1, Temmuz 1957, ss. 10-11.

FARLEY, Tom, "Mobile Telephone History", *Telektronikk*, Cilt 101, Sayı 3/4, 2005, ss. 22-35.

FIDLER, David P., "Tinker, Tailor, Soldier, Duqu: Why Cyberespionage is More Dangerous Than You Think", *International Journal of Critical Infrastructure Protection*, Cilt 1, Sayı 5, 2012, ss. 28-29.

FIDLER, David P., "Cyberspace, Terrorism and International Law", *Journal of Conflict & Security Law*, Cilt 21, Sayı 3, 2016, ss. 475-493.

FINNEGAN, Richard B., "International Relations: The Disputed Search for Method", *The Review of Politics*, Cilt 34, Sayı 1, Ocak 1972, ss. 40-66.

FLASHES MAGAZINE, "The Third Industrial Revolution", Sayı 34, Ekim 2017, ss. 54-58.

FLECK, Dieter, "Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual", *Journal of Conflict and Security Law*, Cilt 18, Sayı 2, Temmuz 2013, ss. 331-351.

FONTANA, Iole, "Disentangling the Cyber Politics – Cyber Security Nexus: The New Challenge of Global Politics", *Global Affairs*, Cilt 3, Sayı 1, 2017, ss. 1-6.

FORSYTH, James Wood Jr., "What Great Powers Make It: International Order and The Logic of Cooperation in Cyberspace", *Strategic Studies Quarterly*, Cilt 7, Sayı 1, Bahar 2013, ss. 93-113.

FOULADI, Ramin Fadaei, Tina SEIFPOOR & Emin ANARIM, "Frequency Characteristics of DoS and DDoS Attacks", *2013 21st Signal Processing and*

Communications Applications Conference (SIU), Haspolat, 24-26 Nisan 2013, ss. 1-4.

FREEMAN, Christopher, "New Technology and Catching Up", *Technology and Development in the Third Industrial Revolution*, Editörler: Charles Cooper & Raphael Kaplinsky, Frank Cass, Londra 2005, ss. 83-96.

FRITSCH, Stefan, "Technology and Global Affairs", *International Studies Perspectives*, Cilt 12, Sayı 1, 2011, ss. 27-45.

FUCHS, Christian & Daniel TROTTIER, "Internet Surveillance After Snowden: A Critical Empirical Study of Computer Experts' Attitudes on Commercial and State Surveillance of the Internet and Social Media Post-Edward Snowden", *Journal of Information, Communication and Ethics in Society*, Cilt 15, Sayı 4, 2017, ss. 412-444.

GAMREKLIDZE, Ellada, "Cyber Security In Developing Countries, A Digital Divide Issue: The Case of Georgia", *Journal of International Communication*, Cilt 20, Sayı 2, 2014, ss. 200-217.

GANDHI, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu & Phillip Laplante, "Dimensions of Cyber-Attacks: Social, Political, Economic, and Cultural", *IEEE Technology and Society Magazine*, Cilt 30, Sayı 1, Bahar 2011, ss. 28-38.

GAYCKEN, Sandra & Maurizio MARTELLINI, "Cyber as Deterrent", Editör: Maurizio Martellini, *Cyber Security: Deterrence and IT Protection for Critical Infrastructures*, Springer, Cham 2013, ss. 1-10.

GEERS, Kenneth, "Cyberspace and the Changing Nature of Warfare", *NATO Science and Technology Organization RTO - Meeting Proceedings Paper*, ST-076/RSY-017, Tallinn, 10 Mart 2008, ss. 1-12.

GELLER, Armando, "The Use of Complexity-Based Models in International Relations: A Technical Overview and Discussion of Prospects and Challenges", *Cambridge Review of International Affairs*, Cilt 24, Sayı 1, Mart 2011, ss. 63-80.

GELLER, Daniel S., "Nuclear Weapons, Deterrence, and Crisis Escalation", *The Journal of Conflict Resolution*, Cilt 34, Sayı 2, 1990, ss. 291-310.

GERDES, Justin, "Jeremy Rifkin: Energizing the Third Industrial Revolution", *Siemens Living Energy: The Magazine for International Energy Leadership*, Sayı 8, Temmuz 2013, ss. 8-13.

GEYER, Robert R., "European Integration, The Problem of Complexity and The Revision of Theory", *JCMS: Journal of Common Market Studies*, Cilt 41, Sayı 1, 2003, ss. 15-35.

GEYER, Robert R., "Beyond The Third Way: The Science of Complexity and The Politics of Choice", *British Jorunal of Politics and International Relations*, Cilt 5, Sayı 2, Mayıs 2003, ss. 237-257.

GEYER, Robert R., "Globalization, Europeanization, Complexity, and the Future of Scandinavian Exceptionalism", *Governance: An International Journal of Policy, Administration, and Institutions*, Cilt 16, Sayı 4, Ekim 2003, ss. 559-576.

GHORI, Karamatullah K., "The Global Challenge of WikiLeaks", *Pakistan Horizon*, Cilt 64, Sayı 1, Ocak 2011, ss. 5-15.

GANDHI, Robin, Anup SHARMA, William MAHONEY, William SOUSAN, Qiuming ZHU & Phillip LAPLANTE, "Dimensions of Cyber-Attacks: Social, Political, Economic, and Cultural", *IEEE Technology and Society Magazine*, Cilt 30, Sayı 1, Bahar 2011, ss. 28-38.

GILBOA, Eytan, "Diplomacy in the Media Age: Three Models of Uses and Effects", *Diplomacy and Statecraft*, Cilt 12, Sayı 2, 2001, ss. 1-28.

GILBOA, Eytan, "Real-Time Diplomacy: Myth and Reality", Editör: Evan H. Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, McGill-Quenn's University Press, Londra 2002, ss. 83-109.

GOLDSMITH, Daniel & Michael SIEGEL, "Cyber Politics: Understanding the Use of Social Media for Dissident Movements in an Integrated State Stability Framework", *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, IEEE, 2012, ss. 1321-1328.

GOTZ, Marta & Barbara JANKOWSKA, "Clusters and Industry 4.0: Do They Fit Together?", *European Planning Studies*, Cilt 25, Sayı 9, 2017, ss. 1633-1653.

GÖKÇE, Yasir, "Güç Kullanımı Olarak Siber Faaliyetler: Uluslararası Hukukun Siber Uzaya Uygulanabilirliği", *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 1, Sayı 1, 2017, ss. 22-54.

GRAVES, Harold N., "European Radio and the War", *The Annals of the American Academy of Political and Social Science*, Cilt 213, New Horizons in Radio, Ocak 1941, ss. 75-82.

GREENWOOD, Jeremy, "The Third Industrial Revolution: Technology, Productivity, and Income Inequality", *Economic Review*, Cilt 35, Sayı 2, Bahar 1999, ss. 2-12.

GUNITSKY, Seva, "Complexity and Theories of Change in International Politics", *International Theory*, Cilt 5, Sayı 1, Mart 2013, ss. 35-63.

GUPTA, Biswanath & Ekta RATHORE, "United Nations General Assembly Resolutions in the Formation of the Outer Space Treaty of 1967", *Astropolitics*, Cilt 17, Sayı 2, ss. 77-88.

GUPTA, Devaryan, "Laser Technology Applications: A Gift to Humanity", *International Journal of Applied Research*, Cilt 1, Sayı 7, 2015, ss. 476-486.

GUPTA, Shubham, Vishal SHARMA & Parshant SHARMA, "Cathode Ray Tube and Its Applications", *International Journal of Innovative Research in Technology*, Cilt 1, Sayı 6, 2014, ss. 1731-1733.

HAASTER, Jelle van, "Assessing Cyber Power", *8th International Conference on Cyber Conflict (CyCon)*, IEEE, 2016, ss. 7-21.

HAATAJA, Samuli, " The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach", *Law, Innovation and Technology*, Cilt 9, Sayı 2, 2019, ss. 159-189.

HAIZLER, Omry, "The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking", *Cyber, Intelligence, and Security*, Cilt 1, Sayı 1, Ocak 2017, ss. 31-45.

HAY, James, "The Invention of Air Space, Outer Space, and Cyberspace", Editörler: Lisa Parks & James Schwoch, *Down to Earth: Satellite Technologies, Industries, and Cultures*, Rutgers University Press, New Jersey 2012, ss. 19-41.

HEADRICK, Daniel R. & Pascal GRISET, "Submarine Telegraph Cables: Business and Politics, 1838-1939", *The Business History Review*, Cilt 75, Sayı 3, Güz 2001, ss. 543-578.

HEALEY, Jason, "Winning and Losing in Cyberspace", *2016 8th International Conference on Cyber Conflict (CyCon)*, 4 Ağustos 2016, Tallinn, ss. 37-49.

HEARN, Kay, Patricia A. H. WILLIAMS & Rachel J. MAHNCKE, "International Relations and Cyber Attacks: Official and Unofficial Discourse", *11th Australian Information Warfare and Security Conference*, Edith Cowan University, Perth Western Australia, 30 Kasım-2 Aralık 2010, ss. 7-12.

HEINEGG, Wolff Heintschel von, "The Tallinn Manual and International Cyber Security Law", Editörler: Terry D. Gill, Robin Geiß, Tim McCormack, Christophe Paulussen & Jessica Dorsey, *Yearbook of International Humanitarian Law*, Cilt 15, 2012, ss. 3-18.

HEINEGG, Wolff Heintschel von, "Territorial Sovereignty and Neutrality in Cyberspace", *International Law Studies*, Cilt 89, Sayı 1, 2013, ss. 123-156.

HERZOG, Stephen, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, Cilt 4, Sayı 2, Yaz 2011, ss. 49-60.

HILL, Richard, "Dealing with Cyber Security Threats: International Cooperation, ITU, and WCIT", *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn 2015, ss. 119-134.

HINTZ, Arne, "Challenges to Freedom of Expression in the Digital World: Lessons from WikiLeaks and the Arab Spring", *ESSACHESS - Journal for Communication Studies*, Cilt 5, Sayı 1(9), 2012, ss. 83-105.

HOFFMAN, Mark, "Conversaitions on Critical International Relations Theory", *Millennium: Journal of International Studies*, Cilt 17, Sayı 1, 1988, ss. 91-95.

HOFFMAN, Matthew J., "Constructing a Complex World: The Frontiers of International Relations Theory and Foreign Policy-making", *Asian Journal of Political Science*, Cilt 11, Sayı 2, Aralık 2003, ss. 37-58.

HOFFMANN, Matthew J. & John RILEY JR., "The Science of Political Science: Linearity or Complexity in Designing Social Inquiry", *New Political Science*, Cilt 24, Sayı 2, 2002, ss. 303-320.

HOLLING, Crawford S., Lance H. GUNDERSON & Donald LUDWIG, "In Quest of a Theory of Adaptive Change", Editörler: Lance H. Gunderson & Crawford S. Holling, *Panarchy: Understanding Transformations in Human and Natural Systems*, 3. Basım, Island Press, Washington DC 2002, ss. 3-24.

HOLLIS, Duncan B., "Why States Need an International Law for Information Operations", *Lewis & Clark Law Review*, Cilt 11, Sayı 4, 2007, ss. 1023-1061.

HOPPIT, Julian, "Counting The Industrial Revolution", *Economic History Review*, Cilt 43, Sayı 2, Mayıs 1990, ss. 173-195.

HORGAN, John, "From Complexity to Perplexity", *Scientific American*, Cilt 272, Sayı 6, Temmuz 1995, ss. 104-109.

HORKÝ, Ondřej, "The Future of Diplomacy: European and Global Challenges", *Institute of International Relations*, Policy Paper, Prag, Şubat 2011, ss. 1-10.

HURLEY, Neil P., "Satellite Communications: A Case Study of Technology's Impact on Politics", *The Review of Politics*, Cilt 30, Sayı 2, Nisan 1968, ss. 170-190.

HURWITZ, Roger, "Depleted Trust in the Cyber Commons", *Strategic Studies Quarterly*, Cilt 6, Sayı 3, Cyber Special Edition, Güz 2012, ss. 20-45.

HURWITZ, Roger, "A New Normal? The Cultivation of Global Norms As Part of A Cybersecurity Strategy", Editörler: Panayotis A. Yannakogeorgos & Adam B. Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, Taylor & Francis, Florida 2014, ss. 233-264.

HSU, Kimberly & Craig MURRAY, "China and International Law in Cyberspace", *U.S.-China Economic and Security Review Commission Staff Report*, 6 Mayıs 2014.

HWANG, Jennie S., "The Fourth Industrial Revolution (Industry 4.0): Intelligent Manufacturing", *SMT (Surface Mount Technology) Magazine*, Temmuz 2016, ss. 10-15.

IASIELLO, Emilio, "Cyber Attack: A Dull Tool to Shape Foreign Policy", *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 4-7 Haziran 2013, Tallinn 2013, ss. 1-18.

IMRE, Iveta, Ivanka Pjesivac & Catherine A. Luther, "Governmental Control of the Internet and WikiLeaks: How does the Press in Four Countries Discuss Freedom of Expression?", *the International Communication Gazette*, Cilt 78, Sayı 5, 2016, ss. 385-410.

ITTEFAQ, Muhammed, "Digital Diplomacy via Social Networks: A Cross-National Analysis of Governmental Usage of Facebook and Twitter for Digital Engagement", *Journal of Contemporary Eastern Asia*, Cilt 18, Sayı 1, Yaz 2019, ss. 49-69.

JARMON, Jack, "Cyber-Terrorism", *Journal on Terrorism and Security Analysis (JTSA)*, Cilt 6, Bahar 2011, ss. 102-117.

JARVIS, Lee & Stuart Macdonald, "What Is Cyberterrorism? Findings From a Survey of Researchers", *Terrorism and Political Violence*, Cilt 27, Sayı 4, 2015, ss. 657-678.

