T. C.
ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

SİBER UZAY GÜVENLİĞİ: ULUSAL GÜVENLİK VE ULUSLARARASI GÜVENLİĞE ETKİLERİ

(YÜKSEK LİSANS TEZİ)

Zafer YENER

BURSA - 2013

U.Ü. S.B.E.
ULUSLARARSI İLİŞKİLER
ANABİLİM DALI

SİBER UZAY GÜVENLİĞİ: ULUSAL GÜVENLİK VE ULUSLARARASI GÜVENLİĞE ETKİLERİ
(YÜKSEK LİSANS TEZİ)

Zafer YENER

BURSA
2013



T. C.
ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER

SİBER UZAY GÜVENLİĞİ: ULUSAL GÜVENLİK VE ULUSLARARASI GÜVENLİĞE ETKİLERİ

(YÜKSEK LİSANS TEZİ)

Zafer YENER

BURSA - 2013

T. C.
ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

SİBER UZAY GÜVENLİĞİ: ULUSAL GÜVENLİK VE ULUSLARARASI GÜVENLİĞE ETKİLERİ

(YÜKSEK LİSANS TEZİ)

Zafer YENER

Danışman:
Doç.Dr. Barış ÖZDAL

BURSA – 2013

T. C.
ULUDAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Uluslararası İlişkiler Anabilim Dalı'nda 701016006 numaralı Zafer YENER'in hazırladığı "Siber Uzay Güvenliği: Ulusal Güvenlik ve Uluslararası Güvenliğe Etkileri" konulu Yüksek Lisans Çalışması ile ilgili tez savunma sınavı, 31/01/ 2013 günü 11⁰⁰ - 12³⁰ saatleri arasında yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin/çalışmasının BAŞARILI (başarılı/~~başarısız~~) olduğuna OYBİRLİĞİ (oybirliği/~~oy çokluğu~~) ile karar verilmiştir.

Üye (~~Tez Danışmanı ve~~ Sınav Komisyonu Başkanı)
Akademik Unvanı, Adı Soyadı
Üniversitesi
Prof. Dr. Tayyar ARI

Üye
Akademik Unvanı, Adı Soyadı
Üniversitesi
Tez Danışmanı
Doç. Dr. Sabri ÇAĞAR

Üye
Akademik Unvanı, Adı Soyadı
Üniversitesi
Prof. Dr. Ö. Göksel IŞIYAR

Üye
Akademik Unvanı, Adı Soyadı
Üniversitesi
Prof. Dr. Kamuran REGBER

Üye
Akademik Unvanı, Adı Soyadı
Üniversitesi
Yrd. Doç. Dr. Sertaç SERDAR

31/01/ 2013

ÖZET

Yazar Adı ve Soyadı : Zafer YENER

Üniversite : Uludağ Üniversitesi

Enstitü : Sosyal Bilimler Enstitüsü

Anabilim Dalı : Uluslararası İlişkiler

Bilim Dalı :

Tezin Niteliği : Yüksek Lisans Tezi

Sayfa Sayısı : XIV + 146

Mezuniyet Tarihi : …. / …. / 20……..

Tez Danışmanı : Doç.Dr. Barış ÖZDAL

SİBER UZAY GÜVENLİĞİ: ULUSAL GÜVENLİK VE ULUSLARARASI GÜVENLİĞE ETKİLERİ

Tezimi siber uzay güvenliğinin ulus güvenliği ve uluslararası güvenliğe etkileri olacağı savından hareketle şekillendirdim. Tezimde siber uzay güvenliğinin ulus güvenliği ve uluslararası güvenliğe olan etkileri üzerinde durdum. Tezimi hazırlarken konu ile ilgili makaleler, kitaplar ve devletlerin hazırlamış olduğu ulusal raporlar ile uluslararası kurumlar tarafından hazırlanan raporlardan yararlandım. Tezimi üç ana bölümden oluşturdum. Birinci bölümde tezim ile ilgili kavramlar ve teorik alt yapıdan bahsettim. Mevcut güvenlik teorilerinin siber uzay güvenliğini açıklamada yetersiz kalacağı sonucuna vardım. İkinci bölümde siber uzay güvenliğinin ulus güvenliğine olan etkileri üzerinde durdum. Ulusların güvenlik alanındaki çalışmalarının siber uzay içerisinde yetersiz kaldığı ve bu anlamda yeni güvenlik oluşumlarına ihtiyaç duyulduğu sonucuna varılmıştır. Üçüncü ve son bölümde ise siber güvenlik alanında uluslararası yapılanmanın mutlaka bir üst organizasyon ile oluşturulması gerektiği ve ulusların bu organizasyondan bilgi alış verişi ile alınacak kararlara da mutlaka uyulması gerektiği sonucuna ulaşılmıştır. Türkiye'nin siber güvenlik alanında ki mevcut durumu, yapmış olduğu çalışmalar ile uluslararası yapılanmada yer alma çalışmaları üzerinde durulmuştur. Özellikle Türkiye'nin siber güvenliğini kimin sağlayacağı noktasında, Türk Silahlı Kuvvetleri'nin siber güvenlik alanındaki mevcut bilgi birikimi ve yapılanması hakkında bilgi verilmiştir.

Anahtar Sözcükler: Siber uzay güvenliği, siber güvenlik, siber savaş

ABSTRACT

Name and Surname	: Zafer YENER
University	: Uludağ University
Institution	: Social Science Institution
Field	:International Relations
Branch	:
Degree Awarded	: Master
Page Number	: XIV + 146
Degree Date	: …. / …. / 20…….
Supervisor (s)	:

CYBER SPACE SECURITY: THE EFFECTS OF NATIONAL SECURITY AND INTERNATIONAL SECURITY

I have shaped my thesis starting from the state that cyber space security would have effects on national security and international security. In my thesis, I have dwelled on the effects of cyber space security on national security and international security. While preparing my thesis, I have benefited from articles related to the subject, books and national reports prepared by governments and reports prepared by international agencies. I have constituted my thesis from three parts. In the first part, I mentioned concepts related to my thesis and theoretic substructure. I concluded that current security theories would be insufficient in explaining cyber space security. In the second part, I dwelled on the effects of cyber space security on national security. In the second part, it is concluded that the security works of nations are insufficient in cyber space and in this sense, new security constitutions are needed. In the third and last part, it is concluded that international structuring in cyber security must be constituted with a high organization and nations must obey the decisions taken by the high organization. The current position of Turkey in cyber security, committed works in this field and taking part woks in the international structuring are dwelled on. Especially on the point of who is going to provide cyber security of Turkey, the information about the current accumulation of knowledge and structuring of Turkish Armed Forces is given.

Keywords: Cyberspace security, cyber security, cyberwar

ÖNSÖZ

2010 yılında Milli Güvenlik Kurulunun siber güvenlik alanında almış olduğu kararları okuduktan sonra tezimi bu konu ile ilgili yazmaya karar verdim. MGK kararlarında siber güvenlik ile ilgili Türkiye de bir üst yapılanmaya ihtiyaç olduğu belirtilmekteydi. Bu yapılanma ile ilgili Türk Silahlı Kuvvetleri'nin öncü olması gerektiği kanaatinden hareketle bu alanda daha önce yapılmayan bir çalışmaya imza attım. Bu çalışmamı hazırlamamda bana her zaman cesaret veren tez danışmanım Doç. Dr. Barış ÖZDAL'a bu vesile ile teşekkür etmek istiyorum. Tezi hazırlarken bana her anlamda yardımcı olan sevgili eşim Canan YENER' e ayrıca teşekkür etmek istiyorum. Beni her zaman varlıkları ile mutlu eden oğullarım Yiğit ve Yağız'a tez çalışmam sebebi ile fazla vakit ayıramadım, onları çok sevdiğimi bu vesile ile tekrar belirtmek istiyorum. Tezimi bu topraklar için gözünü hiç kırpmadan canını feda eden şehitlerimize ithaf ediyorum.

Zafer YENER

ÖZGEÇMİŞ			
Adı, Soyadı	Zafer		YENER
Doğum Yeri ve Yılı	Samsun		02.02.1982
Bildiği Yabancı Diller	İngilizce		
ve Düzeyi	İyi		
Eğitim Durumu	**Başlama - Bitirme Yılı**		**Kurum Adı**
Lise	1996	2000	Maltepe Askeri Lisesi
Lisans	2000	2004	Kara Harp Okulu
Yüksek Lisans	2010	2012	Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı
Doktora			
Çalıştığı Kurum (lar)	**Başlama - Ayrılma Yılı**		**Çalışılan Kurumun Adı**
1.	2004	-	Türk Silahlı Kuvvetleri
2.			
3.			
Üye Olduğu Bilimsel ve Mesleki Kuruluşlar			
Katıldığı Proje ve Toplantılar			
Yayınlar:			
Diğer:			
İletişim (e-posta):	z.yener19@gmail.com		
Tarih **İmza** **Adı Soyadı**			Zafer YENER

İÇİNDEKİLER

Sayfa

TEZ ONAY SAYFASI IV
ÖZET V
ABSTRACT VI
ÖNSÖZ VII
ÖZGEÇMİŞ VIII
İÇİNDEKİLER IX
KISALTMALAR XII
ŞEKİLLER XIV
GİRİŞ 1

BİRİNCİ BÖLÜM

(KAVRAMSAL VE TEORİK ÇERÇEVE)

1. Kavramsal Çerçeve……3
   1.1. Kötücül Yazılımlar…….. 4
      1.1.1. Sayısal Bilgi Savaşı (Digital Data WarfareDDW)……...4
      1.1.2. Sayısal Bilgi Savaşı Araçları ……...4
         1.1.2.1. Bilgisayar Virüsleri…….. 5
         1.1.2.2. Solucanlar (Worm)……...5
         1.1.2.3. Truva Atı (Trojan)……5
         1.1.2.4. Mantık Bombaları…… 6
         1.1.2.5. Tuzak Kapıları, Arka Kapılar (Backdoor)…….. 6
         1.1.2.6. Chipping……...6
         1.1.2.7. Kaydedici (Keylogger)……6
         1.1.2.8. Hizmetin Engellenmesi Saldırıları (DoS/DDoS)……. 6
         1.1.2.9. Botnet……... 8
      1.1.3. Siber……9
      1.1.4. Siber Uzay Kavramı……10
      1.1.5. Bilgi Savaşı…….. 11
      1.1.6. Siber Savaş……...12
      1.1.7. Siber Terörizm…… 12
      1.1.8. Asimetrik Savaş……... 13
      1.1.9. Bilgi Güvenliği…….13