JENSEN, Eric Talbot, "The Tallinn Manual 2.0: Highlights and Insights", *Georgetown Journal of International Law*, Cilt 48, Sayı 3, 2017, ss. 735-778.

JEVONS, H. Stanley, "The Second Industrial Revolution", *The Economic Journal*, Cilt 41, Sayı 161, Mart 1931, ss. 1-18.

KAPLAN, Morton A., "The New Great Debate: Traditionalism vs. Science in International Relations", *World Politics*, Cilt 19, Sayı 1, Ekim 1966, ss. 1-20.

KARATNYCKY, Adrian, "Ukraine's Orange Revolution", *Foreign Affairs*, Cilt 84, Sayı 2, Mart-Nisan 2005, ss. 35-52.

KAVALSKI, Emilian, "The Fifth Debate and the Emergence of Complex International Relations Theory: Notes on the Application of Complexity Theory to the Study of International Life", *Cambridge Review of International Affairs*, Cilt 20, Sayı 3, 2007, ss. 435-454.

KELLNER, Douglas, "Globalisation, Technopolitics and Revolution", *Theoria: A Journal of Social and Political Theory*, Cilt 48, Sayı 98, Aralık 2001, ss. 14-34.

KEOHANE, Robert O., "International Institutions: Two Approaches", *International Studies Quarterly*, Cilt 32, Sayı 4, Aralık 1988, ss. 379-396.

KEOHANE, Robert O. & Joseph S. NYE, Jr., "Power and Interdependence in the Information Age", *Foreign Affairs*, Cilt 77, Sayı 5, Eylül/Ekim 1988, ss. 81-94.

KESSLER, Oliver & Wouter WERNER, "Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare", *Leiden Journal of International Law,* Cilt 26, Sayı 4, Aralık 2013, ss. 793-810.

KILOVATY, Ido, "Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", *American University National Security Law Brief,* Cilt 5, Sayı 1, 2014, ss. 91-124.

KIRAVUO, Timo & Mikko SÄRELÄ, "The Care and Maintenance of Cyberweapons", Editörler: Jari Rantapelkonen & Mirva Salminen, *The Fog of Cyber Defence,* National Defense University, Publication Series 2, Article Collection No 10, Helsinki 2013, ss. 218-230.

KISSANE, Dylan, "Revolution in Political Affairs", *Central European University Political Science Journal*, Cilt 5, Sayı 4, Aralık 2010, ss. 487-491.

KLINGER, Julie Michelle, "Environmental Geopolitics and Outer Space", *Geopolitics*, Cilt 24, Sayı 1, 2019, ss. 1-38.

KNOEPFEL, Sascha, "Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War", Editörler: Jan-Frederik Kremer & Benedikt Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer-Verlag, Berlin Heidelberg 2014, ss. 117-124.

KOBRIN, Stephen J., "Territoriality and The Governance of Cyberspace", *Journal of International Business Studies*, Cilt 32, Sayı 4, 2001, ss. 687-704.

KOH, Harold Hongju, "International Law in Cyberspace", *Harvard International Law Journal*, Cilt 54, Sayı 1, Aralık 2012, ss. 1-12.

KOMAR, Myroslav, Vitaliy Dorosh, Grygoriy Hladiy & Anatoliy Sachenko, "Deep Neural Network for Detection of Cyber Attacks", *2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC)*, Kiev, 8-12 Ekim 2018, ss. 1-4.

KONSTANTOPOULOS, Ioannis L., "Democracy and Ethics vs. Intelligence and Security: From WikiLeaks to Snowden", Editörler: George C. Bitros & Nicholas C. Kyriazis, *Democracy and an Open-Economy World Order*, Springer International Publishing AG, Cham 2017, ss. 3-24.

KOSTYUK, Nadiya, "The Digital Prisoner's Dilemma: Challenges and Opportunities for Cooperation", *2013 World Cyberspace Cooperation Summit IV (WCC4)*, 4-6 Kasım 2013, California, ss. 1-6.

KREMER, Jan-Frederik & Benedikt MULLER, "SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World", Editörler: Jan-Frederik Kremer & Benedikt Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer-Verlag, Berlin Heidelberg 2014, ss. 41-58.

KRIGE, John & Kai-Henrik BARTH, "Introduction: Science, Technology, and International Affairs", *Osiris*, Cilt 21, Sayı 1, 2006, ss. 1-21.

KUEHL, Daniel T., "From Cyberspace to Cyberpower: Defining the Problem", Editörler: Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz, *Cyberpower and National Security*, 1. Basım, National Defense University Press & Potomac Books, Virginia 2009, ss. 24-42.

KULESZA, Joanna, "International Internet Law", *Global Change, Peace & Security*, Cilt 24, Sayı 3, Ekim 2012, ss. 351-364.

KURKI, Milja, "Causes of a Divided Discipline: Rethinking the Concept of Cause in International Relations Theory", *Review of International Studies*, Cilt 32, Sayı 2, Nisan 2006, ss. 189-216.

KUZMACK, Arnold M., "Technological Change and Stable Deterrence", *Journal of Conflict Resolution*, Cilt 9, Sayı 3, Eylül 1965, ss. 309-317.

LACOHÉE, Hazel, Nina WAKEFORD & Ian PEARSON, "A Social History of the Mobile Telephones With A View of Its Future", *BT Technology Journal*, Cilt 21, Sayı 3, 2003, ss. 203-211.

LAKE, David A., "Theory is Dead, Long Live Theory: The End of the Great Debates and the Rise of Eclecticism in International Relations", *European Journal of International Relations*, Cilt 19, Sayı 3, ss. 567-587.

LANDER, Jack, "The Fascinating Invention of Radio, and How It Can Help You Become A More Successful Inventor", *Inventors' Digest*, Cilt 29, Sayı 5, Mayıs 2013, ss. 39-42.

LAPID, Yosef, "The Third Debate: On the Prospects of International Relations Theory in a Post-Positivist Era", *International Studies Quarterly*, Cilt 33, Sayı 3, Eylül 1989, ss. 235-254.

LASI, Heiner, Peter FETTKE, Thomas FED & Michael HOFFMAN, "Industry 4.0", *Business & Information Systems Engineering*, Cilt 6, Sayı 4, 2014, ss. 239-242.

LAZĂR, Marian, "The Russian Cyber Campain Against Georgia (2008)", *The International Scientific Conference Strategies XXI: The Complex and Dynamic Nature of the Security Environment*, "Carol I" National Defence University Publishinghouse, Bükreş, 22-23 Kasım 2012, ss. 500-506.

LAW, John & John URRY, "Enacting The Social", *Economy and Society*, Cilt 33, Sayı 3, 2004, ss. 390-410.

LAWLER, Andrew, "Rising Cost of Shuttle and Hubble Could Break NASA Budget", *Science*, Cilt 305, Sayı 5692, 24 Eylül 2004, ss. 1882-1883.

LEIVE, David M., "Intelsat in a Changing Telecommunications Environment", *Jurimetrics*, Cilt 25, Sayı 1, Güz 1984, ss. 82-93.

LEVY, Steven A., "INTELSAT: Technology, Politics and the Transformation of a Regime", *International Organization*, Cilt 29, Sayı 3, 1975, ss. 655-680.

LEW, Byron & Bruce CATER, "The Telegraph, Co-ordination of Tramp Shipping, and Growth in World Trade, 1870-1910", *European Review of Economic History*, Cilt 10, Sayı 2, 2006, ss. 147-173.

LIAO, Yongxin, Fernando DESCHAMPS, Eduardo de Fritas Rocha LOURES & Luiz Felipe Pierin RAMOS, "Past, Present and Future of Industry 4.0: A Systemic Literature Review and Research Agenda Proposal", *International Journal of Production Research*, Cilt 55, Sayı 12, 2017, ss. 3609-3629.

LIČER, Matjaž, "The Concept of Aether in Classical Electrodynamics and Einstein's Relativity", *Filozofski Vestnik*, Cilt 34, Sayı 2, 2013, ss. 61-77.

LIN, Herbert S., "Offensive Cyber Operations and the Use of Force", *Journal of National Security Law & Policy*, Cilt 4, Sayı 63, 2010, ss. 63-86.

LITFIN, Karen T., "The Status of the Statistical State: Satellites and the Diffusion of Epistemic Sovereignty", *Global Society*, Cilt 13, Sayı 1, 1999, ss. 95-116.

LIU, Shih-Diing, "The Cyberpolitics of The Governed", *Inter-Asia Cultural Studies*, Cilt 14, Sayı 2, 2013, ss. 252-271.

LIVINGSTON, Steven, "The New Media and Transparency: What Are the Consequences for Diplomacy?", Editör: Evan H. Potter, *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century*, McGill-Quenn's University Press, Londra 2002, ss. 110-127.

LOGUE, Danielle M. & Stewart R. CLEGG, "Wikileaks and The News of the World: The Political Circuitry of Labeling", Journal of Management Inquiry, Cilt 24, Sayı 4, 2015, ss. 394-404.

LYON, David, "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique", *Big Data & Society*, Cilt 1, Sayı 2, Temmuz 2014, ss. 1-13.

MALIK, Monika & Yudhvir SINGH, "A Review: DoS and DDoS Attacks", *International Journal of Computer Science and Mobile Computing*, Cilt 4, Sayı 6, Haziran 2015, ss. 260-265.

MANOR, Ilan & James PAMMENT, "Towards Prestige Mobility? Diplomatic Prestige and Digital Diplomacy", *Cambridge Review of International Affairs*, Cilt 32, Sayı 2, 2019, ss. 93-131.

MANSON, Steve M., "Simplifying Complexity: A Review of Complexity Theory", *Geoforum*, Cilt 32, Sayı 3, Ağustos 2001, ss. 405-414.

MARSON, Stephen M., "A Selective History of Internet Technology and Social Work", *Computers in Human Services*, Cilt 14, Sayı 2, 1997, ss. 35-49.

MASCIOTRA, Chris, "International Law and Cyber Warfare: The Case of Stuxnet", Editör: Jocelyn McGrandle, *Political Science Graduate Student Journal:*

Challenges, Disconnects, and Clashes in Political Studies, Volume III, Concordia University, Department of Political Science, Montréal, Québec 2014, ss. 81-127.

MATHEWS, Jessica T., "The Information Revolution", *Foreign Policy*, Sayı 119, Yaz 2000, ss. 63-65.

MATHEWS, Joseph J., "The Radio and International Relations", *The Southwestern Social Science Quarterly*, Cilt 20, Sayı 2, Eylül 1939, ss. 140-149.

MATTERN, Janice Bially, "Why 'Soft Power' Isn't So Soft: Representational Force and the Sociolinguistic Construction of Attraction in World Politcs", *Millennium: Journal of International Studies*, Cilt 33, Sayı 3, 2005, ss. 583-612.

MAURER, Tim, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities Regarding Cyber-security", Harvard Kennedy School, Belfer Center for Science and International Affairs, *Explorations in Cyber International Relations Discussion Paper Series 2011-11*, Eylül 2011.

MAURUSHAT, Alana, "From Cybercrime to Cyberwar: Security Through Obscurity or Security Through Absurdity?", *Canadian Foreign Policy Journal*, Cilt 19, Sayı 2, ss. 119-122.

MAYER, Maximilian, Mariana CARPES & Ruth KNOBLICH, "The Global Politics of Science and Technology: An Introduction", *The Global Politics of Science and Technology – Vol. 1: Concepts From International Relations and Other Disciplines*, Editörler: Maximilian Mayer, Mariana Carpes & Ruth Knoblich, Springer-Verlag, Berlin Heidelberg 2014, ss. 1-35.

MAZANEC, Brian M., "Why International Order in Cyberspace Is Not Inevitable", *Strategic Studies Quarterly*, Cilt 9, Sayı 2, Yaz 2015, ss. 78-98.

MCCARTHY, Daniel R., "Technology and 'the International' or: How I LEarned to Stop Worrying and Love Determinism", *Millennium: Journal of International Studies*, Cilt 41, Sayı 3, ss. 470-490.

MCDOWELL, Stephen D., Zoheb NENSEY & Philip E. STEINBERG, "Cooperative International Approaches to Network Security: Understanding and Assessing OECD and ITU Efforts to Promote Shared Cybersecurity", Editörler: Jan-Frederik Kremer & Benedikt Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer-Verlag, Berlin Heidelberg 2014, ss. 231-252.

MCGRAW, Gary, "Cyber War is Inevitable (Unless We Build Security In)", *Journal of Strategic Studies*, Cilt 36, Sayı 1, 2013, ss. 109-119.

MCMAHON, J. F., "The Legal Aspects of Outer Space", *The World Today*, Cilt 18, Sayı 8, Ağustos 1962, ss. 328-334.

MEIJER, Hugo L. E., "Reflections on Politics, Strategy and Norms in Outer Space", *Defense & Security Analysis*, Cilt 25, Sayı 1, ss. 89-98.

MELISSEN, Jan & Emilie V. De KEULENAAR, "Critical Digital Diplomacy as a Global Challenge: The South Korean Experience", *Global Policy*, Cilt 8, Sayı 3, Eylül 2017, ss. 294-302.

MISHRA, Bimal Kumar & Apeksha PRAJAPATI, "Cyber Warfare: Worms' Transmission Model", *International Journal of Advanced Science and Technology*, Cilt 63, 2014, ss. 83-94.

MITTERLEHNER, Birgit, "Cyber-Democracy and Cybercrime: Two Sides of the Same Coin", Editörler: Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos, *Cyber-Development, Cyber-Democracy and Cyber-*

Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice, 1. Basım, Springer, New York 2014, ss. 207-230.

MONOSTORI, László, "Cyber-Physical Production Systems: Roots, Expectations, and R&D Challenges", *Procedia CIRP*, Cilt 17, 2014, ss. 9-13.

MORUS, Iwan Rhys, " 'The Nervous System of Britain': Space, time and the Electric Telegraph in the Victorian Age", *The British Journal of the History of Science*, On Time: History, Science and Commemoration, Cilt 33, Sayı 4, Aralık 2000, ss. 455-475.

MOWERY, David C. & Timothy SIMCOE, "Is the Internet a US Invention? – An Economic and Technological History of Computer Networking", *Research Policy*, Cilt 31, Sayı 8-9, Aralık 2002, ss. 1369-1387.

MOWERY, David C., "*Plus ca change*: Industrial R&D in the 'Third Industrial Revolution'", *Industrial and Corporate Change*, Cilt 18, Sayı 1, Şubat 2009, ss. 1-50.

MUELLER, Milton, John MATHIASON & Hans KLEIN, "The Internet and Global Governance: Principles and Norms for a New Regime", *Global Governance*, Cilt 13, Sayı 2, 2007, ss. 237-254.

MUNN, Orson Desaix, S.U. WALES & A.E. BEACH, "Centenary of the Steam Engine: James Watt", *Scientific American*, Cilt 20, Sayı 19, Mayıs 1869, ss. 297-298.

MURRAY, Stuart, "Evolution, Not Revolution: The Digital Divide in American and Australian Contexts", Editörler: Corneliu Bjola & Marcus Holmes, *Digital Diplomacy: Theory and Practice*, 1. Basım, Routledge, New York 2015, ss. 127-144.

NAZARIO, Jose, "Politically Motivated Denial of Service Attacks", Editörler: Christian Czosseck & Kenneth Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare, IOS Pres*, Washington, D.C. 2009, ss. 163-181.

NEUREITER, Norman P., "Science and Technology in Foreign Policy", *Issues in Science and Technology*, Cilt 19, Sayı 2, Kış 2003, ss. 23-26.

NOURIAN, Arash & Stuart MADNICK, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet", *IEEE Transactions on Dependable and Secure Computing*, Cilt 15, Sayı 1, Ocak/Şubat 2018, ss. 2-13.

NYE, Joseph S., Jr., "The Regime Complex for Managing Global Cyber Activities", *Global Commission on Internet Governance Paper Series*, Sayı 1, Mayıs 2014, ss. 5-15.

NWEKE, Eugene N., "Diplomacy in Era of Digital Governance: Theory and Impact", *Information and Knowledge Management*, Cilt 2, Sayı 3, 2012, ss. 22-26

ODISHAW, Hugh, "The International Geophysical Year and World Politics", *Journal of International Affairs*, Cilt 13, Sayı 1, 1959, ss. 47-56.

OLIVER, Eric P., "STUXNET: A Case Study in Cyber Warfare", Editörler: Panayotis A. Yannakogeorgos & Adam B. Lowther, *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, Taylor & Francis, Florida 2014, ss. 127-159.

ÖZKAN, Mehmet, Arzu AL & Serkan YAVUZ, "Uluslararası Politik Ekonomi Açısından Dördüncü Sanayi-Endüstri Devrimi'nin Etkileri ve Türkiye", *Siyasal Bilimler Dergisi*, Cilt 1, Sayı 1, ss. 1-30.

PARK, Sejung, Dahoon CHUNG & Han Woo PARK, "Analytical Framework for Evaluating Digital Diplomacy Using Network Analysis and Topic Modeling: Comparing South Korea and Japan", *Information Processing and Management*, Cilt 56, Sayı 4, 2019, ss. 1468-1483.

PEAGLER, Jordan, "The Stuxnet Attack: A New Form of Warfare and The (In)Applicability of Current International Law", *Arizona Journal of International & Comparative Law*, Cilt 31, Sayı 2, 2014, ss. 399-434.

PELICAN, Luke, "Peacetime Cyber-Espionage: A Dangerous But Necessary Game", *CommLaw Conspectus*, Cilt 20, Sayı 2, 2012, ss. 363-390.

PEOPLES, Columba, "The Securitization of Outer Space: Challenges for Arms Control", *Contemporary Security Policy*, Cilt 32, Sayı 1, ss. 76-98.

PIETERSE, Jan Nederveen, "Leaking Superpower: WikiLeaks and the Contradictions of Democracy", *Third World Quarterly*, Cilt 33, Sayı 10, 2012, ss. 1909-1924.

PIPYROS, Kosmas, Lilian MITROU, Dimitris GRITZALIS & Theodoros APOSTOPOULOS, "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare", *Information & Computer Security*, Cilt 24, Sayı 1, 2016, ss. 38-52.

PRICE, Monroe E., Susan HAAS & Drew MARGOLIN, "New Technologies and International Broadcasting: Reflections on Adaptations and Transformations", *The Annals of the American Academy of Political and Social Science*, Cilt 616, Sayı 1, 2008, ss. 150-172.

POLANSKI, Paul Przemyslaw, "Cyberspace: A New Branch of International Customary Law?", *Computer Law & Security Review*, Cilt 33, Sayı 3, 2017, ss. 371-381.

POPKOVA, Elena G., Yulia V. RAGULINA & Aleksei V. BOGOVIZ, "Fundamental Differences of Transition to Industry 4.0 From Previous Industrial Revolutions", *Industry 4.0: Industrial Revolution of the 21st Century*, Editörler: Elena G. Popkova, Yulia V. Ragulina & Aleksei V. Bogoviz, Springer International Publishing AG, Cham 2019, ss. 21-29.

PRESTON, Charles M., "The Information Revolution: The Emergence of Cyber Power", Editör: Thomas A. Johnson, Power, *National Security, and Transformational Global Events: Challenges Confronting America, China, and Iran,* CRC Press, Florida 2012, ss. 275-348.

QIU, Bin, Hoay Beng GOOI, Yilu LIU & Eng Kiat CHAN, "Internet-Based SCADA Display System", *IEEE Computer Applications in Power*, Cilt 15, Sayı 1, ss. 14-19.

RICHARDSON, John, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield", *Journal of Computer & Information Law*, Cilt 29, Sayı 1, Güz 2011, ss. 1-27.

ROBERTS, Alasdair, "WikiLeaks: The Illusion of Transparency", *International Review of Administrative Sciences*, Cilt 78, Sayı 1, 2012, ss. 116-133.

ROBERTS, Lawrence D., "A Lost Connection: Geostationary Satellite Networks and The International Telecommunication Union", *Berkeley Technology Law Journal*, Cilt 15, Sayı 3, Güz 2000, ss. 1098-1144.

RONEN, Royi, Marian RADU, Corina FEUERSTEIN, Elad YOM-TOV & Mansour AHMADI, "Microsoft Malware Classification Challenge", *CoRR,* abs/1802.10135, 2018, ss. 1-7.

RONNOW, Hans-Henrik, "The Information Revolution II: Satellites and Peace", *The World Today*, Cilt 45, Sayı 6, Ocak 1989, ss. 97-99.

ROSENAU, James N., "Information Technologies and The Skills, Networks, and Structures that Sustain World Affairs", Editörler: James N. Rosenau & J. P. Singh, *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, State University of New York Press, New York 2002, ss. 275-287.

ROWLAND, Jill, Mason RICE & Sujeet SHENOI, "The Anatomy of A Cyber Power", *International Journal of Critical Infrastructure Protection*, Cilt 7, Sayı 1, Mart 2014, ss. 3-11.

RUGGIE, John Gerard, "International Responses to Technology: Concepts and Trends", *International Organization*, Cilt 29, Sayı 3, 1975, ss. 557-583.

SALEEM, Muhammad & Jawad HASSAN, "'Cyber Warfare', The Truth In A Real Case", *Project Report for Information Security Course*, University of Linköping, Sweden, 2009, ss. 1-8.

SALKİN, Ceren, Mahir ÖNER, Alp ÜSTÜNDAĞ & Emre ÇEVİKCAN, "A Conceptual Framework for Industry 4.0", *Industry 4.0: Managing The Digital Transformation*, Editörler: Alp Üstündağ & Emre Çevikcan, Springer, Cham 2018, ss. 3-23.

SANGHVI, H. P. & M. S. DAHIYA, "Cyber Reconnaissance: An Alarm Before Cyber Attack", *International Journal of Computer Applications (0975 – 8887)*, Cilt 63, Sayı 6, Şubat 2013, ss. 36-38.

SAPERSTEIN, Alvin M., "The Prediction of Unpredictability: Applications of the New Paradigm of Chaos in Dynamical Systems to the Old Problem of the Stability of a System of Hostile Nations", Editörler: L. Douglas Kiel & Euel Elliott, *Chaos Theory In The Social Sciences: Foundations and Applications*, The University of Michigan Press, Michigan 1997, ss. 139-163.

SARIKAVAK, Naki, "Siber Terörizmi Anlamak", *Milli Güvenlik ve Askeri Bilimler Akademik Dergisi,* Cilt 2, Sayı 6, İlkbahar 2015, ss. 67-92.

SCHMIDT, Brian C., "Introduction", *International Relations and The First Great Debate*, Editör: Brian C. Schmidt, Routledge, New York 2012, ss. 1-15.

SCHMITT, Michael N., "'Attack' as a Term of Art in International Law: The Cyber Operations Context", Editörler: Christian Czosseck, Rain Ottis & Katharina Ziolkowski, *Proceedings of the 4th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn 2012, ss. 283-293.

SCHMITT, Michael N., "Cyberspace and International Law: The Penumbral Mist of Uncertainity", *Harvard Law Review Forum*, Cilt 126, Sayı 176, 2013, ss. 176-180.

SCHMITT, Michael N., "The Law of Cyber Warfare: Quo Vadis?", *Stanford Law & Policy Review*, Cilt 25, Sayı 2, 2014, ss. 269-299.

SCIENTIFIC AMERICAN, "The First Steam Engine: James Watt", Cilt 6, Sayı 6, Ekim 1850.

SHAHIN, Jamal, "The European Union's Performance in the International Telecommunication Union", *European Integration*, Cilt 33, Sayı 6, Kasım 2011, ss. 683-698.

SHELDON, John B., "Deciphering Cyberpower: Strategic Purpose in Peace and War", *Strategic Studies Quarterly*, Cilt 5, Sayı 2, Yaz 2011, ss. 95-112.

SHOCKLEY, William, "Transistor Physics", *American Scientist*, Cilt 42, Sayı 1, Ocak 1954, ss. 41-72.

SLACK, Chelsey, "Wired yet Disconnected: The Governance of International Cyber Relations", *Global Policy*, Cilt 7, Sayı 1, Şubat 2016, ss. 69-78.

SLOTTEN, Hugh R., "Satellite Communications, Globalization, and the Cold War", *Technology and Culture*, Cilt 43, Sayı 2, Nisan 2002, ss. 315-350.

SMEETS, Max & Jason HEALEY, "Cyber Conflict History", *Tech & Policy Initiative, Working Paper Series 2*, Cyber Conflict Studies Association (CCSA), School of International and Public Affairs (SIPA), 2017, ss. 203-212.

SMITH, Steve, "The Discipline of International Relations: Still An American Social Science?", *British Journal of Politics and International Relations*, Cilt 2, Sayı 3, Ekim 2000, ss. 374-402.

SMYTHE, Dallas W. & J. R. PIERCE, "Communication Satellites", *Science, New Series*, Cilt 135, Sayı 3499, Ocak 1962, ss. 253-255.

SOLIS, Gary D., "Cyber Warfare", *Military Law Review*, Cilt 219, Bahar 2014, ss. 1-52.

SOLMS, Rossouw von & Johan van NIEKERK, "From Information Security to Cyber Security", *Computers & Security*, Cilt 38, 2013, ss. 97-102.

SOLMS, Suné von & Renier van HEERDEN, "The Consequences of Edward Snowden NSA Related Information Disclosures", *Proceedings of The 10th International Conference on Cyber Warfare and Security ICCWS-2015*, University of Venda & The Council for Scientific and Industrial Research, Kruger National Park, Güney Afrika, 24-25 Mart 2015, ss. 358-368.

SOYSAL, Mehmet & Nurten Sinem PAMUK, "Yeni Sanayi Devrimi Endüstri 4.0 Üzerine Bir İnceleme", *Verimlilik Dergisi*, Sayı 1, 2018, ss. 41-66.

SPAFFORD, Eugene H., "Computer Viruses as Artificial Life", *Artificial Life*, Cilt 1, Sayı 3, 1994, ss. 249-265.

SPEAR, Brian, "James Watt: The Steam Engine and The Commercialization of Patents", *World Patent Information*, Cilt 30, Sayı 1, Mart 2008, ss. 53-58.

STĂNCIOIU, Alin, "The Fourth Industrial Revolution 'Industry 4.0'", *Fiabilitate Şi Durabilitate,* Sayı 1, 2017, ss. 74-78.

STEELE, Cherie & Arthur A. STEIN, "Communications Revolutions and International Relations", *Technology, Development, and Democracy: International Comflict and Cooperation in the Information Age*, Editör: Juliann Emmons Allison, SUNY Series in Global Politics, University of New York Press, Albany 2002, ss. 25-53.

STEEN-THORNHAMMAR, Hannes, "VIEWPOINT: Combating Censorship Should be a Foreign Policy Goal", Editörler: Sean S. Costigan & Jake Perry, *Cyberspaces and Global Affairs*, Ashgate Publishing, Farnham 2012, ss. 223-232.

STIENNON, Richard, "A Short History of Cyber Warfare", Editör: James A. Green, *Cyber Warfare: A Multidisciplinary Analysis*, 1. Basım, Routledge, New York 2015, ss. 7-32.

SUBRAMANYA, S. Ravi & Natraj LAKSHMINARASIMHAN, "Computer Viruses", *IEEE Potentials*, Cilt 20, Sayı 4, 2001, ss. 16-19.

SULLIVANA, Julia E. & Dmitriy KAMENSKY, "How Cyber-Attacks In Ukraine Show The Vulnerability of the U.S. Power Grid", The Electric Journal, Cilt 30, Sayı 3, Nisan 2017, ss. 30-35.