1.1.10. Siber Güvenlik…… 14
1.1.11. Siber Suç…….. 15
1.1.12. Siber İstihbarat…… 15
1.1.13. Bilişim Suçları……..15
1.2. Teorik Çerçeve……... 16
1.2.1. Uluslararası İlişkilerde Çatışmayı Açıklayan Teoriler Kapsamında; Küreselleşme ve Siber Uzay Güvenliği……... 22
1.2.2. Uluslararası İlişkilerde İşbirliğini Açıklayan Teoriler: Siber Güvenlik ve Kopenhag Okulu……. 25
1.2.3. Güvenlikleştirme Teorisi……..29
1.2.4. Siber Güvenlik Modelleri…….33
1.2.4.1. Yüksek Güvenlikleştirme…….33
1.2.4.2. Günlük Güvenlik Uygulamaları……...34

İKİNCİ BÖLÜM

(SİBER UZAY GÜVENLİĞİNİN ULUS GÜVENLİĞİNE ETKİLERİ)

1. Ulusal Egemenlik ve Genel Ağ…… 42
2. Askeri Alanda Konsept Değişikliği…..……45
2.1. Asimetrik Bilgi Harbi……48
2.2. Siber Savaş ve Siber Savaşçı……..50
2.3. Körfez Savaşı Örneği…… 54
2.4. Estonya Örneği……... 55
3. Siber Hedefler: Devletlerin Siber Saldırılara Karşı Hassas Tarafları……59
3.1. SCADA Sunucuları…… 60
3.2. Uzak Terminal Birimleri (UTB)…….61
3.3. Elektrik Üretim ve Dağıtım Sistemleri……...63
3.4. Kritik Alt Yapılar……... 64
3.5. Web Uygulamaları Güvenliği…….67
3.6. Kablosuz Mobil Sensör Ağlar…… 67
3.7. Veri Güvenliği…… 68
3.8. Mobil Sistemler…….. 70
3.9. Endüstriyel Sistemler…… 71
4. İç Tehdit……74
5. Kişisel Gizlilik……...74

6. Verilerin Saklama Ortamlarından Silinmesi veya Saklama Ortamlarının İmha Edilmesi……75
7. Siber Saldırıların Maliyeti……76
8. Siber Güvenliğin Sınırları……..77
9. Siber Güvenlik ve Özel Sektör…….. 77
10. ABD'nin Siber Güvenlik Önlemleri Teşkilatlanması……... 79

ÜÇÜNCÜ BÖLÜM

(SİBER UZAY GÜVENLİĞİNİN ULUSLARARASI GÜVENLİĞE VE TÜRKİYE'YE ETKİLERİ)

1. Siber Terör……89
2. Uluslararası İşbirliği…….. 99
3. Uluslararası Siber Güvenlik Tatbikatları…….. 101
3.1. Dark Screen (2002 – 2003)……101
3.2. Cyber Storm I-II-III (2006 – 2008 – 2010)…… 101
3.3. APCERT Drill 2006 – 2011 (Ocak 2010)…….. 102
3.4. NATO Cyber Defense Exercise (2008 – 2009 – 2010)……..102
4. Dünyada Veri kaçağı……. 102
5. Siber Güvenliğin Öngörülemeyen Sonuçları……103
6. NATO Siber Savunma Mükemmeliyet Merkezi……... 107
6.1. NATO Bilgi Harekâtı Konsepti Çalışmaları…….. 109
6.2. NATO'nun Bilgi Harekâtına Bakışı……...110
6.3. NATO'nun Bilgi Harbi ve Bilgi Harekâtı Tanımlar…….. 111
7. Türkiye ve Siber Güvenlik…… 113
7.1. Türkiye'nin Siber Güvenlik Alanındaki Durumu…….....114
7.2. Siber Güvenlik Ulusal Eylem Planı……120
7.3. Türkiye'nin Siber Güvenlik Stratejisi…… 123
7.4. Siber Güvenlik Tatbikatları……127
7.4.1. BOME 2008 Tatbikatı……. 128
7.4.2. Amaçları……...128
7.4.3. Ulusal Siber Güvenlik Tatbikatı (USGT) 2011……... 128
7.4.4. Ulusal Siber Güvenlik Tatbikatı Uygulama Konuları……..129
7.5. Siber Kuvvet Komutanlığı……..130
SONUÇ……134
KAYNAKLAR……138

KISALTMALAR

Kısaltma	Bibliyografik Bilgi
AAD	Askerî Alanda Devrim
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
Bkz.	Bakınız
BM	Birleşmiş Milletler
BS	Bilgi Savaşı
BT	Bilişim Teknolojileri
C&C	Komuta Kontrol - Command&Control
C.	Cilt
C4I	Command, Control, Communications, Computers, and Intelligence
CAST	Center for Advanced Security Theory
CERT	Computer Emergency Response Team
CSTB	Computer Science and Telecommunications Board
çev.	Çeviren
DDW	Digital Data Warfare
DNS	Domain Name System
ed.	Editör
FBI	Federal Bureau of Investigation
haz.	Hazırlayan
IP	Internet Protocol
IW	Information Warfare
md.	Madde
NATO	North Atlantic Treaty Organization
nu.	Numara
p.	Page
S.	Sayı
s.	Sayfa
ss.	Sayfadan sayfaya
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
TSE	Türk Standartları Enstitüsü
TSK	Türk Silahlı Kuvvetleri
Vol.	Volume
VPN	Virtual Private Network

Kısaltma	Bibliyografik Bilgi
APCERT	Asya Pasifik Bilgisayar Olayları Müdahale Ekibi
BBC	British Broadcasting Corporation
BDDK	Bankacılık Düzeleme ve Denetleme Kurumu
BOME	Bilgisayar Olaylarına Müdahale Ekibi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CAC	Common Access Card
CPNI	Center for Protection of National Infrastructure
CSI	Computer Security Institute
DARPA	The Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DHS	Department of Homeland Security
DOS	Denial of Service
EKDS	Elektronik Kimlik Doğrulama Sistemi
GSM	Global System for Mobile Communications
HAY	Harp Akademileri Yayınları
HTTP	Hyper Text Transfer Protocol
IBM	International Business Machines
IMS	International Military Staff
IRC	Internet Relay Chat
ITU	International Telecommunication Union
MGK	Milli Güvenlik Kurulu
NETWARCOM	Donanma Ağ Savaş Komutanlığı
P2P	Point To Point
PLC	Programmable Logic Control
RF	Radyo Frekansı
RFID	Radio Frequency Identification
SCADA	Supervisory Control and Data Acquisiton
TBMM	Türkiye Büyük Millet Meclisi
TC	Türkiye Cumhuriyeti
TSK	Türk Silahlı Kuvvetleri
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
USGT	Ulusal Siber Güvenlik Tatbikatı
UTB	Uzak Terminal Birimleri
WSIS	World Summit on the Information Society

ŞEKİLLER

	Sayfa
Şekil 1- Siber Ortamın Kapsadığı Alan	**43**
Şekil 2- Siber Saldırganlar	**52**
Şekil 3- Siber Uzayda Stratejik Hedefler	**60**
Şekil 4- SCADA Sistemi	**62**
Şekil 5- 2012 İnternet Kullanıcıları Sayıları (Milyon)	**86**
Şekil 6- Symantec firması tarafından yıllara göre tespit edilen zararlı yazılımlar	**87**
Şekil 7- Veri Kaçağı Tehditlerinin Yıllara Göre Durumu	**103**
Şekil 8- Türkiye'de Geniş Bant İnternet Abone Sayısı	**117**
Şekil 9- Ulusal Siber Güvenlik Tatbikatına Katılanlar	**129**

GİRİŞ

Bilişimin büyük bir silah haline dönüştüğü günümüzde devletler, sanal silah üretimine büyük önem vermektedirler. Siber uzayın oluşuma bağlı olarak ortaya çıkan bu yeni tehdidin hiç şüphesiz göz ardı edilmemesi gerekmektedir. Zira, kişisel bilgilerinizi veya ulusal sırlarınızı elde etmeye çalışan bir hacker, günümüzün en çok karşılaşılan modern casusu, ajanı veya halk tabiri ile hırsızıdır. Bu bağlamda siber saldırılar da günümüzün en sinsi savaş yöntemi olarak tanımlanabilinir. Çok hızlı bir biçimde gelişen ve değişen teknolojinin imkânları sayesinde geride hemen hemen hiç iz bırakmayan, fail ve azmettiricisinin siber dünyanın derinliklerinde kaybolmasını sağlayan soyut bir düşmanla mücadelenin ise ne kadar zor olduğunu devletler günümüzde anlamaya başlamışlardır.

Daha geniş bir ifade ile belirtirsek, teknolojide kaydedilen inanılmaz gelişmeler ve bilgi birikimi; dünya siyasetinin, askerî stratejisinin, ekonominin ve en önemlisi de güvenliğin yapısını önemli ölçüde değiştirmiştir. Bu bağlamda tezimi hazırlarken savunduğum temel sav; içerisinde bulunduğumuz bilgi çağında, siber uzay güvenliğinin ulusal güvenliği ve uluslararası güvenliği hızlı bir şekilde ve çok farklı yönlerden etkilediğidir. Zira siber uzay güvenliği devletlerin güvenliğini doğrudan etkilemekte ve uluslararası güvenliği koruma adına tahmin edilemez sonuçlar doğurabilmektedir. Diğer bir deyişle, yaşadığımız bilgi çağında artık savaşlar bilgi ve bilgi sistemlerine bağımlı hale gelmiştir ve görünür gelecekte daha da bağımlı hale gelecektir. Bu bağlamda siber savaşlar belki kısa vadede savaşın kazanılması noktasında temel faktör olmayacaktır ama buna sebep olacak en önemli unsurlardan birisi olacaktır. Uzun vadede ise savaşları kazanmak devletin sahip olduğu tesislerin bomba ile imhası şeklinde değil, sahip olduğu bilgi sistemlerini bilgi savaşı araç ve vasıtaları ile etkisiz hale getirme şeklinde olacaktır.