SURMACZ, Beata, "New Technologies in Diplomacy", Editörler: Monika Szkarlat & Katarzyna Mojska, *New Technologies as a Factor of International*

Relations, Cambridge Scholars Publishing, 1. Basım, Newcastle upon Tyne 2016, ss. 72-90.

TABANSKY, Lior, "Basic Concepts in Cyber Warfare", *Military and Strategic Affairs*, Cilt 3, Sayı 1, Mayıs 2011, ss. 75-92.

TABANSKY, Lior, "Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy", *8th International Conference on Cyber Conflict (CyCon)*, IEEE, 2016, ss. 51-63.

THOMAS, Sabu, "'Cyber Protests and Electronic Disobedience': Examinig Non-Violence in Times of Cyber Politics", *Gandhi Marg*, Cilt 34, Sayı 3&4, Temmuz-Aralık 2012, ss. 293-306.

TIKK, Eneken, "Ten Rules for Cyber Security", *Survival: Global Politics and Strategy*, Cilt 53, Sayı 3, Haziran-Temmuz 2011, ss. 119-132.

TKACIK, John J., Jr., "Trojan Dragon: China's Cyber Threat", *Backgrounder*, The Heritage Foundation, Sayı 2106, 8 Şubat 2008, ss. 1-12.

TRAUTMAN, Lawrence J. & Peter C. ORMEROD, "Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things", *University of Miami Law Review*, Cilt 72, Sayı 3, 2018, ss. 761-826.

TROXLER, Peter, "Making the Third Industrial Revolution: The Struggle for Polycentric Structures and a New Peer-Production Commons in the FabLab Community", *FabLab of Machines, Makers and Inventions*, Editörler: Julia Walter-Herrmann & Corinne Büching, Transcript Publishers, Bielefeld 2013, ss. 181-198.

TSAGOURIAS, Nicholas, "Cyber Attacks, Self-defence and The Problem of Attribution", *Journal of Conflict & Security Law*, Cilt 17, Sayı 2, 2012, ss. 229-244.

TSAGOURIAS, Nicholas, "The Legal Status of Cyberspace", Editörler: Nicholas Tsagouris & Russell Buchan, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, Cheltenham 2015, ss. 13-29.

UMA, M. & Padmavathi GANAPATHI, "A Survey on Various Cyber Attacks and Their Classification", *International Journal of Network Security*, Cilt 15, Sayı 5, Eylül 2013, ss. 390-396.

URRY, John, "The Complexities of the Global", *Theory, Culture & Society*, Cilt 22, Sayı 5, 2005, ss. 235-254.

ÜNALMIŞ, Ahmet Nafiz & Şafak OĞUZ, "2008 Rusya-Gürcistan Savaşının Vekâlet Savaşı Teorisi Açısından İncelenmesi", *Karadeniz Araştırmaları*, Cilt 16, Sayı 61, 2019, ss. 31-41.

VAISHNAV, Chintan, Nazli CHOUCRI & David CLARK, "Cyber International Relations as an Integrated System", *Environment Systems and Decisions*, Cilt 33, Sayı 4, Kasım 2013, ss. 561-576.

VALERIANO, Brandon & Ryan C. MANESS, "International Relations Theory and Cyber Security: Threat, Conflict, and Ethics in an Emergent Domain", Editörler: Chris Brown & Robyn Eckersley, *The Oxford Handbook of International Political Theory*, 1. Basım, Oxford University Press, New York 2018, ss. 259-272.

VATIS, Michael A., "The Council of Europe Convention on Cybercrime", *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, The National Academic Press, Washington 2010, ss. 207-223

VINCENT, Hannah, Lee WELLS, Pablo TARAZAGA & Jaime CAMELIO, "Trojan Detection and Side-Channel Analyses for Cyber-Security in Cyber-Physical

Manufacturing Systems", *Procedia Manufacturing*, 43rd Proceedings of the North American Manufacturing Research Institution of SME, Cilt 1, 2015, ss. 77-85.

VLEUTEN, Erik van der & Arne KAIJSER, "Networking Europe", *History and Technology*, Cilt 21, Sayı 1, Mart 2005, ss. 21-48.

VOSBURGH, John A., "Where Does Outer Space Begin?", *American Bar Association Journal*, Cilt 56, Sayı 2, Şubat 1970, ss. 134-136.

YAN, Li, "Reforming Internet Governance and the Role of China", *Focus Asia: Perspectives & Analysis*, Institute for Security and Development Policy, Sayı 12, Şubat 2015, ss. 1-9.

YE, Nong, Clark NEWMAN & Toni FARLEY, "A System-Fault-Risk Framework for Cyber Attack Classification", *Information, Knowledge, Systems Management*, Cilt 5, 2006, ss. 135-151.

YU, Shui, Guojun WANG & Wanlei ZHOU, "Modeling Malicious Activities in Cyber Space", *IEEE Network*, Cilt 29, Sayı 6, Kasım-Aralık 2015, ss. 83-87.

ZEADALLY, Sherali, Gregorio MARTINEZ & Han-Chieh CHAO, "Securing Cyberspace in the 21st Century", *Computer*, Cilt 46, Sayı 4, ss. 22-23.

WÆVER, Ole, "Figures of International Thought: Introducing Persons Instead of Paradigms", *The Future of International Relations: Masters in the Making?*, Editörler: Iver B. Neumann & Ole Wæver, Routledge, Londra 2005, ss. 1-40.

WAGNER, Abraham R., "Terrorism and the Internet: Use and Abuse", Editörler: Mark Last & Abraham Kandel, *Fighting Terror In Cyberspace*, World Scientific Publishing, 2005 Singapur, ss. 1-28.

WALDEN, Ian, "Crime and Security in Cyberspce", *Cambridge Review of International Affairs*, Cilt 18, Sayı 1, Nisan 2005, ss. 51-68.

WANGEN, Gaute, "The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism", *Information*, Cilt 6, Sayı 2, 2015, ss. 183-211.

WARNER, Michael, "Cybersecurity: A Pre-history", *Intelligence and National Security*, Cilt 27, Sayı 5, Ekim 2012, ss. 781-799.

WASSERSTROM, Jeffrey N., "Chinese Students and Anti-Japanese Protests, Past and Present", *World Policy Journal*, Cilt 22, Sayı 2, Yaz 2005, ss. 59-65.

WATERMAN, Alan T., "The International Geophysical Year", *American Scientist*, Cilt 44, Sayı 2, Nisan 1956, ss. 130-133.

WEAVER, Nicholas, Vern PAXSON, Stuart STANIFORD & Robert CUNNINGHAM, "A Taxonomy of Computer Worms", *WORM '03: Proceedings of the 2003 ACM Workshop on Rapid Malcode,* CCS03: 10th ACM Conference on Computer and Communications Security, Washington, D.C., Ekim 2003, ss. 11-18.

WEBER, Amalie M., "The Council of Europe's Convention on Cybercrime", *Berkeley Technology Law Journal*, Cilt 18, Sayı 1, Annual Review of Law and Technology, 2003, ss. 425-446.

WEIMANN, Gabriel, "Cyberterrorism: The Sum of All Fears?", *Studies in Conflict & Terrorism*, Cilt 28, Sayı 2, 2005, ss. 129-149.

WEISS, Charles, "Science, Technology and International Relations", *Technology in Society*, Cilt 27, Sayı 3, Ağustos 2005, ss. 295-313.

WEISS, Charles, "How Do Science and Technology Affect International Affairs?", *Minerva*, Cilt 53, Sayı 4, Kasım 2015, ss. 411-430.

WENGER, Andreas, "The Internet and the Changing Face of International Relations and Security", *Information & Security: An International Journal*, Cilt 7, 2001, ss. 5-11.

WHEATLEY, Steven, "The Emergence of New States in International Law: The Insights from Complexity Theory", *Chinese Journal of International Law*, Cilt 15, Sayı 3, ss. 579-606.

WHITTON, John B., "War by Radio", *Foreign Affairs*, Cilt 19, Sayı 3, Nisan 1941, ss. 584-596.

WHITTON, John B., "Radio After The War", *Foreign Affairs*, Cilt 22, Sayı 2, Ocak 1944, ss. 309-317.

WHYTE, Christopher, "Power and Predation in Cyberspace", *Strategic Studies Quarterly*, Cilt 9, Sayı 1, Bahar 2015, ss. 100-118.

WIRTZ, James J., "The Cyber Pearl Harbor", Editörler: Emily O. Goldman & John Arquilla, *Cyber Analogies*, Technical Report: NPS-DA-14-001, Naval Postgraduate School, California 2014, ss. 7-14.

WOLLSCHLAEGER, Martin, Thilo SAUTER & Jürgen JASPERNEITE, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0", *IEEE Industrial Electronics Magazine*, Cilt 11, Sayı 1, Mart 2017, ss. 17-27.

WORTHAM, Anna, "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions

Prohibiting the Threat or Use of Force?", *Federal Communications Law Journal*, Cilt 64, Sayı 3, 2012, ss. 643-660.

WRANGE, Pål, "Intervention in National and Private Cyberspace and International Law", *Stockholm University Research Paper*, Sayı 23, 2017, ss. 1-20.

İnternet Kaynakları:

AARNET, "What Is A Do Sor DDoS Attack?", *https://support.aarnet.edu.au/hc/en-us/articles/115001952194-What-is-a-DoS-or-DDoS-attack-*, (Erişim Tarihi: 20 Nisan 2020).

AL JAZEERA, "WikiLeaks, political hacks and the US election", 23 Ekim 2016, *https://www.aljazeera.com/programmes/listeningpost/2016/10/wikileaks-political-hacks-election-161023102730794.html*, (Erişim Tarihi: 23 Mayıs 2020).

ALBRIGHT, David & Jacqueline SHIRE, "A Witches' Brew? Evaluating Iran's Uranium-Enrichment Progress", Arms Control Association (ACA), *https://www.armscontrol.org/act/2007-11/iran-nuclear-briefs/witches%E2%80%99-brew-evaluating-iran%E2%80%99s-uranium-enrichment-progress*, (Erişim Tarihi: 8 Mayıs 2020).

ALEXANDER, Harriet, "Who is Chelsea Manning and why is she being released from prison?", 17 Mayıs 2017, *https://www.telegraph.co.uk/news/2017/05/17/chelsea-manning-released-prison/*, (Erişim Tarihi: 22 Mayıs 2020).

ASIA PACIFIC COMPUTER EMERGENCY RESPONSE TEAM (APCERT), "About APCERT", *https://www.apcert.org/about/index.html*, (Erişim Tarihi: 1 Nisan 2020).

AVAST, "How Does Malware Work?", *https://www.avast.com/c-malware*, (Erişim Tarihi: 11 Nisan 2020).

AVAST, "Spyware: Detection, Prevention, and Removal", *https://www.avast.com/c-spyware*, (Erişim Tarihi: 16 Nisan 2020).

AVAST, “What Is A Trojan Horse?”, *https://www.avast.com/c-trojan,* (Erişim Tarihi: 14 Nisan 2020).

BALL, James, “NSA's Prism Surveillance Program: How It Works and What It Can Do”, The Guardian, 8 Haziran 2013, *https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google*, (Erişim Tarihi: 25 Mayıs 2020).

BBC NEWS, “WikiLeaks posts video of 'US military killings' in Iraq”, 6 Nisan 2010, *http://news.bbc.co.uk/2/hi/americas/8603938.stm,* (Erişim Tarihi: 21 Mayıs 2020).

BBC NEWS, “UN Sanctions Against Iran”, 26 Temmuz 2010, *https://www.bbc.com/news/world-middle-east-10768146*, (Erişim Tarihi: 8 Mayıs 2020).

BBC NEWS, “Wikileaks: Iraq war logs 'reveal truth about conflict'”, 23 Ekim 2010, *https://www.bbc.com/news/world-middle-east-11612731,* (Erişim Tarihi: 21 Mayıs 2020).

BBC NEWS, “Stuxnet 'Hit' Iran Nuclear Plans”, 22 Kasım 2010, *https://www.bbc.com/news/technology-11809827,* (Erişim Tarihi: 9 Mayıs 2020).

BBC NEWS, “Wikileaks Diplomatic Cables Release 'Attack on World'”, 29 Kasım 2010, *https://www.bbc.com/news/world-us-canada-11868838*, (Erişim Tarihi: 23 Mayıs 2020).

BBC NEWS, “Ukraine Protests After Yanukovych EU Deal Rejection”, 30 Kasım 2013, *https://www.bbc.com/news/world-europe-25162563,* (Erişim Tarihi: 12 Mayıs 2020).

BBC NEWS, “Wikileaks US diplomatic cables: Key issues”, 3 Aralık 2010, *https://www.bbc.com/news/world-us-canada-11858990*, (Erişim Tarihi: 21 Mayıs 2020).

BBC NEWS, “Swiss banker linked to Wikileaks is found guilty”, 19 Ocak 2011, *https://www.bbc.com/news/business-12231036,* (Erişim Tarihi: 20 Mayıs 2020).

BBC NEWS, “Saab Wins $4.5bn Brazil Fighter Jet Contract”, 19 Aralık 2013, *https://www.bbc.com/news/business-25441231*, (Erişim Tarihi: 26 Mayıs 2020).

BBC NEWS, “Putin: Russia Helped Yanukovych to Flee Ukraine”, 24 Ekim 2014, *https://www.bbc.com/news/world-europe-29761799*, (Erişim Tarihi: 12 Mayıs 2020).

BBC NEWS, “Snowden NSA: Germany drops Merkel phone-tapping probe”, 12 Haziran 2015, *https://www.bbc.com/news/world-europe-33106044*, (Erişim Tarihi: 25 Mayıs 2020).