Siber uzayın genişliği düşünüldüğünde saldırıların her yerden gelebileceği unutulmamalıdır. Bu sebeple özel ve kamu sektörünün, devletlerin bu anlamdaki güvenlik yapılanmalarının ve uluslararası yapılanmaların, sürekli bilgi paylaşımında bulunması suçluların en kısa sürede yakalanması konusunda önemlidir. Siber uzayın her an gelişen bir yapı olması sebebiyle güvenliğin ve kontrolün bir an bile bırakılmaması gerekmektedir. Örneğin, günümüzde internet edinimi oldukça ucuz olduğu için hemen hemen bütün terör örgütleri tarafından kullanmaktadır. Çünkü eylem için çoğu ülkede kolaylıkla temin edilebilecek küçük bir ağ bağlantısı yeterlidir. Ancak verilebilecek zararlar çok daha yüksek

olduğu ve sistemlerin birçoğunda güvenlik önlemleri yetersiz kaldığından siber saldırıları düzenlemek oldukça kolaydır. Devletler ise siber savaş taktiklerini ve imkânlarını gizli tutarak karşı tarafa kendi güçlerini belli etmemeye çalışmaktadırlar. Zira soyutluklar ve gri boşluklar hasım tarafı korkutmaya yetmese de siber dünyanın geniş sınırları içerisinde devletleri olduğundan daha güçlü göstermeye yetmektedir.

Yukarıda genel ve soyut olarak belirttiğimiz faktörler bağlamında siber güvenlik temalı tez çalışmamızda öncelikle konu ile ilgili belli başlı temel kavramlar açıklanmıştır. Bu kısımda, Türk Silahlı Kuvvetleri'nin siber güvenlik alanında alabileceği sorumlulukları tanımlaması çerçevesinde "*E-Mehmetçik*"kavramı ilk kez kullanılarak, literatürde tartışmaya açılmıştır. Birinci bölümün ikinci kısmında ise siber güvenliğin ulusal ve uluslararası güvenliğe olan etkilerine teorik bir arka plan oluşturması için uluslararası ilişkiler teorileri genel hatlarıyla değerlendirilmiştir. Bu değerlendirmenin ardından ise uluslararası ilişkilerde çatışmayı ve işbirliğini açıklayan teoriler kapsamında çalışmanın teorik zeminini oluşturan Kopenhag Okulu, siber güvenliğe yaklaşımı itibarıyla analiz edilmiş ve söz konusu ekolün teorik bakış akışı tezin tamamında irdelenmiştir.

İkinci bölümde ise siber güvenliğin ulus güvenliğine olan etkileri, teorik çerçeveye dayandırarak açıklamaya çalışılmıştır. "*Siber Güvenliğin Uluslararası Güvenliğe ve Türkiye'ye Olan Etkileri*" başlıklı son bölümdeyse siber saldırıların uluslararası boyutlarda ulaşmış olduğu seviyeleri ve yapılanmaları, bu anlamda bu saldırılara karşı alınan kararlar, bağlayıcı bazı yasal düzenlemeleri incelendikten sonra, Dünya'da siber terörün ulaşmış olduğu seviye analiz edilmiştir. Son bölümde ayrıca Türkiye'nin siber güvenlik alanında yapmış olduğu çalışmalar, hazırlanan strateji belgelerine değinilmiştir. Bu kapsamda çalışmada, TSK'nin siber güvenlik alanında etkisini arttırırken, ülkemizin siber güvenliğinden esas sorumlu olabilmesi için (örneğin "*E-Mehmetçik*" uygulaması ile) atılması gereken adımların neler olabileceği de tespit edilmeye çalışılmıştır.

BİRİNCİ BÖLÜM

KAVRAMSAL VE TEORİK ÇERÇEVE

İçerisinde yaşadığımız bilgi çağı yeni fırsatları ve her anlamda değişimleri bizlere yaşatırken güvenlik algısı da bu değişimde yeni kavramlara ihtiyaç duymaktadır. Kimi zaman bir devlet için tehdit "*terör*" veya dünyayı tamamen etkisine alan siyasal akım olmuştur. Doğa olayları bile kimi zaman ülkenin güvenliğini tehdit edecek boyutlara ulaşmıştır. Bilgi çağı bilgisayarlar ile o kadar iç içi geçmiştir ki bilgisayarlar olmadan hayatı düşünmek imkânsız hale gelmiştir. Kişisel bilgisayarların artması ile birlikte internet kullanımı da yaygınlaşmıştır. Günümüzde internet finans, alt yapı, ulaşım, enerji gibi birçok alanda vazgeçilmez bir unsur olup, kullanıcıları sınırları aşarak birbirleri ile rahatlıkla iletişime geçebilmektedir. Teknolojideki değişim beraberinde iletişim ve bilgi alt yapısında da değişikliklere sebep olmuştur. Kablosuz ve mobil iletişim her zaman ve her yerde bilgiye ulaşmayı sağlamıştır.

Devletlerin ekonomisi ve ulusal güvenliği her geçen gün bilgi teknolojisi ve altyapısına daha da bağımlı hale gelmektedir. Genel olarak örneklendirmek gerekirse siber güvenliğin içerisine; ziraat, yiyecek, su, kamu sağlığı, acil hizmetler, hükümet ve savunma kuruluşları, bilgi ve haberleşme, enerji, ulaşım, bankacılık ve finans, kimyasallar ve tehlikeli maddeler, posta ve diğer taşıma hizmetlerinin görüldüğü kamu ve özel tesisleri sıralayabiliriz.[1] Siber uzayı bir sinir ağına benzetirsek, bunun içeriğinde birbirine bağlı milyonlarca bilgisayar, sunucular, binlerce sistem yönlendiricisi, anahtarlar ve kilometrelerce uzunluğunda fiber optik kablolar karşımıza çıkmaktadır. Canlıların hayatında sinir ağları ne kadar hayatiyse, devletlerin ekonomik ve ulusal güvenliği için bu ağın güvenli çalışabilir durumda olması o kadar önemlidir.

Tezin birinci bölümünde, siber uzay güvenliği içerisinde sıklıkla karşımıza çıkan kavramlar ayrıntılı olarak incelemeden açıklanmaya çalışılacaktır. Sonrasında tezin ana hatlarıyla dayandığı teorik çerçeve farklı yönleriyle ele alınacaktır.

1. KAVRAMSAL ÇERÇEVE

Teorik bir konu olan siber güvenliğin daha iyi anlaşılabilmesi için bazı teknik kavramların bilinmesi gerekmektedir. Bu sebeple çalışmamın birinci bölümünde bu teknik

---

[1] YILMAZ Sait, Olcay SALCAN, **Siber Uzayda Güvenlik ve Türkiye,** Milenyum Yayınları, İstanbul, 2008, s. 3.

kavramlar tanımlanacaktır. Bu teknik kavramlar açıklanırken kavramların siber güvenliği teorik olarak ilgilendiren kısımları üzerinde durulacaktır.

1.1. KÖTÜCÜL YAZILIMLAR (MALWARE): Kullanıcının bilgisi dışında bilgisayarlara sızmak ya da zarar vermek amacıyla tasarlanan yazılımların ortak adıdır. Bir bilişim sistemine zarar vermek amacıyla veya kullanıcılarının amaçları dışında kullanılmak üzere sisteme yerleştirilir.[2] Kötücül yazılımlar; bilgisayar virüsleri, kurtçuk ya da solucanlar (worm), Truva atı (trojan), klavye izleme (key logger) yazılımları, istem dışı olarak gönderilen ticari tanıtım (adware) yazılımları ve bilgi toplayan casus (spyware) yazılımlarıdır. Ayrıca virüs, Truva atı ve casus yazılımlar gibi kötü amaçlı programlar taşınabilir bellekler aracılığıyla çok kolay yayılabilir. Kötücül yazılımlar internet üzerinden de kullanıcıların haberi olmadan bilgisayarlara bulaşabilir.[3]

1.1.1. Sayısal Bilgi Savaşı (Digital Data Warfare, DDW), askeri, politik, ekonomik ya da kişisel amaçların elde edilmesi maksadıyla bir bilgisayar sistemine ya da ağına gizlice zararlı bilgisayar yazılımı (Malicious Computer Code) sokulmasıdır. Saldırgan, bir devlet, bir terörist organizasyon, uluslararası bir şirket ya da bir şahıs olabilir. [4]

1.1.2. Sayısal Bilgi Savaşı Araçları

Bilgi çağında devlet savunması, daha yüksek oranda bilim ve teknoloji tabanlı olacaktır. Bilgisayarın kullanılmasıyla; insansız hava araçları, tanklar, gemiler, denizaltılar ve özellikle uydular ile 24 saat kesintisiz harekât yapılabilecektir. Telsiz sensor ağlarıyla ülkenin her noktası donatılacak, kara, deniz, hava, uzay ve siber boyuttan gelecek her tehdit, anında merkez bilgisayarlarını ve koruma sistemlerini harekete geçirerek önlem alınmasını sağlayacaktır. Tüm askerî personel ve teçhizatlar silikon-çipler ve mikrobilgisayarlarla donatılacaktır.[5] Harekât alanındaki personelin bilgilendirilmesi ve yönlendirilmesi aynı anda olabilecektir. Savaş araçları artık boyut değiştirmiş ve sayısal alanda kendini göstermektedir. [6]

---

[2] **Malicious Software (Malware): A Security Threat to the Internet Economy Report**, Organisation For Economik Co-Operation and Development(OECD), 17-18 June 2008, http://www.oecd.org/dataoecd/53/34/40724457.pdf, (e.t. 12.11.2011), p.19.

[3] ULAŞANOĞLU M. Emin, Ramazan YILMAZ, M. Alper TEKİN, **Bilgi Güvenliği: Riskler ve Öneriler**, Bilgi Teknolojiler ve İletişim Kurumu(BTK), 2010, Ankara, s.19.

[4] Türk Silahlı Kuvvetleri (TSK), **Türk Silahlı Kuvvetleri Bilgi Harbine Nasıl Hazırlanmalıdır?**, Harp Akademileri Basım Evi, Yenilevent , İstanbul, Nisan 1999, s. 17.

[5] Ibid., s.110.

[6] SAREM, **Üçüncü Uluslararası Sempozyum Bildirileri**, İstanbul, 12–13 Mayıs 2005, "Bilgi Çağı ve Teknolojik Gelişmeler Işığında Toplum, Yönetim, Yönetici ve Lider Yaklaşımları", Ankara, Genelkurmay Basımevi, 2005, s. XIII.

Sayısal Bilgi Savaşı'nin araçlarına değinmek gerekirse, bu araçlar şu şekilde isimlendirilmektedir:

1.1.2.1. Bilgisayar virüsleri; kendi kendini büyük programların içine kopyalayabilen program parçalarıdır. Bir virüs, yalnız bulunduğu ana program çalıştırılınca aktif hale geçer ve görevini yapar. Bilgisayarların çökmesine, sabit disklerin silinerek tüm bilgilerin kaybolmasına neden olabilirler. Virüsler, bilgi savaşında, kişisel bilgisayarlardan çok dijital telefon ağı devreleri gibi program tabanlı sistemlerde etkili olarak kullanılabilir. Genellikle program ve dosyalara eklenerek harekete geçer ve bilgisayar sistemlerine zarar verirler.[7]

Bilgisayarlara zarar vermek üzere hazırlanmış programlardır. E-postalar ve dosyalar ile bilgisayarlara bulaşan virüsler bilgisayarların çalışmasını engelleyebilmekte, bilgilerinin kaybolmasına, bozulmasına veya silinmesine neden olabilmektedir. Ayrıca bilgisayarları yavaşlatabilmektedir. Bunlar bilgisayar belleğine yerleşen, çalıştırılabilen programlara kendini ekleyebilen, yerleştiği programların yapısını değiştirebilen ve kendi kendini çoğaltabilen programlardır.[8]

1.1.2.2. Solucanlar (Worm) : Bağımsız birer bilgisayar programlarıdır. Kendini ağlar üzerinde bilgisayardan bilgisayara kopyalayarak çoğaltır. Ağların çökmesine, bilgilerin kaybolmasına, bağlantıların kesilmesine sebep olabilir.[9] Solucanlar bilgisayar ağları arasında herhangi bir donanıma veya yazılıma zarar vermeden dolaşabilen, kullanıcılardan bağımsız olarak kendilerini aktif hale getirebilen ve bir kopyasını ağa bağlı diğer bilgisayarlara bulaştırabilen programlardır. Solucanların virüslerden en büyük farkı hızla ve büyük sayılarda çoğalabilmedir. E-postalar ve dosyalar ile diğer bilgisayarlara bulaşmaktadır. Solucanlar bilgisayarları kilitlemekte ve internet sayfaları açılırken uzun süre beklenmesine neden olmaktadır. Herhangi bir anti-virüs programı kullanılmaması durumunda, bir süre sonra sistem çökebilmekte ve kullanılamaz hale gelebilmektedir.[10]

1.1.2.3. Truva atı (Trojan) : Yararlı gibi görünen fakat arkasında gizli bir kodun da yer alması nedeniyle bilişim güvenliğine zarar veren programlardır.[11] Bu programlar kaleyi içerden fethetmek için kılık değiştirerek kaleye giren askerlere benzerler. Genellikle e-

---

7 TSK, op.cit., s.11.

8 NICKOLOV E., 7-8 Ekim 2008, **Modern Trends In The Cyber Attacks Against The Critical Information Infrastructure**, Regional Cybersecurity Forum, Sofia, Bulgaria, akt. ULAŞANOĞLU, op.cit., s. 25.

9 Ibid.

10 OECD, op.cit., s.24.

11 Ibid, s. 22.

postalara ekli olarak gelen dosyalar aracılığı ile bilgisayarlara bulaşırlar. Truva atı diğer kötücül yazılımlar olan bilgisayar virüsleri ve bilgisayar solucanları gibi kendi başlarına işlem yapamazlar.[12] Çünkü programlar içine programın gerçek fonksiyonundan başka fonksiyonları gerçekleştirmesini sağlamak için koyulmuş program parçalarıdır. Bu tür bir program, özellikle ağ güvenlik programı gibi programlara yerleştirilerek, sistemin güvenlik açısından zayıf noktalarının programı yerleştiren kişilerin eline geçmesini sağlayabilir. Truva atı programları virüslerin ve kurtların gizlenmesinde de kullanılırlar. [13]

1.1.2.4. Mantık bombaları: Bir çeşit truva atı programıdırlar. Esas amaçları önceden üretilmiş virüs, kurt gibi programları aktif hale getirmek için gerekli ikazı sağlar. Hemen hemen tüm dünyada yaygın olarak kullanılan ağ işletim sistemlerine üretici firma tarafından yerleştirilebilecek mantık bombaları aktif hale geldiklerinde söz konusu ağ işletim sisteminin kullanıldığı, banka şebekesi, borsa bilgisayar ağı gibi, sistemlerin çökmesine neden olabilir.[14]

1.1.2.5. Tuzak kapıları, arka kapılar (Backdoor): Bu mekanizmalar kullanıcıya hissettirmeden sistemlere nüfuz etme ve sistem güvenliğini aşarak sistemden istediği bilgiyi alma ve kendi arzusu doğrultusunda kullanabilme imkânını verir.[15]

1.1.2.6. Chipping: Yazılımlarda olduğu gibi, donanım sistemlerinin de, çok rahatlıkla kendinden beklenen fonksiyonlar haricinde son kullanıcısının bilmediği bir veya birden fazla fonksiyonu yapacak şekilde üretilmesi mümkündür. Bunun için özel imal edilmiş mikroçipler, çeşitli amaçlar için, silah ve sistemlerde kullanılan kartlara monte edilebilir. Belirli bir fonksiyon için üretilmiş devrelere ilave fonksiyonlar kazandırılabilir.[16]

1.1.2.7. Kaydedici (Keylogger): Kullanıcıların bilgisayar üzerinden yaptığı her işlemin kaydederek görüntülenmesini sağlar.[17] Klavye üzerinde bastığınız her tuşun kaydedilerek karşı tarafa iletilmesini sağlayan bir çeşit programlardır.

1.1.2.8. Hizmetin engellenmesi saldırıları (DoS/DDoS): Kurumların veya şirketlerin bilgi ve iletişim sistemlerini ve hizmetlerini devre dışı bırakmak için yapılan saldırılardır. Saldırıların amacı; web sitesine erişimi engellemekten, başka radyo sitesinin dinlenmesini

---

12 ULAŞANOĞLU, op.cit., s. 22.
13 TSK, loc.cit.
14 Ibid., s.12.
15 Ibid.
16 TSK, op.cit., s. 12.
17 Dış Politika ve Savunma Araştırmaları Grubu, **BİLGESAM**, "Siber Tehdit, Güvenlik, Savaş ve Stratejiler", www.bilgesam.org/, (e.t. 09.11.2011), s.1.

engellemeye, banka hesabınızdan para transferini engellemekten, gemilerin limana yanaştırılmasını durdurmaya kadar çok geniş bir alanda düşünülebilir. Bu saldırılar sistemlerin aşırı şekilde yüklenmesi ile oluşmaktadır. Bilgisayar korsanları bilgisayar kullanıcılarına bir program yüklemekte ve belirlenen günde bütün bilgisayarlar aynı anda, önceden belirlenmiş bir internet sitesine giriş talebi göndermeye başlamaktadır. Bu tür talep sayısı on binleri bulduğunda karşı tarafın sunucusu yanıt veremez duruma gelmektedir. İlgili internet sitesi çökmekte, işlem yapamaz hale gelmekte ve site sahipleri maddi zarara uğramaktadır. Kullanıcıların e-posta gönderme ve alma isteğine yanıt veremediğinden aynı zamanda servis sağlayıcı açısından bir itibar kaybı oluşturmaktadır.[18]

Saldırıları, taşırma, yük arttırma, kapasite dışına çıkarma ve yanıltarak askıda bırakma olarak özetleyebiliriz. Bu olayı somutlaştırmak için günlük yaşamda kullandığımız telefon kulübelerini ve santralleri örnek vermek yeterli olur. Bir telefon kulübesinde bulunan rehber kitapçığı veya sarı sayfaları günümüz "*Domain Name System*" (DNS) hizmeti gibi düşünebiliriz. Telefon etmek için kulübedeki ahizeyi de internet gezgini gibi düşünelim. Kulübede sıraya giren kişileri de, günümüz web sitesine girmek isteyen bilgisayarlar olarak düşünelim. Eğer telefon rehberinde aradığımız numarayı aynı anda binlerce kişi farklı kulübelerden ararsa o telefon numarasına kimse ulaşamaz ve şehirlerarası telefon santrali kilitlenip hizmet veremez. Telefonda ki kişiyle, başka birisinin sesini taklit ederek konuşarak, aslında internette protokol bulandırma saldırısı yapmış gibi oluruz. Görüşmeyi normalin dışında uzatarak, kulübe dışında sıra bekleyenlerin konuşmasını engelleriz. Bu da "*Transmission Control Protocol*" (TCP) parametreleriyle oynayarak protokolün askıda kalmasını sağlamak gibi olur. Eğer binlerce kişi aynı anda şehirde ki tüm telefonlardan bunu yaparsa sistem erişilemez. İşte interneti durdurma ve erişilemez hale getirme saldırıları da buna benzer mantık içerir. Şehirdeki binlerce kişinin telefon kulübelerinden aynı anda aramasını, DDoS için kullanılan, halen internet üzerinden satışı yapılan zombi ve botnetlere benzetebilirsiniz. Telefon rehberinden veya sarı sayfalardan birinin yırtılması, karalanması ve yerine yeni numara yazılmasını da, internette ele geçirilen root DNS'ler olarak düşünebiliriz.[19]

DoS ve DDoS, genelde başlangıç düzeyindeki acemiler ile botnet ve zombileri kontrol eden çok iyi organize olmuş sanal saldırganlar, sosyal gruplar ve devletler tarafından düşük

---

[18] KRAUSE M., H. TIPTON, 2007, **Information Security Management Handbook**, CRC Press, 6th. Ed., akt. ULAŞANOĞLU, op.cit., s. 18.