BBC NEWS, “Iran's Key Nuclear Sites”, 14 Temmuz 2015, *https://www.bbc.com/news/world-middle-east-11927720*, (Erişim Tarihi: 8 Mayıs 2020).

BBC NEWS, “Ukraine Power Cut 'Was Cyber-Attack'”, 11 Ocak 2017, *https://www.bbc.com/news/technology-38573074*, (Erişim Tarihi: 13 Mayıs 2020).

BBC NEWS, “Chelsea Manning: Wikileaks source celebrates 'first steps of freedom'”, 17 Mayıs 2017, *https://www.bbc.com/news/world-us-canada-39947602,* (Erişim Tarihi: 22 Mayıs 2020).

BBC NEWS, “Israel Admits Striking Suspected Syrian Nuclear Reactor in 2007”, 21 Mart 2018, *https://www.bbc.com/news/world-middle-east-43481803,* (Erişim Tarihi: 26 Şubat 2020).

BBC NEWS, “Julian Assange: A timeline of Wikileaks founder's case”, 19 Kasım 2019, *https://www.bbc.com/news/world-europe-11949341,* (Erişim Tarihi: 22 Mayıs 2020).

BBC NEWS, “Gambling on Credit Cards to be Banned”, 14 Ocak 2020, *https://www.bbc.com/news/business-51103006*, (Erişim Tarihi: 21 Mart 2020).

BBC NEWS, “DDoS: Man Who Sold Website Defences Pleads Guilty to Attacks”, 21 Ocak 2020, *https://www.bbc.com/news/technology-51189386*, (Erişim Tarihi: 20 Mart 2020).

BEAUCHAMP, Zack, “WikiLeaks just tried to justify its behavior this year in a bizarre Election Day statement”, 8 Kasım 2016, *https://www.vox.com/world/2016/11/8/13563750/wikileaks-2016-election-statement,* (Erişim Tarihi: 23 Mayıs 2020).

BINGHAMTON UNIVERSITY, THE STATE UNIVERSITY OF NEW YORK, “Publications: Gulbenkian Commision on the Restructuring of the Social Sciences”, *https://www.binghamton.edu/fbc/publications/gulbenkian.html#members,* (Erişim Tarihi: 18 Kasım 2019).

BİLGİ VE İLETİŞİM TEKNOLOJİLERİ KURUMU, “Uluslararası Telekomünikasyon Birliği-ITU”, *https://www.btk.gov.tr/itu*, (Erişim Tarihi: 2 Nisan 2020).

BRANDON, John, “Inside the NSA’s Secret Utah Data Center”, Fox News, 11 Haziran 2013, *https://www.foxnews.com/tech/inside-the-nsas-secret-utah-data-center*, (Erişim Tarihi: 25 Mayıs 2020).

BRENT, Laura, "NATO's Role In Cyberspace", NATO Review, 12 Şubat 2019, *https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html*, (Erişim Tarihi: 4 Mayıs 2020).

BROWN, Gary D. & Owen W. TULLOS, "On The Spectrum of Cyberspace Operations", Small Wars Journal, 11 Aralık 2012, *https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations*, (Erişim Tarihi: 10 Nisan 2020).

CANVAS NETWORK, *https://www.canvas.net/*, (Erişim Tarihi: 17 Kasım 2019).

CARROLL, Rory, "Welcome to Utah, the NSA's Desert Home For Eavesdropping On America", The Guardian, 14 Haziran 2013, *https://www.theguardian.com/world/2013/jun/14/nsa-utah-data-facility*, (Erişim Tarihi: 25 Mayıs 2020).

CBS NEWS, "Opposition Signs Deal Aiming to End Ukraine's Deadly Crisis", 21 Şubat 2014, *https://www.cbsnews.com/news/ukraine-protest-leaders-sign-deal-to-end-crisis-in-kiev/*, (Erişim Tarihi: 12 Mayıs 2020).

CERTIFICATIONKITS, "CCNA Security: Common Network Attacks", *https://www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-describe-security-threats/ccna-security-common-network-attacks/*, (Erişim Tarihi: 19 Nisan 2020).

CERTIFIED MANAGEMENT CONSULTANT AND STRATEGIC ADVISOR WITH THE TECHNOLYTICS INSTITUTE, "Cyber Espionage Targets Sensitive Data", SIP Trunking Report, 29 Aralık 2008, *http://sip-trunking.tmcnet.com/topics/security/articles/47927-cyber-espionage-targets-sensitive-data.htm*, (Erişim Tarihi: 20 Şubat 2020).

CHEN, Te-Ping, “Snowden Alleges U.S. Hacking in China”, The Wall Street Journal, 23 Haziran 2013, *https://www.wsj.com/articles/SB10001424127887324577904578562483284884530*, (Erişim Tarihi: 25 Mayıs 2020).

CIA, “The World Factbook: Estonia”, *https://www.cia.gov/library/publications/the-world-factbook/geos/en.html*, (Erişim Tarihi: 1 Mayıs 2020).

CISCO, “What Is Malware?”, *https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html*, (Erişim Tarihi: 11 Nisan 2020).

CISCO, “What Is The Difference: Viruses, Worms, Trojans, and Bots?”, *https://tools.cisco.com/security/center/resources/virus_differences*, (Erişim Tarihi: 12 Nisan 2020).

CISCO CERTIFIED SECURITY PROFESSIONAL CERTIFICATION (CCSP), “The Four Primary Types of Network Attacks”, *http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+I+Introduction+to+Network+Security/Chapter+1+Understanding+Network+Security+Threats/The+Four+Primary+Types+of+Network+Attack/*, (Erişim Tarihi: 19 Nisan 2020).

CISCO NETWORKING ACADEMY (NUM), “Keeping The Network Safe: Vulnerabilities and Network Attacks”, *http://cisco.num.edu.mn/CCNA_R&S1/course/module11/11.2.2.2/11.2.2.2.html*, (Erişim Tarihi: 18 Nisan 2020).

COUNCIL OF EUROPE, “Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime”, Treaty Office, *https://www.coe.int/en/web/conventions/full-list/-*

/conventions/treaty/185/signatures?p_auth=EyR6nySC, (Erişim Tarihi: 30 Mart 2020).

COUNCIL OF EUROPE, "Convention on Cybercrime", No: 185, 23 Kasım 2001, Budapeşte, *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185*, (Erişim Tarihi: 23 Şubat 2020).

COUNCIL OF EUROPE, "Details of Treaty No. 185: Convention on Cybercrime", Treaty Office, *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185*, (Erişim Tarihi: 30 Mart 2020).

COUNCIL OF EUROPE, "Details of Treaty No.201: Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse", *https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/201*, (Erişim Tarihi: 28 Mart 2020).

COUNCIL ON FOREIGN RELATIONS, "Titan Rain", Ağustos 2005, *https://www.cfr.org/interactive/cyber-operations/titan-rain*, (Erişim Tarihi: 29 Nisan 2020).

COURSERA, *https://www.coursera.org/*, (Erişim Tarihi: 17 Kasım 2019).

COWLEY, Matthew, "Saab Gets $4.5 Billion Contract From Brazil for 36 Fighter Jets", The Wall Street Journal, 18 Aralık 2013, *https://www.wsj.com/articles/brazil-to-announce-fighter-jet-contract-results-1387388061*, (Erişim Tarihi: 26 Mayıs 2020).

DAVENPORT, Kelsey, "UN Security Council Resolutions on Iran", Arms Control Association (ACA), Ağustos 2017, *https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran#res1696*, (Erişim Tarihi: 8 Mayıs 2020).

DAVIES, Nick & David LEIGH, "Afghanistan war logs: Massive leak of secret files exposes truth of occupation", The Guardian, 25 Temmuz 2010, *https://www.theguardian.com/world/2010/jul/25/afghanistan-war-logs-military-leaks*, (Erişim Tarihi: 21 Mayıs 2020).

DAVIES, Nick, Jonathan STEELE & David LEIGH, "Iraq war logs: secret files show how US ignored torture", The Guardian, 22 Ekim 2010, *https://www.theguardian.com/world/2010/oct/22/iraq-war-logs-military-leaks*, (Erişim Tarihi: 21 Mayıs 2020).

DENNING, Dorothy, "Cyberwar: How Chinese Hackers Became A Major Threat To The U.S.", Newsweek, 10 Mayıs 2017, *https://www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-678378*, (Erişim Tarihi: 29 Nisan 2020).

DEUTSCHE WELLE TÜRKÇE (DW), "İnternetin Kontrolü ABD'de", *https://www.dw.com/tr/internetin-kontrol%C3%BC-abdde/a-2523743*, (Erişim Tarihi: 3 Nisan 2020).

DER SPIEGEL, "Explosive Leaks Provide Image of War from Those Fighting It", 25 Temmuz 2010, *https://www.spiegel.de/international/world/afghanistan-explosive-leaks-provide-image-of-war-a-708314.html*, (Erişim Tarihi: 21 Mayıs 2020).

DER SPIEGEL, "Greatest Data Leak in US Military History", 22 Ekim 2010, *https://www.spiegel.de/international/world/the-wikileaks-iraq-war-logs-greatest-data-leak-in-us-military-history-a-724845.html*, (Erişim Tarihi: 21 Mayıs 2020).

DER SPIEGEL, "How America Views the World", 29 Kasım 2010, *https://www.spiegel.de/international/world/state-department-secrets-revealed-how-america-views-the-world-a-732819.html*, (Erişim Tarihi: 21 Mayıs 2020).

DOUGLAS, Susan J., *Inventing American Broadcasting: 1899-1922*, 3. Basım, The John Hopkins University Press, Maryland 1989, *https://archive.org/details/InventingAmericaBroadcasting1899-1922*, (Erişim Tarihi: 18 Aralık 2018).

EARN, "The History of the EARN Network", *https://earn-history.net/*, (Erişim Tarihi: 15 Şubat 2020).

edX, *https://www.edx.org/,* (Erişim Tarihi: 17 Kasım 2019).

ENCYCLOPÆDIA BRITANNICA, "Espionage: International Relations", *https://www.britannica.com/topic/espionage*, (Erişim Tarihi: 21 Şubat 2020).

EUROPEAN FACTORIES OF THE FUTURE RESEARCH ASSOCIATION (EFFRA), "Factories of the Future", *https://www.effra.eu/factories-future*, (Erişim Tarihi: 5 Temmuz 2019).

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), "About ENISA", *https://www.enisa.europa.eu/about-enisa*, (Erişim Tarihi: 1 Nisan 2020).

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA), "Botnets", *https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets*, (Erişim Tarihi: 15 Nisan 2020).

FEDERAL BUREAU OF INVESTIGATION, INTERNET CRIME COMPLAINT CENTER, "2018 Internet Crime Report", *https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2018-internet-crime-report*, (Erişim Tarihi: 24 Şubat 2020).

FERRAN, Lee & Akiko FUJITA, "Edward Snowden Claims NSA Documents Show U.S. Hacks China: Report", ABC News, 12 Haziran 2013,

https://abcnews.go.com/Blotter/edward-snowden-claims-evidence-shows-us-hacks-china/story?id=19384436, (Erişim Tarihi: 25 Mayıs 2020).

GCHQ, "Mission Overview",
https://www.gchq.gov.uk/section/mission/overview, (Erişim Tarihi: 25 Mayıs 2020).

GEERS, Kenneth, *Strategic Cyber Security*, NATO Cooperative Cyber Defence Centre of Excellence (NATO-CCDCOE) Publication, Tallinn Haziran 211.; Center For Strategic & International Studies (CSIS), "Significant Cyber Incidents", *https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents*, (Erişim Tarihi: 28 Nisan 2020).

GERMANY TRADE & INVEST (GTAI), "The High-Tech Strategy", *https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Why-germany/industrie-4-0-why-germany-policy,t=the-hightech strategy,did=1798576.html*, (Erişim Tarihi: 5 Temmuz 2019).

GHOSH, Iman, "This is the Crippling Cost of Cybercrime on Corporations", World Economic Forum, 7 Kasım 2019, *https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/*, (Erişim Tarihi: 24 Şubat 2020).

GOTSIRIDZE, Andria, "The Cyber Dimension of the 2008 Russia-Georgia War", Georgian Foundation For Strategic And International Studies, 9 Ağustos 2019, *https://www.gfsis.org/blog/view/970*, (Erişim Tarihi: 6 Mayıs 2020).

GOVERNMENT OFFICE FOR SCIENCE AND DEPARTMENT FOR BUSINESS, INNOVATION & SKILLS, "Future of Manufacturing", *https://www.gov.uk/government/collections/future-of-manufacturing*, (Erişim Tarihi: 5 Temmuz 2019).

GREENBERG, Andy, "Visa, MasterCard Move To Choke WikiLeaks", Forbes, 7 Aralık 2010, *https://www.forbes.com/sites/andygreenberg/2010/12/07/visa-mastercard-move-to-choke-wikileaks/#7821c00f2cad*, (Erişim Tarihi: 23 Mayıs 2020).

GREENBERG, Andy, "WikiLeaks Announces 'The Detainee Policies': A History Of U.S. Post-9/11 Military Prisoners In Leaked Documents", Forbes, 25 Ekim 2012, *https://www.forbes.com/sites/andygreenberg/2012/10/25/wikileaks-announces-the-detainee-policies-a-history-of-american-military-detainees-in-leaked-documents/#3778d3841455*, (Erişim Tarihi: 20 Mayıs 2020).

GREENBERG, Andy, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired, 22 Ağustos 2018, *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*, (Erişim Tarihi: 13 Mayıs 2020).

GREENBERG, Andy, "Meet the Mad Scientist Who Wrote the Book on How to Hunt Hackers", Wired, 12 Ekim 2019, *https://www.wired.com/story/meet-the-mad-scientist-who-wrote-the-book-on-how-to-hunt-hackers/*, (Erişim Tarihi: 22 Nisan 2020).