[19] CEYLAN Cenk, "İnterneti Durdurmak için Siber Savaş Aracı olarak DDoS Saldırıları", **Turkish Forensic**, http://www.bilgiguvenligi.gov.tr/siber-savunma/interneti-durdurmak-icin-siber-savas-araci-olarak-ddos-saldirilari.html, (e.t. 03.01.2012).

yoğunluklu gerçek savaş taktiği olarak siyasi ve ticari olarak tercih edilir. Halen günümüzde DDoS saldırılarına karşı, savunma için %100 çözüm bulunamamıştır. Ancak çok iyi ağ analizi ve "*Internet Protocol*" IP trafiğine ilişkin sonuçların veri madenciliği çalışmasıyla, "*Transmission Control Protocol/ Internet Protocol*" TCP/IP ve diğer protokollere ait parametrelerin kontrollü olarak değiştirilmesiyle, saldırılara karşı savunma gücü kazanmak mümkündür. [20]

1.1.2.9. Botnet: "*Bot çobanı*" ya da "*bot yöneticisi*" olarak adlandırılan tek bir bilgisayar tarafından uzaktan kontrol edilebilen kodlar yardımıyla ele geçirilmiş bilgisayarlar ağıdır. Binlerce bilgisayarın gücü bir araya getirildiğinde istenilen bir web sitesini çökertmek için kullanılabilir. Gelişmiş satın alınabilir güvenlik programları da dâhil hızlı bir şekilde değişen yazılımlardan dolayı, botnet kodlarının yayılımı e-posta eklentilisiyle İstem Dışı Elektronik Postalar spam mesajlar [21] yayarak ve hatta internet sağlayıcılarının kırılganlık avantajlarını kullanan sessiz yüklemelerle yapılabilmektedir.[22]

Bot kelimesi "*robot*" kelimesinden türetilmiştir. Robot daha önceden planlanmış işleri yapan makinedir. Bu botların bir merkezden yönetilen büyük gruplarına botnet adı verilmektedir. Botnetler genellikle tek bir merkezden yönetilerek botların bir koordinasyon içerisinde belli amaçlar için yönlendirilmesinde kullanılırlar. Botnetler tarafından kontrol edilen bilgisayarlar "*botnet üyesi*" ya da "*köle bilgisayar (Zombie*)" olarak adlandırılmaktadır. Köle bilgisayarlar sahibinin isteklerini yaparlar. Uzaktan kontrol edilen bu bilgisayarlar ile verilerin çalınmasından başka bir fabrikada veya nükleer tesiste yangın dahi çıkartabilirsiniz. Botnetler, verdikleri zararlar ve uygulama alanları açısından zararlı yazılımlar içinde ön sıralarda bulunmaktadır. Botnetler çevrimiçi (online) bilgisayar sistemlerinin karşı karşıya olduğu en büyük tehdittir. Dağıtık bilgisayar sistemleri olan botnetler, finansal dolandırıcılık, siber ataklar, dağıtık servis dışı bırakma atakları (DDoS), istenmeyen e-posta gönderme, ajan yazılımlar, yemleme (Phising) e-postaları, yazılımların yasal olmayan dağıtımı, bilgi ve bilgisayar kaynaklarının çalınması, kimlik hırsızlığı gibi birçok bilgisayar saldırısı için de kullanılabilirler.[23]

---

[20] Ibid.

[21] SPAM mesajın en basit tanımı sizin isteğiniz olmadan size gönderilen reklam içerikli maillerdir.

[22] CARAFANO James Jay, Eric SAYERS, " Building Cyber Security Leadership For The 21st Century", **The Heritage Foundation**, No.2218, 16.12.2008, http://www.carlisle.army.mil/DIME/documents/bg_2218[1].pdf , (e.t. 02.11.2011), p.4.

[23] KARA Mehmet, Necati E. ŞİŞECİ, "Botnetlerle Mücadelede Dünyadaki ve Türkiye'deki Durum", **TÜBİTAK-UEKAE**, 15.03.2011,

Botnetler, karmaşık matematiksel problemleri çözmek için, internet ağına bağlı bilgisayarların kombine işlem gücünü kullanmak gibi iyi niyetli kullanılabileceği gibi, servis sağlayıcılarını işlevsiz hale getirmek gibi kötü amaçlara da hizmet edebilmektedir.[24]

Botnetler birkaç katmanlı C&C (komuta kontrol - Command&Control) merkezleri sayesinde farklı dil, ülke, zaman dilimleri ve farklı yasalar altındaki bilgisayarları kontrol edebilmektedirler. Bu mekanizmalar botnetlerin izlerini sürmeyi zorlaştırdığı için onları bilişim suçları için çekici bir araç haline getirmektedir. Önceki nesil virüs ve kurtçuklarda olduğu gibi botnetler de kendi kendilerine açıklık içeren bilgisayarlara bulaşarak yayılan zararlı yazılımlardır. Buna karşın botnetleri diğerlerinden ayıran özellik C&C merkezi ile haberleşerek, kendilerini güncelleyebilmeleri ve yönetilebilmeleridir. Çok katmanlı komuta kontrol yapısı botnet yöneticilerini gizleyen yapılar sunmaktadır. Tipik bir botnetin yaşam döngüsü, enfeksiyon, bilgi çalma, bağlantıyı sürdürme, zararlı faaliyetleri yerine getirme, enfekte etme ve botnet oluşturma olmak üzere beş fazdan oluşur. Enfeksiyon fazında kurban bilgisayara botnet zararlı yazılımı bulaşır. İkinci fazda zararlı yazılım aracılığı ile bilgisayardaki önemli bilgiler (kredi kartı numarası, lisans anahtarları, kişisel bilgiler, parolalar vb.) C&C merkezine gönderilir: Üçüncü aşamada saldırgan C&C merkezinden aldığı komutlarla bilinen açıklıklar için tarar ve açıklık bulduğu makineleri enfekte eder. Dördüncü aşamada C&C merkezinden gelen komutlarla istenilen zararlı faaliyetler yürütülür. Beşinci aşamada ise kendini günceller ve faaliyetlerine devam eder. Köle bilgisayar her başlatıldığında bot uygulaması otomatik olarak başlar ve çevrimdeki görevlerini yerine getirir.[25]

Kötücül Yazılımlar veya Sayısal Bilgi Harbi Araçları içerisinde ağırlıkla kullanılan kavramlar dışında, siber uzay güvenliği içerisinde karşımıza çıkan diğer kavramlara da değinmek gerekirse, bunları da şu şekilde açıklayabiliriz.

1.1.3. Siber: Siber (cyber) ve sanal (virtual) kavramları da ayrı kavramlardır. Çoğunlukla karıştırılmalarına rağmen birbirlerinden farklı anlamlara sahiptirler. Siber terim olarak sibernetik kökeninden gelmektedir. Sibernetik ise makine ve canlılardaki kontrol ve iletişim teorisidir. Daha spesifik olarak mekanik bilgi işlem sistemleri ile canlı varlıkların kontrol ve iş haberleşme yöntemlerinin karşılaştırmalı araştırmasını ifade etmektedir. Siber

---

http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/botnetlerle-mucadelede-dunyadaki-ve-turkiyedeki-durum.html, (e.t. 07.11.2011).

[24] ANDRESS, WINTERFELD, op.cit., p.6.

[25] KARA, ŞİŞECİ, op.cit., s. 1.

(cyber) kelimesi daha çok İngilizcede bilgisayar, bilgisayar şebekesi, ağ sistemlerine atfen önek olarak kullanılmaktadır. Örneğin siber uzay ya da diğer sık kullanılan tabiriyle sanal âlem terimi kullanıcılar tarafından bilgisayarlar aracılığıyla internet ve sosyal ağlar içerisinde kurulan iletişimden doğan sanal ortamı ifade etmektedir. Siber kelimesini Birleşmiş Milletler (BM), "*internete bağlı bilgisayarların, iletişim alt yapılarının, çevrimiçi iletişim yapan kişilerin, veri tabanı ve bilgi sistem araçlarının oluşturduğu küresel bir sistem*" olarak tanımlamaktadır.[26] Siber uzay, siber âlem ve sanal âlem terimlerinin tamamı daha özel olarak internete karşılık olarak da kullanılmaktadır. Çünkü internet, iletişim yöntemi açısından siber olmakla birlikte meydana getirdiği ortam açısından sanaldır.[27]

1.1.4. Siber Uzay Kavramı: Siber savaş ve tehditlerin oluştuğu siber alan; kara, hava, deniz, denizaltı ve uzayda operasyon yürütülen bütün alanları kapsayan alan anlamına gelir. Siber uzay; bilgisayar, donanım (bilgisayar çipleri ve silah sistemleri dahil olmak üzere), yazılım (özel sektör ve devletler tarafından geliştirilen), uygulamalar (komuta kontrol sistemleri gibi), protokoller, mobil cihazlar ve bu sistemi yöneten insanlardan oluşur.[28] Ayrıca, (ungoverned space), (infosphere), (terra nullius), sanal vatan gibi deyimler de kullanılabilir.[29] Geçmişte harp meydanı, savaş alanı gibi tabirler yakın zamanda ki meskûn mahal gibi somut, fiziksel alanların yerini soyut ve sanal, siber alanlar almaya başlamıştır.

Siber uzayın karmaşıklığı iki ayrı oyun alanı arasındaki ayrımla başlar. Birincisi, ticari internet; kamunun günlük aktiviteleri için ayrılır ve genel olarak devlet dışı aktörlerin hedefidir. Bu alanın kırılganlığı, sırasıyla Nisan, Mayıs 2007 ve Ağustos 2008 de Estonya ve Gürcistan da gerçekleşen siber ataklarda açığa çıkmıştır. İkincisi, askeri ağlar; Özellikle 1990 ve 2012 yılları arasında ordu savaş yeteneklerini ağ merkezi savaşla geliştirmeye çalıştı. Bilgi işlem ile ilgili artan güven, bir saldırı anında bağlantının düşeceği ihtimalini ortadan kaldırmayı gerekli kılmaktadır.[30] Ordunun askeri ağları arttıkça silahların etkinliği her anlamda güçlenecek ama siber saldırılara karşı da hassasiyet o derece de artmış olacaktır.

Siber uzayın belirsizliği, teknik olarak çok gelişmiş, birçok sayıda saldırıların gözlenmesine sebep olabilmektedir. Gelişmiş siber tehdit analizleri uzun zamanlı bir tehdit ve hassasiyet takipleri ile mümkün olabilir. Saldırı araçları ve yöntemleri çok geniş bir sahaya

---

[26] ANDRESS Jasan, Steve WINTERFELD**, Cyber Warfare:Teckniques, Tactics and Tools for Security Practitioners**, Syngress, 1 edition, p.2

[27] ULAŞANOĞLU, op.cit., s.8.