GREENWALD, Glenn, "NSA Collecting Phone Records of Millions of Verizon Customers Daily", The Guardian, 6 Haziran 2013, *https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order*, (Erişim Tarihi: 25 Mayıs 2020).

GREENWALD, Glenn & Ewen MACASKILL, "NSA Prism Program Taps In To User Data of Apple, Google and Others", The Guardian, 7 Haziran 2013, *https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data*, (Erişim Tarihi: 25 Mayıs 2020).

GROLL, Elias, "Did Russia Knock Out Ukraine's Power Grid?", Foreign Policy, 8 Ocak 2016, *https://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/*, (Erişim Tarihi: 13 Mayıs 2020).

GRYTSENKO, Oksana, "Ukrainian Protesters Flood Kiev After President Pulls Out of EU Deal", 24 Kasım 2013, *https://www.theguardian.com/world/2013/nov/24/ukraine-protesters-yanukovych-aborts-eu-deal-russia*, (Erişim Tarihi: 12 Mayıs 2020).

HAFEZI, Parisa, "Iran Admits Cyber Attack On Nuclear Plants", Reuters, 29 Kasım 2010, *https://www.reuters.com/article/us-iran/iran-admits-cyber-attack-on-nuclear-plants-idUSTRE6AS4MU20101129*, (Erişim Tarihi: 9 Mayıs 2020).

HARVARD ONLINE COURSES, *https://online-learning.harvard.edu/*, (Erişim Tarihi: 17 Kasım 2019).

HM GOVERNMENT, "National Cyber Security Strategy 2016-2021", 1 Kasım 2016, *https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021*, (Erişim Tarihi: 9 Şubat 2020).

HOPKINS, Nick & Jake MORRIS, "UK Firm's Surveillance Kit 'Used to Crush Uganda Opposition'", BBC News, 15 Ekim 2015, *https://www.bbc.com/news/uk-34529237*, (Erişim Tarihi: 2 Mart 2020).

HOSENBALL, Mark, "WikiLeaks faces U.S. probes into its 2016 election role and CIA leaks: sources", Reuters, 7 Aralık 2017, *https://www.reuters.com/article/us-usa-trump-russia-wikileaks/wikileaks-faces-u-s-probes-into-its-2016-election-role-and-cia-leaks-sources-idUSKBN1E12J2*, (Erişim Tarihi: 23 Mayıs 2020).

ILYUSHINA, Mary, "Edward Snowden Requests A Three-Year Extension of Russian Residency", CNN, 17 Nisan 2020,

https://edition.cnn.com/2020/04/16/europe/edward-snowden-russian-residency-intl/index.html, (Erişim Tarihi: 26 Mayıs 2020).

INTELSAT, "Intelsat History", *http://www.intelsat.com/about-us/history/*, (Erişim Tarihi: 18 Şubat 2019).

INTERNET SOCIETY (IS), "About Internet Society", *https://www.internetsociety.org/about-internet-society/*, (Erişim Tarihi: 1 Nisan 2020).

INTERNATIONAL TELECOMMUNICATION UNION (ITU), "About GCA", *https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx*, (Erişim Tarihi: 2 Nisan 2020).

INTERNATIONAL TELECOMMUNICATION UNION (ITU), "About International Telecommunication Union (ITU)", *https://www.itu.int/en/Pages/default.aspx*, (Erişim Tarihi: 1 Nisan 2020).

INTERNATIONAL TELECOMMUNICATION UNION (ITU), "Discover ITU's History", *https://www.itu.int/en/history/Pages/DiscoverITUsHistory.aspx*, (Erişim Tarihi: 2 Nisan 2020).

INTERNATIONAL TELECOMMUNICATION UNION (ITU), "World Summit on the Information Society: Geneva 2003-Tunis 2005", *https://www.itu.int/net/wsis/index.html*, (Erişim Tarihi: 3 Nisan 2020).

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN), "About ICANN", *https://www.icann.org/resources/pages/welcome-2012-02-25-en*, (Erişim Tarihi: 1 Nisan 2020).

INTERNET CORPORATION FOR ASSİGNED NAMES AND NUMBERS (ICANN), "Beginner's Guide to Participating In ICANN",

https://www.icann.org/resources/pages/beginners-guides-2012-03-06-en, (Erişim Tarihi: 2 Nisan 2020).

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN), "ICANN's Multistakeholder Model", *https://www.icann.org/community#groups*, (Erişim Tarihi: 2 Nisan 2020).

INTERNET GOVERNANCE FORUM (IGF), "About IGF FAQs", *https://www.intgovforum.org/multilingual/content/about-igf-faqs*, (Erişim Tarihi: 3 Nisan 2020).

INTERNET WORLD STATS, "Internet Usage Statistics: World Internet Users and 2020 Population Statas", *https://www.internetworldstats.com/stats.htm,* (Erişim Tarihi: 2 Nisan 2020).

İTÜ BİLGİ İŞLEM DAİRE BAŞKANLIĞI (İTÜBİDB), "DNS (Domain Name System - Etki Alanı Ad Sunucusu)", *https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/dns-(domain-name-system---etki-alan%C4%B1-ad-sunucusu),* (Erişim Tarihi: 3 Nisan 2020).

İTÜ BİLGİ İŞLEM DAİRE BAŞKANLIĞI (İTÜBİDB), "Virüs, Solucan ve Truva Atı", *https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1*, (Erişim Tarihi: 13 Nisan 2020).

JARVIS, Jacob, "Julian Assange's Extradition Hearing Delayed to at Least September, WikiLeaks Announces", Newsweek, 5 Nisan 2020, *https://www.newsweek.com/julian-assange-extradition-delayed-september-wikileaks-1501780,* (Erişim Tarihi: 22 Mayıs 2020).

JARVIS, Jeff, "The Debate Continues On Edward Snowden: Hero or Traitor", The Guardian, 26 Kasım 2013, *https://www.theguardian.com/commentisfree/2013/nov/26/edward-snowden-hero-traitor-debate*, (Erişim Tarihi: 26 Mayıs 2020).

KACHKACHISVILI, David, "NATO'dan Rusya'ya 'Gürcistan'ın Egemenliğine Saygı Duy' Çağrısı", Anadolu Ajansı, 3 Ekim 2019, *https://www.aa.com.tr/tr/dunya/natodan-rusyaya-gurcistanin-egemenligine-saygi-duy-cagrisi/1601543*, (Erişim Tarihi: 5 Mayıs 2020).

KASPERSKY, "Malware & Computer Virus Facts & FAQs", *https://www.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs*, (Erişim Tarihi: 12 Nisan 2020).

KASPERKY, "Sıfır Gün Güvenlik Açığı Saldırısı Nedir?", *https://www.kaspersky.com.tr/resource-center/definitions/zero-day-exploit*, (Erişim Tarihi: 9 Mayıs 2020).

KASPERSKY, "Types of Malwares", *https://www.kaspersky.com/resource-center/threats/malware-protection*, (Erişim Tarihi: 11 Nisan 2020).

KASPERSKY, "What Is A Computer Virus or A Computer Worm?", *https://www.kaspersky.com/resource-center/threats/viruses-worms*, (Erişim Tarihi: 13 Nisan 2020).

KASPERSKY, "What Is A Trojan Virus?", *https://www.kaspersky.com/resource-center/threats/trojans*, (Erişim Tarihi: 14 Nisan 2020).

KASPERSKY, "What Is Spyware? - Definition", *https://www.kaspersky.com/resource-center/threats/spyware*, (Erişim Tarihi: 16 Nisan 2020).

KERR, Donald E., *Propagation of Short Radio Waves*, Dover Publications, Inc., New York 1965, *https://archive.org/details/PropagationOfShortRadioWaves/page/n15*, (Erişim Tarihi: 17 Aralık 2018), ss. 1-8.

KHAN ACADEMY, *http://www.khanacademy.org.tr/*, (Erişim Tarihi: 17 Kasım 2019).

KIELY, Cecilia, "Titans of Technology", *PassageMakers*, 1 Eylül 2018, *https://www.passagemaker.com/trawler-news/titans-of-technology*, (Erişim Tarihi: 16 Aralık 2018), ss. 44-48.

KIRKUP, James & Christopher HOPE, "BNP membership list leaked onto internet", The Telegraph, 18 Kasım 2008, *https://www.telegraph.co.uk/news/politics/3479612/BNP-membership-list-leaked-onto-internet.html*, (Erişim Tarihi: 20 Mayıs 2020).

KONOŃCZUK, Wojciech, "Ukraine Withdraws From Signing The Association Agreement in Vilnius: The Motives and Implications", Centre For Eastern Studies (OSW), 27 Kasım 2013, *https://www.osw.waw.pl/en/publikacje/analyses/2013-11-27/ukraine-withdraws-signing-association-agreement-vilnius-motives-and*, (Erişim Tarihi: 12 Mayıs 2020).

KRAMER, Andrew E. & Michael R. GORDON, "Ukraine Reports Russian Invasion on a New Front", The New York Times, 27 Ağustos 2014, *https://www.nytimes.com/2014/08/28/world/europe/ukraine-russia-novoazovsk-crimea.html?auth=login-google*, (Erişim Tarihi: 12 Mayıs 2020).

LAMB, Brian, "Clifford Stoll Röportajı", C-SPAN, 13 Ekim 1989, *https://www.c-span.org/video/?10122-1/the-cuckoos-egg*, (Erişim Tarihi: 22 Nisan 2020).

LANDLER, Mark & John MARKOFF, "In Estonia, What May Be The First War In Cyberspace", 28 Mayıs 2007, *https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html*, (Erişim Tarihi: 1 Mayıs 2020).

LAPSLEY, Phil, "Phone Phreaks: What We Can Learn From the First Network Hackers?", The Advanced Computing Systems Association (USENIX), *https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/phone-phreaks-what-we-can-learn-first*, (Erişim Tarihi: 22 Nisan 2020).

LICHTENSTEIN, Jesse, "Digital Diplomacy", The New York Times Magazine, 16 Temmuz 2010, *https://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html*, (Erişim Tarihi: 14 Mart 2020).

LEVER, Rob, "Snowden Revelations Costly For US Tech Firms, Study Says", 9 Haziran 2015, *https://phys.org/news/2015-06-snowden-revelations-costly-tech-firms.html*, (Erişim Tarihi: 26 Mayıs 2020).

MACASKILL, Ewen, "Hillary Clinton Attacks Release of US Embassy Cables", The Guardian, 29 Kasım 2010, *https://www.theguardian.com/world/2010/nov/29/clinton-reacts-us-embassy-cables*, (Erişim Tarihi: 23 Mayıs 2020).

MACASKILL, Ewen, "WikiLeaks website pulled by Amazon after US political pressure", The Guardian, 2 Aralık 2010, *https://www.theguardian.com/media/2010/dec/01/wikileaks-website-cables-servers-amazon*, (Erişim Tarihi: 23 Mayıs 2020).

MACASKILL, Ewen, Julian BORGER, Nick HOPKINS, Nick DAVIES & James BALL, "GCHQ Taps Fibre-Optic Cables For Secret Access To World's Communications", The Guardian, 21 Haziran 2013, *https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa*, (Erişim Tarihi: 25 Mayıs 2020).

MALIK, Nesrine, "Why is the left blinkered to claims about Assange and sexual assault?", The Guardian, 15 Nisan 2019, *https://www.theguardian.com/commentisfree/2019/apr/15/left-blinkered-claims-julian-assange-sexual-assault*, (Erişim Tarihi: 22 Mayıs 2020).

MALTHUS, Thomas Robert, *An Essay On The Principle of Population; or, A View of Its Past and Present Effects On Human Happiness; With An Inquiry Into Our Prospects Respecting The Future Removal or Mitigation of The Evils Which It Occasions*, Cilt 1, 5. Basım, John Murray, Albemarle-Street, Londra 1817, *https://archive.org/details/essayonprinciple01maltuoft*, (Erişim Tarihi: 01 Temmuz 2019).

MARKOFF, John & Andrew E. KARMER, "In Shift, U.S. Talks to Russia on Internet Security", The New York Times, 12 Aralık 2009, *https://www.nytimes.com/2009/12/13/science/13cyber.html*, (Erişim Tarihi: 30 Mart 2020).

MARTINS, Constantino Pereira, "What is Cyberpolitics?", Nova University of Lisbon, Lizbon Aralık 2013, *https://www.academia.edu/7554424/What_is_Cyberpoliticsi*, (Erişim Tarihi: 12 Mart 2020).

MAZETTI, Mark & Helene COOPER, "U.S. Confirms Israeli Strikes Hit Syrian Target Last Week", The New York Times, 12 Eylül 2007, *https://www.nytimes.com/2007/09/12/world/middleeast/12syria.html*, (Erişim Tarihi: 26 Şubat 2020).

MCFADDEN, Christopher, "A Chronological History of Social Media", Interesting Engineering, 16 Ekim 2018, *https://interestingengineering.com/a-chronological-history-of-social-media*, (Erişim Tarihi: 15 Mart 2020).

MCGUINNES, Damien, "How A Cyber Attack Transformed Estonia", BBC News, 27 Nisan 2017, *https://www.bbc.com/news/39655415*, (Erişim Tarihi: 1 Mayıs 2020).

MILLIGAN, Ellen, "Julian Assange's Extradition Trial Delayed by Coronavirus", Bloomberg, 27 Nisan 2020, *https://www.bloomberg.com/news/articles/2020-04-27/wikileak-s-assange-extradition-trial-delayed-by-coronavirus*, (Erişim Tarihi: 22 Mayıs 2020).

MINISTRY FOR THE ECONOMY AND FINANCE, "New Industrial France: Building France's Industrial Future", *https://www.economie.gouv.fr/files/files/PDF/web-dp-indus-ang.pdf*, (Erişim Tarihi: 5 Temmuz 2019).

MINISTRY OF EDUCATION, CULTURE, SPORTS, SCIENCE AND TECHNOLOGY-JAPAN, "Science and Technology Basic Plan", *http://www.mext.go.jp/en/policy/science_technology/lawandplan/title01/detail01/1375311.htm*, (Erişim Tarihi: 6 Temmuz 2019).

MINUTELLA, David, Jeremy CIOARA & Heather STEVENSON, "CCENT Exam Prep: General Network Security", Pearson It Certification, *https://www.pearsonitcertification.com/articles/article.aspx?p=1151753&seqNum=2*, (Erişim Tarihi: 19 Nisan 2020).

MIT OPEN COURSEWARE, *https://ocw.mit.edu/index.htm*, (Erişim Tarihi: 17 Kasım 2019).

MOOC (Massive Open Online Courses), *http://mooc.org/*, (Erişim Tarihi: 17 Kasım 2019).

MUTH, John, "WikiLeaks and The 2016 Presidential Election", Towson University Journal of International Affairs, 8 Kasım 2016,

https://wp.towson.edu/iajournal/2016/11/08/wikileaks-and-the-2016-presidential-election/, (Erişim Tarihi: 23 Mayıs 2020).

NAKASHIMA, Ellen, Greg MILLER & Julie TATE, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say", The Washington Post, 19 Haziran 2012, *https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html*, (Erişim Tarihi: 10 Mayıs 2020).

NATIONAL CYBER SECURITY CENTRE (NCSC), "Denial of Service (DoS) Guidance", *https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection*, (Erişim Tarihi: 20 Nisan 2020).

NATIONAL RESEARCH FOUNDATION PRIME MINISTER'S OFFICE SINGAPORE, "RIE2020 Plan", *https://www.nrf.gov.sg/rie2020*, (Erişim Tarihi: 6 Temmuz 2019).

NATO, "Kuzey Atlantik Antlaşması", 4 Nisan 1949, Washington, D. C., *https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=tr*, (Erişim Tarihi: 4 Mayıs 2020).

NATO, "Bucharest Summit Declaration", 3 Nisan 2008, *https://www.nato.int/cps/en/natolive/official_texts_8443.htm*, (Erişim Tarihi: 5 Mayıs 2020).

NATO, "Joint Statement of the NATO-Ukraine Commission", Wales Summit, 4-5 Eylül 2014, *https://www.nato.int/cps/en/natohq/news_112695.htm?selectedLocale=en*, (Erişim Tarihi: 4 Mayıs 2020).

NATO, “Cyber Defence Pledge”, Warsaw Summit, 8-9 Temmuz 2016, *https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en*, (Erişim Tarihi: 4 Mayıs 2020).

NORTH, Anna, “The rape allegation against Julian Assange, explained”, 13 Mayıs 2019, *https://www.vox.com/identities/2019/4/12/18306901/julian-assange-arrest-wikileaks-rape-sweden-embassy*, (Erişim Tarihi: 22 Mayıs 2020).

NORTON, “Emerging Threats: What Are Denial of Service (DoS) Attacks? DoS Attacks Explained”, *https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html*, (Erişim Tarihi: 20 Nisan 2020).

NORTON, “What Are Bots?”, *https://us.norton.com/internetsecurity-malware-what-are-bots.html*, (Erişim Tarihi: 15 Nisan 2020).

NORTON, “What Is A Computer Virus?”, *https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html*, (Erişim Tarihi: 12 Nisan 2020).

NORTON, “What Is Malware and How Can We Prevent It?”, *https://us.norton.com/internetsecurity-malware.html*, (Erişim Tarihi: 11 Nisan 2020).

NORTON, “What Is A Trojan? Is It A Virus or Is It Malware?”, *https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html*, (Erişim Tarihi: 14 Nisan 2020).

NORTON-TAYLOR, Richard, “Titan Rain – How Chinese Hackers Targeted Whitehall”, The Guardian, 5 Eylül 2007, *https://www.theguardian.com/technology/2007/sep/04/news.internet*, (Erişim Tarihi: 29 Nisan 2020).

NSA, DOMESTIC SURVEILLANCE DIRECTORATE, "Utah Data Center", *https://nsa.gov1.info/utah-data-center/index.html*, (Erişim Tarihi: 25 Mayıs 2020).

OFFICE OF SCIENCE AND TECHNOLOGY POLICY, EXECUTIVE OFFICE OF THE PRESIDENT, "Report To The President On Ensuring American Leadership In Advanced Manufacturing", Haziran 2011, *https://www.manufacturing.gov/sites/default/files/2018-01/pcast-advanced-manufacturing-june2011.pdf*, (Erişim Tarihi: 5 Temmuz 2019).

OPEN SOCIETY FOUNDATIONS, "Understanding Ukraine's Euromaidan Protests", Mayıs 2019, *https://www.opensocietyfoundations.org/explainers/understanding-ukraines-euromaidan-protests*, (Erişim Tarihi: 12 Mayıs 2020).

OTTE, Jedidajah, "Release Julian Assange, says woman who had two children with him while in embassy", The Guardian, 12 Nisan 2020, *https://www.theguardian.com/media/2020/apr/12/release-julian-assange-says-woman-who-had-two-children-with-him-while-in-embassy*, (Erişim Tarihi: 22 Mayıs 2020).

OUR WORLD IN DATA, "Internet Users by World Region", *https://ourworldindata.org/*, (Erişim Tarihi: 16 Şubat 2020).

PAGANINI, Pierluigi, "Cybercrime Statistics in 2019", Security Affairs, 18 Ocak 2020, *https://securityaffairs.co/wordpress/96531/cyber-crime/cybercrime-statistics-in-2019.html*, (Erişim Tarihi: 24 Şubat 2020).

PANDA, "What Do Computer Worms Do?", *https://www.pandasecurity.com/en/security-info/worm/*, (Erişim Tarihi: 13 Nisan 2020).

PANDA, "What Is A Botnet?",

https://www.pandasecurity.com/mediacenter/security/what-is-a-botnet/, (Erişim Tarihi: 15 Nisan 2020).

PHRASEE, "The History of Social Media: A Timeline", *https://phrasee.co/the-history-of-social-media-a-timeline/*, (Erişim Tarihi: 15 Mart 2020).

POLITYUK, Pavel, "Ukraine Power Distributor Plans Cyber Defense System for $20 Million", Reuters, 6 Şubat 2018, *https://www.reuters.com/article/us-ukraine-cyber-ukrenergo/ukraine-power-distributor-plans-cyber-defense-system-for-20-million-idUSKBN1FQ1TD,* (Erişim Tarihi: 13 Mayıs 2020).

POMFRET, James, "Ex-CIA man's snooping claims raise alarm bells in Hong Kong", Reuters, 13 Haziran 2013, *https://www.reuters.com/article/us-usa-security-hongkong/ex-cia-mans-snooping-claims-raise-alarm-bells-in-hong-kong-idUSBRE95C08920130613*, (Erişim Tarihi: 25 Mayıs 2020).

REGAN, Joseph, "What Is A Trojan Horse? Is It Malware or Virus?", AVG, 10 Aralik 2019, *https://www.avg.com/en/signal/what-is-a-trojan*, (Erişim Tarihi: 14 Nisan 2020).

REGAN, Joseph, "What Is Spyware?", *https://www.avg.com/en/signal/what-is-spyware*, (Erişim Tarihi: 16 Nisan 2020).

REPUBLIC OF TURKEY, MINISTRY OF TRANSPORT MARITIME AFFAIRS AND COMMUNICATIONS, "2016-2019 National Cyber Security Strategy", *https://www.uab.gov.tr/siber-guvenlik*, 2016, (Erişim Tarihi: 9 Şubat 2020).

REUTERS, "China Tightens Web Screws After Xinjiang Riot", 6 Temmuz 2009, *https://www.reuters.com/article/us-china-xinjiang-internet/china-tightens-*

web-screws-after-xinjiang-riot-idUSTRE5651K420090706, (Erişim Tarihi: 21 Mart 2020).

REUTERS, "Coronavirus forces delay in U.S. extradition case against Assange", 27 Nisan 2020, *https://www.reuters.com/article/us-britain-assange/coronavirus-forces-delay-in-us-extradition-case-against-assange-idUSKCN22913S*, (Erişim Tarihi: 22 Mayıs 2020).

RICE, Xan, "The Looting of Kenya", The Guardian, 31 Ağustos 2007, *https://www.theguardian.com/world/2007/aug/31/kenya.topstories3*, (Erişim Tarihi: 20 Mayıs 2020).

SAHIMI, Mohammad, Pirouz MOJTAHED-ZADEH & Kaveh L. AFRASIABI, "Energy: Iran Needs Nuclear Power", The New York Times, 14 Ekim 2003, *https://www.nytimes.com/2003/10/14/opinion/IHT-energy-iran-needs-nuclear-power.html*, (Erişim Tarihi: 8 Mayıs 2020).

SCHOR, Elena, "Wikileaks posts a hack of Palin's e-mail account", The Guradian, 18 Eylül 2008, *https://www.theguardian.com/world/deadlineusa/2008/sep/17/uselections2008.sarahpalin*, (Erişim Tarihi: 20 Mayıs 2020).

SHANE, Scott & Andrew W. LEHREN, "Leaked Cables Offer Raw Look at U.S. Diplomacy", 28 Kasım 2010, *https://www.nytimes.com/2010/11/29/world/29cables.html*, (Erişim Tarihi: 21 Mayıs 2020).

SIMPSON, John, "Russia's Crimea Plan Detailed, Secret and Successful", BBC News, 19 Mart 2014, *https://www.bbc.com/news/world-europe-26644082*, (Erişim Tarihi: 12 Mayıs 2020).

SMITH, David, "WikiLeaks emails: what they revealed about the Clinton campaign's mechanics", The Guardian, 6 Kasım 2016, *https://www.theguardian.com/us-news/2016/nov/06/wikileaks-emails-hillary-clinton-campaign-john-podesta*, (Erişim Tarihi: 23 Mayıs 2020).

SPENDER, Tom, "Wikileaks: Is Julian Assange interfering in US election?", BBC News, 19 Ekim 2016, *https://www.bbc.com/news/uk-37704393*, (Erişim Tarihi: 23 Mayıs 2020).

SPUTNIK NEWS, "Iran installs Reactor Cap at Bushehr NPP", 23 Kasım 2010, *https://sputniknews.com/world/20101123161458962/*, (Erişim Tarihi: 8 Mayıs 2020).

SPUTNIK TÜRKİYE, "Snowden Rusya'dan Oturma İzninin Uzatılmasını Talep Etti", 17 Nisan 2020, *https://tr.sputniknews.com/politika/202004171041850401-edward-snowden-rusyadan-oturma-izninin-uzatilmasini-talep-etti/*, (Erişim Tarihi: 26 Mayıs 2020).

STANFORD ONLINE, *https://online.stanford.edu/*, (Erişim Tarihi: 17 Kasım 2019).

STIEBER, Josh & Ethan MCCORD, "US Soldiers from Wikileaks 'Collateral Murder' Video Apologize", Global Policy Forum, 19 Nisan 2010, *https://www.globalpolicy.org/invasion-and-war/atrocities-and-criminal-homicides-/48984-us-soldiers-from-wikileaks-collateral-murder-video-apologize.html*, (Erişim Tarihi: 21 Mayıs 2020).

SUK-YEE, Jung, "Innovation in Manufacturing 3.0 Stretegy Needs Better Focus with Clearer Direction", *BussinessKorea*, 19 Kasım 2015, *http://www.businesskorea.co.kr/news/articleView.html?idxno=13060*, (Erişim Tarihi: 5 Temmuz 2019).

T.C. CUMHURBAŞKANLIĞI, STRATEJİ VE BÜTÇE BAŞKANLIĞI, BİLGİ VE İLETİŞİM TEKNOLOJİLERİ DAİRESİ, "Dünya Bilgi Toplumu Zirvesi", *http://www.bilgitoplumu.gov.tr/uluslararasi-calismalar/dunya-bilgi-toplumu-zirvesi/*, (Erişim Tarihi: 3 Nisan 2020).

T.C. RESMİ GAZETE, "Birleşmiş Milletler Aııdlaşması", Kanun No: 4801, Sayı: 6092, 24 Ağustos 1945, s. 9238, *https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf*, (Erişim Tarihi: 26 Mart 2020).

T.C. MİLLİ GÜVENLİK KURULU GENEL SEKRETERLİĞİ, "Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı (Uluslararası Siber Güvenlik Hukuku)", *https://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakkinda-tallinn-el-kitabi-uluslararasi-siber-guvenlik-hukuku*, (Erişim Tarihi: 31 Mart 2020).

TDK, "Türk Dil Kurumu Sözlükleri", *https://sozluk.gov.tr/*, (Erişim Tarihi: 22 Nisan 2020).

THE CALOUSTE GULBENKIAN FOUNDATION, *https://gulbenkian.pt/en/*, (Erişim Tarihi: 18 Kasım 2019).

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, "Security Tip (ST04-015): Understanding Denial-of-Service-Attacks", *https://www.us-cert.gov/ncas/tips/ST04-015*, (Erişim Tarihi: 20 Nisan 2020).

THE GOVERNMENT OF JAPAN, "Cybersecurity Strategy", 4 Eylül 2015, *https://www.mofa.go.jp/policy/page18e_000015.html*, (Erişim Tarihi: 9 Şubat 2020).

THE GUARDIAN, "Chinese Human Rights Activist Liu Hiaobo Sentenced to 11 Years in Jail", 25 Aralık 2009,

https://www.theguardian.com/world/2009/dec/25/china-jails-liu-xiaobo, (Erişim Tarihi: 20 Mart 2020).

THE GUARDIAN, "WikiLeaks embassy cables: the key points at a glance", 7 Kasım 2010, *https://www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points,* (Erişim Tarihi: 21 Mayıs 2020).