[28] ANDRESS, WINTERFELD, op.cit., p.20.

[29] BİLGESAM, op.cit., s.1.

[30] CARAFANO, SAYER, op.cit., p.3.

yayılmış ve teknik kapasitenin çoğalması ile birlikte daha karmaşık bir hal almaya başlamıştır.[31]

1.1.5. Bilgi Savaşı: Information Warfare (IW) Türkçeye "*Bilgi Savaşı*" olarak çevrilebilecek yeni nesil bir savaştır. Askeri literatürde kabul edilen, amacı askeri avantaj sağlamak için bilginin yönetimini ve kullanımını kontrol altına almak, daha kapsamlı bir tanımla; *Düşmanın sahip olduğu bilgi ve onun fonksiyonlarını engellemek, imha etmek, bozmak ve kendi çıkarlarımız doğrultusunda kullanmak için yapılan hareketlerle, düşmanın bu faaliyetimize karşı önlem almasını engellemek ve benzeri harekâtına karşı korunmak.*[32] Tüm dünyada bilgisayar teknolojilerinin hızlı bir şekilde gelişmesi, bilgisayar kullanımını birey-şirket-devlet piramidinde elzem hale getirmiştir. Aynı zamanda bilgisayar-ağ sistemlerini bizim açımızdan da vazgeçilmez kılmıştır. Bu vazgeçilmezlik aynı zamanda bir zayıflığı da beraberinde getirmiş olup, son yıllarda Bilgi Savaşı denen yeni nesil savaş doktrinini meydana getirmiştir. Aslında düşman bilgi ağlarına zarar verecek her türden saldırı BS (Bilgi Savaşı) içine dâhil edilebilir. Örneğin düşman fiberoptik komünikasyon ağına zarar veren bir özel harekât bir nevi askeri BH operasyonudur. [33]

Bilgi Harbi FM 100–6 Amerikan Talimnamesinde "*Kendi bilgi işlem sürecimizi, bilgi sistemlerimizi ve bilgisayar ağlarımızı korurken, düşmanın bilgi işlem süreci, bilgi sistemleri ve bilgisayar ağları üzerinde bilgi üstünlüğü sağlamak için icra edilen bir dizi hareket*" olarak tanımlanmaktadır. Aynı talimnamede Bilgi Harekâtı konusunda "*Bilgi Harekâtı: muharebe alanında, kaynakların doğru zaman ve yerde kullanılmasını, silahların seçilmesini, bilginin kontrol altında tutularak muharebenin desteklenmesini ve muharebe etkinliğinin artırılmasını sağlar. Bilgi harekâtı, askeri harekâtın bütün safhalarında tesis edilen askeri bilgi ortamındaki bütün bilgi işlem faaliyetlerinin geliştirilmesi, işlenmesi ve korunmasına yönelik olarak yapılan sürekli bir askeri faaliyettir. Bilgi harekâtı aynı zamanda küresel bilgi ortamında yapılan önleyici çalışmalarla düşmanın bilgi ve karar verme kabiliyetlerinin istismar edilmesi ve çalışamaz hale getirilmesi faaliyetleridir*" şeklinde ilave fonksiyonlar üzerine de ayrıntılı açıklamalarda bulunulmuştur.

---

[31] The White House, **The National Strategy to Secure Syberspace**, Washington D.C., Feb. 2003, http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20GAO-Powner-SFR_10Mar09.pdf, (e.t. 18.11.2011), p.viii.

[32] SCHLEHER Curtis, **Bilgi Çağında Elektronik Harp**, Çev. Berna Kara, Ankara, Doruk Yayımcılık, 2004, s.22, akt. Hüseyin ATMACA, "Psikolojik Harbin Asimetrik Harp Vasıtası Olarak Kullanılması", Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü, (Yayınlanmamış Yüksek Lisans Tezi), Bolu, 2009, s.26.

[33] ÇAY Ömer, "Bilgi Harbi ve Türkiye", **Ekopolitik**, 03.11.2009, http://www.ekopolitik.org/public/news.aspx?id=4348&pid=4082, (e.t. 06.09.2011).

1.1.6. Siber Savaş: ABD Savunma Bakanlığı siber savaşı "*Bilgisayar ve internet kullanımı aracılığıyla siber alanda savaş yürütmek*" olarak tanımlıyor. Ancak siber savaş, aslında çok daha geniş kapsamlı bir olgunun parçasıdır.[34] Başka bir tanımla "*Siber savaş; Bir devletin başka bir devletin bilgisayar sistemlerine ve ağlarına sızarak hasar veya kesinti yaratmak üzere hareket etmesi*" [35]

Siber savaş aslında bir "*asimetrik savaş*" olarak da tanımlanabilir. Bir taraf geleneksel imkânlar açısından zayıf olmakla beraber zeki ve atik, diğeri ise hantal ve katı bir tutum sergileyebilir. Siber savaş ve tehdidin en önemli niteliği son derece süratle gelişmesidir. Tehdit öylesine hızlı gelişebilir ki geleneksel stratejideki eylem/tepki geç kalabilir. Siber savaş devletlerarası bir ihtilaf olmakla beraber, değişik yollardan devlet dışı aktörler de devreye girebilir. Siber savaş da belirgin ve orantılı gücü devreye sokmak son derece zordur. Hedef askeri, sanayi, sivil veya değişik sektörlere hizmet veren veya onlardan sadece birisi örneğin sunucuların (server) bulunduğu bir oda dahi olabilir.[36]

1.1.7. Siber Terörizm: Uluslararası düzeyde terör tanımı üzerinde mutabık olmadığından bu tanımların şimdilik ucu açıktır. Siber terörü bilgi çağının terör şekli olarak da tanımlayabiliriz. Bu tanımdan hareketle, bilgi çağının enstrümanlarının, yani bilgi harbinin enstrümanlarının da terörizm maksatlarıyla kullanılabileceğini söyleyebiliriz. Siber terör yanlış bilgi yayarak aldatır, şaşırtır, yanıltır. Dehşet, korku ve şüphe yaratır. Bilgiyi bozar, ülkenin fiziksel alt ve üst yapılarını etkiler.[37]

Her ne kadar bazı yetkililer gerçek anlamda bir siber terörizm saldırısının olmadığını söyleseler de bazıları da teröristlerin çoktan siber dünya da üstünlüğü ele geçirdiğini iddia etmektedirler. Bu büyük fark "*terörizm*" ve "*siber terörizm*" tanımlamasındaki anlaşmazlıklardan kaynaklanmaktadır. Terörizm ve siber terörizmin evrensel olarak kabul edilmiş bir tanımı yoktur.[38]

---

34 BİLGESAM, op.cit., s.2 .

35 CLARK Richard A., Robert K. KNAKE, Siber Savaş, Çeviren Murat ERDURAN, İstanbul Kültür Üniversitesi, İKÜ Yayın Evi, 2010, s.8.

36 BİLGESAM, op.cit., s.6.

37 Ibid., s.2.

38 DOĞRUL Murat, Adil ASLAN, Eyyüp ÇELİK, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism" , **Turkish Air War College**, Istanbul, Turkey, p.3.

Teröristler bombalama gibi geleneksel formları kolaylaştırmak için siber uzayı kullanabilirler. Mesajlarını destekçilerine duyurmak, eylemlerinin koordinasyonu sağlamak için web sitelerini kullanabilirler.[39]

1.1.8. Asimetrik Savaş: Teknolojik ve askeri açıdan üstün olan veya olmayan bir düşmana kendi çıkarlarımızı zorla kabul ettirmek maksadıyla; hassasiyetlerini istismar ederken, kuvvetli yanından kaçınarak, ölümcül veya ölümcül olmayan, askeri veya askeri olmayan araçlar ile yeni strateji ve taktiklerin kullanımıdır.[40] Yarattığı ani ve hazırlıksız durum nedeni ile ülkelerin siyasi, sosyal ve ekonomik sistemlerinde istikrarsızlıklarına neden olan, düşük seviyede kuvvet ve teknoloji kullanarak etkin olmayı amaçlayan tehdit algılamasıdır.[41] Düzensiz Savaş veya Konvansiyonel Olmayan Savaş olarak da isimlendirilebilen Asimetrik Savaş, baskın güç ya da kuvvetli taraf ile baskın olmayan güçsüz taraf arasında, savaşta güçsüz tarafın gerilla taktikleri kullanarak doğrudan sıcak çatışmaya girmeden yaptığı mücadele gibi tanımlar da getirilebilir.[42]

1.1.9. Bilgi Güvenliği: Bilgi güvenliği ve bilişim güvenliği ifadeleri yaygın kanının aksine aynı anlamda kullanılıyor olmakla birlikte, kapsamları farklıdır. Bilgi güvenliği genel olarak bilginin bir varlık olarak her türlü tehditten korunması olarak tanımlanabilir. Bilgi ve iletişim teknolojilerini dikkate alarak bilgi güvenliğini "*doğru teknolojinin doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme*", bilişim güvenliğini ise "*bilgi ve bilginin işlenmesi, aktarılması, kullanılması ve depolanmasına aracılık eden her türlü teknolojik ortamın istenmeyen, yetkisiz kişilerce erişilmesi, değiştirilmesi, bozulması, yok edilmesi gibi her türlü tehdidi önleme"* olarak tanımlayabiliriz.[43]

Bilginin korunması için bütünlük (integrity), gizlilik (confidentiality) ve erişilebilirlik (availability) özelliklerinin her zaman sağlanıyor olması gerekir. Bilginin üretilmesinden imha edilmesine kadar geçen süreçte güvenliğinin sağlanması için Bilişim Teknolojileri (BT) Güvenliği, Yedekleme, Fiziksel Güvenlik vb. kontrollerinin de devreye alınmış olması

---

39 DENNING Dorothy E, "Cyber terrorism. Testimony before the Special Oversight Panel on Terrorism," **Committee on Armed Services U.S. House of Representatives**, Georgetown University, May 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, (e.t. 10.08.2010).

40 ATMACA, op.cit., s. 52.

41 Milli Güvenlik Kurulu Genel Sekreterliği, **Asimetrik Tehdit Nedir?**, http://www.mgk.gov.tr/Turkce/sss.html#soru_13 , (e.t. 03.11.2011).

42 ANDRESS, WINTERFELD, op.cit., p.9.

43 SAĞIROĞLU Ş., **Bilgi Güvenliği ve Yapılması Gerekenler Sunumu**, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, akt., ULAŞANOĞLU, op.cit., s.7.

gerekmektedir. Bu açıdan bakıldığında BT Güvenliği, Bilgi (Veri) Güvenliği'nin sağlanması için etkenlerden sadece bir tanesidir.[44]

Bilgi güvenliği, bilgi ve bilgi sistemlerinin yetkisiz girişlere, ihlallere, değiştirmelere, imhalara karşı koruyarak bilgi güvenilirliğini, gizliliğini ve kullanabilirliğini sağlamayı amaçlar. En önemli konu ulusal altyapının korunmasıdır. Ulusal düzeyde çeşitli kurumların aldıkları önlemler demeti ülkenin siyasi, sosyal, ekonomik yaşamını destekleyen varlıklarını, hizmetleri ve sistemleri korumayı amaçlar. Bunların tümünün veya bir kısmının kaybı veya tehlikeye düşmesi ulusal çıkarları doğrudan etkiler.[45]

Yazılı, sözlü veya elektronik ortamdaki tüm bilgilerin korunması ve bunların doğru zamanda, doğru kişiye ulaştırılmasıyla ilgilidir. Bilgi güvenliği bilgilerin izinsiz erişim, kullanım, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden koruma işlemidir. Bilgi güvenliği kavramı verilerin mahremiyeti, bütünlüğü ve ulaşılabilirliği ile ilgilidir. Son zamanlarda bilgi güvenliğinin kapsamı gelişme göstermiştir. Bu bağlamda Türk Standartları Enstitüsü (TSE) tarafından yayınlanan TS ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardı, bilgi güvenliği konusunu gizlilik, bütünlük ve kullanılabilirlik başlıkları altında incelemektedir.[46]

1.1.10. Siber Güvenlik: Bilgi güvenliği, bilişim güvenliği terimleri ile aynı anlamda kullanılıyor olmakla birlikte daha çok bilişim güvenliğini kapsar. Siber güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünü olarak tanımlar. Kurum, kuruluş ve kullanıcıların varlıkları; bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, elektronik haberleşme sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır. Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini amaçlar.[47] Bu tanım kurum, kuruluş ve kullanıcıların bilgi işlem donanımlarını, personel, altyapı, uygulamalar, hizmetler, elektronik haberleşme sistemleri ve siber ortamda iletilen ve saklanan tüm bilgileri

---

44 IŞIKÇI Çağatay, "COBIT Denetimleri Açısından Bilgi Güvenliği", Şekerbank Bilgi İşlem, http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/cobit-denetimleri-acisindan-bilgi-guvenligi.html, (e.t. 07.11.2011).

45 BİLGESAM, op.cit., s.5.

46 ULAŞANOĞLU, op.cit., s.8.

47 Ibid.

kapsamaktadır.[48] ABD Başkanı Barack Obama'nın tanımına göre ise "*bir ülkenin karşı karşıya bulunduğu en ciddi ekonomik ve ulusal güvenlik tehdidi*" [49] olarak nitelendirilmektedir.

Siber uzay da güvenlik anlamında ilk bulgu, 1986 yılında kuzey Kaliforniya'da yer alan Lawrence Berkeley Ulusal Laboratuarı'nda çalışan Doktor Cliff Stoll tarafından tespit edilmiştir. ALPANET'e bağlı bilgisayar kayıtlarındaki basit bir toplama hatasını Stoll bilgisayar ağlarını kullanarak elde etmiştir.[50] Bu tecrübesini "*The Cuckoo's Egg*" adlı kitabında anlatması ve bu olayın kötü niyetle kullanılabileceğinden bahsetmesi, sonrasında dünyada bu anlamda sisteme müdahalelere sebep olabileceği fikrini ortaya çıkarmıştır.

1.1.11. Siber Suç: Mali kaynak amaçlı özel kişi veya kurumlara hırsızlık/sahtecilik amacıyla saldırı düzenlemesi olarak tanımlanabilir.[51]

1.1.12. Siber İstihbarat: Bilgi sağlamak amacıyla kamu ve özel kurumlara yönelik saldırılardır.[52] Ülkeler siber istihbarata daha fazla önem vermeye başlamışlardır. Çünkü terör örgütleri siber uzayın nimetlerinden daha fazla yararlanmaktadırlar.

1.1.13. Bilişim Suçları: Bilgisayarların ya da bilgi ve iletişim şebekelerinin suç işlenmesinde araç, amaç veya ortam olarak kullanıldığı suçlardır. İnternette virüsler, solucanlar, Truva atı gibi binlerce kötücül yazılım yer almakta ve bunlara her geçen gün yenileri eklenmektedir. Özellikle sosyal amaçlı eğlence ve paylaşım siteleri siber tehditlerin ve kötücül yazılımların dağıtılması için araç olarak kullanılmaktadır.[53] Ticari ve askeri siber bağlantılara tehdit oluşturabilecek birçok farklı tip aktör bulunmaktadır. Bu tür ticari bilgisayar korsanları yaygın olarak "*Siyah Şapkalı Bilgisayar Korsanı*" olarak adlandırılırlar. İkincisi politik ya da sosyal görevler; siber çevreyi kullanma girişiminde bulunan siber teröristler yıllar önce internetin hedef zengini ortamında savaşa girmişlerdir. Giriş için sınırların kolay aşılabilir olmasından dolayı siber çevre teröristler için şiddete başvurmak,

---

48 Ibid., s.11

49 CNNTÜRK, "Pentagon'da bir İlk: Siber Savaş Birimi", 24.05.2010, http://www.cnnturk.com/2010/dunya/05/24/pentagonda.bir.ilk.siber.savas.birimi/577439.0/index.html , (e.t. 03.11.2011).

50 QT Worldtel Inc., "Southeast Europe Cybersecurity Conference", **C.O.B.A.S., (Centralized Out of Band Authentication System)**, Sofya, Bulgaristan, 8-9 Eylül 2003, http://www.cybersecuritycooperation.org/documents/QT_COBAS_White_Paper.pdf , (e.t. 13.04.2011).

51 BİLGESAM, op.cit., s.2.

52 Ibid.

53 ULAŞANOĞLU, op.cit., s.14.

saldırı planlayıp gerçekleştirmek için en etkili asimetrik araçlardan biri olduğunu kanıtlamıştır.[54]

1.2. TEORİK ÇERÇEVE

Uluslararası ilişkiler teorilerine bakıldığında güvenlik kavramının, askeri-stratejik seviyede ele alındığı tespit edilmektedir. Diğer bir değişle güvenlik, uluslararası ilişkilerde devletlerarası güç ve çekişme ile ilgili olup askeri tehditler ve düşman, geleneksel güvenlik anlayışının ana konularıdır. Realist görüşün güvenlik ile güç arasında bağlantı kurması, güvenlik ile ilgili analizleri daha da karmaşık hale getirerek aynı zamanda kendi içinde bir çelişkiyi de doğurmaktadır. Zira güç unsuru kullanılarak başkalarının aleyhine bir statüko yaratılması, güvenlik kavramının kendisi ile çelişmektedir. Karşı tarafın kendi güvenliğini tehdit altında hissetmesi, onunda güvenliğini sağlamak için harekete geçmesine, kendini güvende hissedebilecek tedbirlere başvurmasına neden olmakta, bu durumda diğer tarafın aynı şekilde karşılık vermesine neden olmaktadır.[55] Klasik realist yaklaşımda güç kavramı ve ulusal güç unsuru merkezi bir öneme sahip olmuştur. Realizmde uluslararası çatışmaların sonucunun belirlenmesinde ve diğer devletlerin davranışlarını etkileme konusunda devletlerin sahip oldukları kapasiteler büyük bir önem taşımaktadır. Realist yaklaşımı benimseyen yazarlar, devletin güç kapasitesini askeri gücü dışında askeri olmayan unsurları da kapsadığını kabul etmektedirler.[56]

Güvenlik olgusu, tehdit algılamasıyla başlamıştır. Soğuk Savaş düzeninin sonuna kadar güvenlik, daha çok bir devlete ait silahlı kuvvetlerin tüm milli unsurlarıyla karşı devlette yarattığı tehdit ve buna karşı alınan tedbirler olarak gündeme gelmiştir. İki kutuplu dünya düzeninin yıkılmasını müteakip oluşan "*Yeni Dünya*" düzeni içerisinde tehdit ve güvenlik algılamaları da değişmiştir.[57] Siber uzay güvenliği artık devletlerin tedbir alması gereken yeni bir güvenlik boyutunu oluşturmaktadır. Güvenlik çalışmalarını, klasik "*Savaş*

---

54 CARAFANO, SAYERS, op.cit., p.3.

55 DEMİRAY Muhittin, İsmail Hakkı İŞCAN, "Uluslararası Sistemde Güvenlik Kavramının Değişimi Ekonomik ve Jeopolitik Arka Planı", **Dumlupınar Üniversitesi Sosyal Bilimler Dergisi**, Sayı 21, Ağustos 2008, s.152.

56 ARI Tayyar, **Uluslararası İlişkiler Teorileri Çatışma, Hegemonya, İşbirliği**, 2010, 6.Baskı, MKM Yayıncılık, s. 159.

57 KÜÇÜKŞAHİN Ahmet, Tamer AKKAN, "Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit", http://vizyon21yy.com/documan/genel_konular/Milli%20Guvenlik/Strateji/Degisen_Guvenlik_Algilamalari_Isiginda_Tehdit_ve_Asimetrik_Tehdit.pdf, (e.t. 30.12.2011), s.1.

Doktrini" içerisinde düşünmek ve buna yönelik tedbirler almak, sanal dünya veya siber uzay içerisinde birçok güvenlik tedbirinin eksik algılanmasına sebep olacaktır.