THE GUARDIAN, "The NSA Files: Verizon Forced to Hand Over Telephone Data – Full Court Ruling", 6 Haziran 2013, *https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order*, (Erişim Tarihi: 25 Mayıs 2020).

THE INDEPENDENT, "Online Gamblers will no Longer be Allowed to Use Credit Cards for Betting", 14 Ocak 2020, *https://www.independent.co.uk/news/uk/home-news/gambling-credit-cards-betting-ban-regulation-commission-deposits-a9282751.html*, (Erişim Tarihi: 21 Mart 2020).

THE INTERNET GOVERNANCE FORUM (IGF), "About the IGF", *https://www.intgovforum.org/multilingual/tags/about*, (Erişim Tarihi: 1 Nisan 2020).

THE MANDIANT REPORT, "APT1: Exposing One of China's Cyber Espionage Units", Mart 2013, *https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf,* (Erişim Tarihi: 29 Nisan 2020).

THE NATIONS ONLINE PROJECT, "Independent States of the World", *https://www.nationsonline.org/oneworld/states.htm*, (Erişim Tarihi: 6 Mart 2020).

THE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (NATO CCD-CoE), "About Us", *https://ccdcoe.org/about-us/,* (Erişim Tarihi: 1 Nisan 2020).

THE NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE (NATO StratCom COE), "Hybrid Threats: 2007 Cyber Attacks on Estonia", ss. 51-69, *https://www.stratcomcoe.org/hybrid-threats-2007-cyber-attacks-estonia*, (Erişim Tarihi: 3 Mayıs 2020).

THE NEW YORK TIMES, "Focus on Internet Imams as Al Qaueda Recruiters", 31 Aralık 2009, *https://www.nytimes.com/2010/01/01/us/01imam.html*, (Erişim Tarihi: 20 Mart 2020).

THE NEW YORK TIMES, "Iran Disrupts Internet Service Ahead of Protests", 10 Şubat 2010, *https://www.nytimes.com/2010/02/11/world/middleeast/11tehran.html*, (Erişim Tarihi: 21 Mart 2020).

THE NEW YORK TIMES, "View Is Bleaker Than Official Portrayal of War in Afghanistan", 25 Temmuz 2010, *https://www.nytimes.com/2010/07/26/world/asia/26warlogs.html*, (Erişim Tarihi: 21 Mayıs 2020).

THE NEW YORK TIMES, "The Iraq Archive: The Strands of a War", 22 Ekim 2010, *https://www.nytimes.com/2010/10/23/world/middleeast/23intro.html*, (Erişim Tarihi: 21 Mayıs 2020).

THE SHANGHAI COOPERATION ORGANISATION (SCO), "Documents", *http://eng.sectsco.org/documents/*, (Erişim Tarihi: 28 Mart 2020).

THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA, "Internet Plus", *http://english.gov.cn/2016special/internetplus/*, (Erişim Tarihi: 5 Temmuz 2019).

THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA, "Made in China 2025", *http://english.gov.cn/2016special/madeinchina2025/*, (Erişim Tarihi: 5 Temmuz 2019).

THE STATE OF SECURITY, "3 Types of Network Attacks to Watch Out For", *https://www.tripwire.com/state-of-security/vulnerability-management/3-types-of-network-attacks/*, (Erişim Tarihi: 19 Nisan 2020).

THE WORLD WIDE WEB CONSORTIUM (W3C), "The World Wide Web Security FAQ: Securing Against Denial of Service Attacks", *https://www.w3.org/Security/Faq/wwwsf6.html*, (Erişim Tarihi: 20 Nisan 2020).

THORNBURGH, Nathan, "Inside The Chinese Hack Attack", Time, 25 Ağustos 2005, *http://content.time.com/time/nation/article/0,8599,1098371,00.html*, (Erişim Tarihi: 29 Nisan 2020).

TOYNBEE, Arnold, *Lectures on the Industrial Revolution of the 18th Century in England: Popular Adresses, Notes and Other Fragments*, 4. Basım, Longmans, Green and Co., Londra 1894, *https://archive.org/details/LecturesOnTheIndustrialRevolutionOfThe18thCenturyInEngland*, (Erişim Tarihi: 20 Şubat 2019).

TRAYNOR, Ian & Oksana GRYTSENKO, "Ukraine Suspends Talks On EU Trade Pact As Putin Wins Tug of War", The Guardian, 21 Kasım 2013, *https://www.theguardian.com/world/2013/nov/21/ukraine-suspends-preparations-eu-trade-pact*, (Erişim Tarihi: 12 Mayıs 2020).

TÜRK DİL KURUMU, Büyük Türkçe Sözlük, *http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5bb924c4932158.33702650*, (Erişim Tarihi: 7 Ekim 2018).

UDACITY, *https://www.udacity.com/*, (Erişim Tarihi: 17 Kasım 2019).

UDEMY, *https://www.udemy.com/*, (Erişim Tarihi: 17 Kasım 2019).

UNITED NATIONS, "The Right To Privacy In The Digital Age", A/RES/68/167, 18 Aralık 2013, *https://undocs.org/en/A/RES/68/167*, (Erişim Tarihi: 26 Mayıs 2020).

UNITED NATIONS, OFFICE FOR DISARMAMENT AFFAIRS, "Developments In The Field of Information and Telecommunications In The Context of International Security", *https://www.un.org/disarmament/ict-security/*, (Erişim Tarihi: 24 Nisan 2020).

UNITED NATIONS, OFFICE FOR OUTER SPACE AFFAIRS, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies", *https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html*, (Erişim Tarihi: 4 Şubat 2020).

USA WASHINGTON PRINTING OFFICE, *International Radio Telegraph Convention of Berlin: 1906 And Propositions For The International Radio Telegraph Conference of London*, Washington 1912, *https://archive.org/details/internationalrad00interich*, (Erişim Tarihi: 17 Aralık 2018).

U.S. DEPARTMENT OF HOMELAND SECURITY, "Cybersecurity Strategy", 15 Mayıs 2018, *https://www.dhs.gov/publication/dhs-cybersecurity-strategy*, (Erişim Tarihi: 9 Şubat 2020).

U.S. DEPARTMENT OF STATE, "The United States and Ukraine Hold Third Cyber Dialogue", Media Note, Office of the Spokesperson, 3 Mart 2020, *https://www.state.gov/the-united-states-and-ukraine-hold-third-cyber-dialogue/*, (Erişim Tarihi: 13 Mayıs 2020).

UNITED STATES NAVAL ACADEMY (USNA), "Cyber Operations: Phases of A Cyber Attack / Cyber-Recon", *https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l32/lec.html*, (Erişim Tarihi: 18 Nisan 2020).

UNIVERSITY OF CENTRAL ARKANSAS, INFORMATION TECHNOLOGY, "What Is Malware?", *https://uca.edu/it/knowledgebase-legacy/what-is-malware/*, (Erişim Tarihi: 11 Nisan 2020).

UNIVERSITY OF CENTRAL ARKANSAS, INFORMATION TECHNOLOGY, "What Is Spyware?", *https://uca.edu/it/knowledgebase-legacy/what-is-spyware/*, (Erişim Tarihi: 16 Nisan 2020).

VIRUSBLOKADA, *http://anti-virus.by/en/index.shtml*, (Erişim Tarihi: 9 Mayıs 2020).

VOICE OF AMERICA (VOA), "Iran's New Nuclear Power Plant to be Closely Monitored", 31 Ekim 2010, *https://www.voanews.com/world-news/middle-east-dont-use/irans-new-nuclear-power-plant-be-closely-monitored*, (Erişim Tarihi: 8 Mayıs 2020).

WIKILEAKS, "Côte d'Ivoire: Toxic Waste Scandal Unfolds", 8 Eylül 2006, *https://wikileaks.org/plusd/cables/06ABIDJAN1004_a.html*, (Erişim Tarihi: 20 Mayıs 2020).

WIKILEAKS, "The looting of Kenya under President Moi", 30 Ağustos 2007, *https://wikileaks.org/wiki/The_looting_of_Kenya_under_President_Moi*, (Erişim Tarihi: 20 Mayıs 2020).

WIKILEAKS, "Camp Delta Standard Operating Procedure", 7 Kasım 2007, *https://wikileaks.org/wiki/Camp_Delta_Standard_Operating_Procedure*, (Erişim Tarihi: 20 Mayıs 2020).

WIKILEAKS, “Church of Scientology's 'Operating Thetan' documents leaked online”, 26 Mart 2008, *https://wikileaks.org/wiki/Church_of_Scientology%27s_%27Operating_Thetan%27_documents_leaked_online*, (Erişim Tarihi: 20 Mayıs 2020).

WIKILEAKS, “Bank Julius Baer USA tax evasion trusts”, 16 Nisan 2008, *https://www.wikileaks.org/wiki/Bank_Julius_Baer_USA_tax_evasion_trusts*, (Erişim Tarihi: 20 Mayıs 2020).

WIKILEAKS, “VP contender Sarah Palin hacked”, 17 Eylül 2008, *https://wikileaks.org/wiki/VP_contender_Sarah_Palin_hacked*, (Erişim Tarihi: 20 Mayıs 2020).

WIKILEAKS, “Financial collapse: Confidential exposure analysis of 205 companies each owing above EUR45M to Icelandic bank Kaupthing, 26 Sep 2008”, 30 Temmuz 2009, *https://wikileaks.org/wiki/Financial_collapse:_Confidential_exposure_analysis_of_205_companies_each_owing_above_EUR45M_to_Icelandic_bank_Kaupthing,_26_Sep_2008*, (Erişim Tarihi: 20 Mayıs 2020).

WIKILEAKS, “British National Party membership list and other information, 15 Apr 2009”, 20 Ekim 2009, *https://wikileaks.org/wiki/British_National_Party_membership_list_and_other_information,_15_Apr_2009*, (Erişim Tarihi: 20 Mayıs 2020).

WIKILEAKS, “The Afghan War Diary”, 25 Temmuz 2010, *https://wikileaks.org/afg/*, (Erişim Tarihi: 21 Mayıs 2020).

WIKILEAKS, “The Iraq War Logs”, 22 Ekim 2010, *https://wikileaks.org/irq/*, (Erişim Tarihi: 21 Mayıs 2020).

WIKILEAKS, “Cablegate: 250,000 US Embassy Diplomatic Cables”, 28 Kasım 2010, https://www.wikileaks.org/Cablegate-250-000-US-Embassy.html, (Erişim Tarihi: 21 Mayıs 2020).

WIKILEAKS, “What is WikiLeaks”, 3 Kasım 2015, *https://wikileaks.org/What-is-WikiLeaks.html*, (Erişim Tarihi: 20 Mayıs 2020).

WIKILEAKS, “Collateral Murder”, 5 Nisan 2020, *https://collateralmurder.wikileaks.org/*, (Erişim Tarihi: 21 Mayıs 2020).

YUHAS, Alan, “Russian Propaganda Over Crimea and the Ukraine: How Does It Work?”, The Guardian, 17 Mart 2014, *https://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media*, (Erişim Tarihi: 12 Mayıs 2020).

ZENESYS, “Social Media Evolution”, 24 Haziran 2019, *https://www.zenesys.com/infographics/social-media-evolution*, (Erişim Tarihi: 15 Mart 2020).

ZETTER, Kim, “Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid”, Wired, 3 Mart 2016, *https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/*, (Erişim Tarihi: 13 Mayıs 2020).

WAKEFIELD, Jane, “Wikileaks' Struggle to Stay Online”, BBC News, 7 Aralık 2010, *https://www.bbc.com/news/technology-11928899*, (Erişim Tarihi: 23 Mayıs 2020).

WARREN, Lydia, “Inside America's $1.9 Billion Data Mine: How All Your Pivate Details Will Soon Be Stored In This Vast NSA Nerve Center In Utah Valley”, Daily Mail, 7 Haziran 2013, *https://www.dailymail.co.uk/news/article-2337420/Utah-Data-Center-The-million-square-foot-Utah-data-mining-facility-built-NSA.html*, (Erişim Tarihi: 25 Mayıs 2020).

WATT, Nicholas & Rowena MASON, "Angela Merkel phone-bugging claims are result of Snowden leaks, MP claims", The Guardian, 24 Ekim 2013, *https://www.theguardian.com/world/2013/oct/24/angela-merkel-bugging-snowden-leaks-mp*, (Erişim Tarihi: 25 Mayıs 2020).

WE ARE SOCIAL INC., "Digital 2020: Global Digital Overview", *https://wearesocial.com/digital-2020,* (Erişim Tarihi: 17 Şubat 2020).

WEINBERGER, Sharon, "How Israel Spoofed Syria's Air Defense System", Wired, *https://www.wired.com/2007/10/how-israel-spoo/,* (Erişim Tarihi: 26 Şubat 2020).

WOLFRAM, Stephen, "Computating A Theory Of All Knowledge", TED2010, Şubat 2010, *https://www.ted.com/talks/stephen_wolfram_computing_a_theory_of_all_knowledge,* (Erişim Tarihi: 24 Kasım 2019).

WORLD SUMMIT ON THE INFORMATION SOCIETY, "Tunis Agenda For The Information Society", WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 Kasım 2005, *https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html*, (Erişim Tarihi: 3 Nisan 2020).

Belgeseller:

GIBNEY, Alex (Yapımcı & Yönetmen), *Zero Days*, [Belgesel], Magnolia Pictures, ABD 2016.

POITRAS, Laura, Mathide BONNEFOY & Dirk WILUTZKY (Yapımcılar), Laura Poitras (Yönetmen), *Citizenfour* [Belgesel], Radius-TWC, ABD 2014.

POITRAS, Laura, Yoni GOLIJOV & Brenda COUGHLIN (Yapımcılar), Laura Poitras (Yönetmen), *Risk*, [Belgesel], Neon, ABD 2016.