Günümüz konjonktüründe uluslararası güvenlik içerisinde devletlerin alışageldikleri güvenlik anlayışı değişmiştir. Güvenlik anlayışındaki bu değişim, insanları ve de sınırları birbirlerine daha fazla yaklaştıran teknolojik gelişmelerin ve bunun sonucu olarak ortaya çıkan küreselleşmenin bir sonucu olarak kabul edilmektedir. Soğuk Savaş'ın sona ermesi ile birlikte uluslararası güvenliğin dengesini bozan organize suçlar, yasadışı göç, insan kaçakçılığı, uyuşturucu ve silah kaçakçılığı, para aklama gibi yeni suçlar ön plana çıkmaya başlamıştır. Soğuk Savaş sonrasında küresel güvenlik ortamını derinden etkileyen ve şekillendiren en önemli olay 11 Eylül terör saldırıları olmuştur. Saldırılar sonucunda yeni küresel güvenlik tehditleri, terörizm, kitle imha silahlarının yayılması, siber güvenlik vb. uluslararası güvenlik gündeminin ön sıralarına oturmuştur. Bu açıdan 11 Eylül olayları, bölgesel güvenlik problemlerinin küresel etkilerini ortaya çıkarmış ve bölgesel güvenlik problemlerini de küreselleştirmiştir.[58] Güvenlik problemlerinin küreselleşmesi başta hâkim güçler olmak üzere tüm devletleri kendi ulusal güvenlikleri için yeni bir anlayış çerçevesinde tedbirler almaya yöneltmiştir.

Realistlere göre uluslararası ilişkilerin ana konusu ulusal güvenliktir. Siyasi ve askeri konuları en önemli konular olarak görmektedirler. Realistlere göre devletler ulusal çıkarı maksimum kılmak için çaba gösterirler. Realistler tarafından devletin varlığını sürdürmeye ilişkin olan ulusal güvenlik konusu yüksek politika olarak tanımlanmaktadır. Ticari, mali ve sağlıkla ilgili konular ise alçak politika olarak nitelenmektedir. Realistlere göre devletlerin amaçlarına ulaşmak ve çıkarlarını gerçekleştirmek için kullanacakları temel unsur güçtür.[59] Bu anlamda güç tanımına siber güç unsurlarını veya siber uzay içerisine koyabileceğimiz unsurları eklemek son derece zordur. Realist teoriler gücü ağırlıklı olarak askeri bir tanım içerisine sokmaktadır. Sanal dünya içerisinde bir ulusun insanlarını etkilemek veya kendi istekleri çerçevesinde onları yönlendirmek mümkündür. Sosyal medya gibi unsurlar siber güvenliğin en önemli etkenleri arasındadır.

Kendini savunma kavramı oldukça geniş bir çerçevede ele alındığından realizmde emperyalizme meşruluk tanınmaktadır. Zira tehdit açıkça algılanabiliyorsa karşının saldırısını

---

[58] KULOĞLU Armağan, "Broken Balances After The Cold War: Searches for Regional Stability", **The Thirteenth International Confrence on Security and Cooperation**, Antalya, 2003, s.102, akt. KÜÇÜKŞAHİN, op.cit., s.2.

[59] ARI, op.cit., s.163.

beklemeye gerek yoktur ve dolayısıyla böyle bir savaş gereklidir ve meşru kabul edilmektedir.[60] Bu noktada realizm siber dünya içerisinde kendisini tam olarak açıklayamayacaktır ve teorik anlamda yetersiz kalacaktır.

Jeopolitik güvenlik anlayışı, çeşitli teorilerle birçok bilim insanı tarafından farklı açılardan ele alınmış, yorumlanmış ve günümüzün uluslararası güvenlik politikalarının temel kalıplarındaki biçimlenme içerisinde köklü parametreleri oluşturmuştur. Devletin ve/veya toplumun güvenliği ile jeopolitik son derece yakından ilintili olarak kabul edilmiştir.[61]

Realizmin diğer önemli bir varsayımı ise devletlerin güvenliğini sağlayacak bir merkezi otoritenin olmadığı uluslararası yapının anarşik olacağıdır. Realistler bu yapı içinde her bir devletin kendi güvenliğini kendisi sağlamak zorunda olduğunu varsayarak diğer devletlerin de aynı şekilde davranacağını ve dolayısıyla her bir devletin kendi çıkarı doğrultusunda hareket edeceğini ileri sürmektedir. Realistlere göre uluslararası yapıdaki istikrarsızlıklar devletlerin güvenliği için tehdit oluşturmakta olup, devletler olası tehditlere karşı destek sağlamak için ittifak antlaşmaları imzalayabilirler. Ancak devletler güvenlikleri için bunlara çok fazla güvenmezler ve kendi güvenliklerini kendileri sağlayabilecek bir güce erişmeye çalışırlar. Realistler maksimum güce ulaşmak arzusuyla hareket eden tüm devletlerin birbirlerinin bu tür amaçlarına engel olmaya çalıştıklarını; bunun sonucunda ortaya çıkan güç dengesinin ise istikrarı sağlayan önemli bir unsur olduğunu iddia etmektedirler.[62]

Liberal düşünce ve neo-Marksist yaklaşımlar, 1960'ların sonlarında ve 1970'lerdeki yumuşama döneminde klasik güvenlik anlayışını her ne kadar sorgulamaya açmış ve bu düzlemde güvenlik çalışmalarında bir geçiş dönemini simgelemişse de, uluslararası sistemin egemen güvenlik paradigması realist ve neo-realist düşüncenin ana varsayımlarıyla belirlenmiştir. Ontolojik çerçevesini realist ve neo-realist kuramın çizdiği geleneksel güvenlik değerler dizisi; realist tezlerin temel savlarını yansıtır şekilde devlet merkezli, ulusal güvenlik endeksli, güç ve özellikle de askeri güç eksenli bir yapıdadır. Klasik realizm ve neorealizmin tekelinde var olan ve bu temel özelliğiyle iki kutuplu sistemin öne çıkan biçimde resmeden geleneksel güvenlik anlayışı, Soğuk Savaş yıllarının güvenlik paradigması olarak literatürdeki yerini almıştır.[63] Tüm realistler iç politika ile uluslararası politikayı birbirinden ayırarak ele

---

60 Ibid., s.161.

61 DEMİRAY, İŞCAN, op.cit., s. 163.

62 ARI, op.cit., s.163.

63 SANDIKLI Atilla - Bilgehan EMEKLİER, "21. Yüzyılda Yeni Güvenlik Anlayışları ve Yaklaşımları", **Uluslararası Balkan Kongresi**, 2011, Kocaeli,

almaktadır. Oysa siber güvenlik söz konusu olduğunda bu ayırımı yapmak mümkün değildir.[64]

Realist teorinin özünü oluşturan güç kavramına yüklenen anlamların oldukça farklı olduğu dikkati çekmektedir. Güç kavramını en sık kullanan ve uluslararası politika analizinin merkezine yerleştiren Morgenthau, politikayı güç mücadelesi olarak tanımlamakla beraber güç kavramını ayrıca ele alıp açık bir tanımını yapmamıştır. K.J. Holsti ve Frankel gibi birçok yazar tarafından kapasite olarak tanımlanan, Morgenthau'ya göre ise bir ulusu diğer uluslar karşısında kuvvete sahip kılan faktörler ve doğrudan ulusal güç olarak kabul edilen nicel ve nitel unsurlardan oluşmaktadır. Bunlardan coğrafya, doğal kaynaklar, endüstriyel kapasite, askeri hazırlık derecesi ve nüfus nicel unsurlar, ulusal moral, ulusal karakter, diplomasinin niteliği ve hükümetin niteliği ise niteliksel unsurları oluşturmaktadır.[65] Klasik realist teorisyenler aslında doğrudan bir güvenlik kuramı ortaya koymamışlar; ancak uluslararası politikaya dair öne sürdükleri savlar ve yaptıkları kavramsallaştırmalarla daha sonra ortaya çıkan güvenlik literatürüne ciddi ve dolaylı bir katkıda bulunmuşlardır.[66]

Bu bağlamda ayrıca gerçek güç ile potansiyel güç arasında da ayırıma gidilmektedir. Özellikle devletin sahip olduğu askeri ve ekonomik kaynaklar gerçek gücü hesap ederken dikkate alınan fiziksel unsurlardır. Ekonomik gücü karşılaştırırken daha çok gayri safi milli hâsıla veya kişi başına düşen milli gelir kavramlarına başvurulmaktadır. Potansiyel güç içerisinde siber gücün bir ulus için potansiyel güç olarak eklenmesi son derece doğru bir yaklaşım olacaktır. Devletin potansiyel güçlerinden söz ederken de henüz kullanmadığı fakat ileride kullanabileceği kaynaklar ifade edilmeye çalışılmaktadır. Örneğin, zengin doğal kaynaklara sahip olmalarına karşılık nüfusa sahip olmadığı için bu kaynakları tam olarak kullanamayan Avustralya ve Kanada'nın askeri ve ekonomik güçlerinin ileride artabileceği ifade edilmektedir.[67]

Realizmin artık mevcut gelişmeler karşısındaki betimleme ve açıklama gücünün de sorgulandığı gözlenmektedir. Realizmin genellemeleri ile mevcut koşulların örtüşmediğini düşünen yazarlar artık realizmin gerçek olmadığını ileri sürmektedirler. Küresel gündemde meydana gelen gelişmelere dikkat çekenler, hegemonya mücadelesinin karakterize ettiği

---

http://www.bilgesam.org/tr/index.php?option=com_content&view=frontpage&Itemid=251, (e.t. 04.02.2012), s.22.

64 ARI, op.cit., s.164.

65 Ibid., s. 165.

66 SANDIKLI, EMEKLİER, op.cit., s.22.

67 ARI, op.cit., s.172.

Soğuk Savaşın gündeminin yerini uluslaraşırı karşılıklı bağımlılık, çevre sorunları, AIDS, ozon tabakasının tahribi, uyuşturucu kaçakçılığı, doğal kaynakların etkin kullanımı, hızlı nüfus artışı ve insan hakları gibi konuların aldığını işaret etmektedirler. Uluslararası ilişkilerin artık realist teorinin gerçekçi bir şekilde anlayamayacağı yeni bir eksene kaydığını iddia etmektedirler. Bu nedenlerden dolayı realist teorinin uluslararası ilişkiler alanındaki çalışmalara rehberlik etme yeteneğini kaybettiğini ifade etmektedirler.[68]

Güç, bir devlete bir şey yaptırmayı ya da bir davranıştan vazgeçirmeyi sağlayan araçtır. Ulusal güç unsularının başında askeri güç gelmekle beraber; siyasal altyapı, ekonomik durum, coğrafi konum ve büyüklük, nüfus ve teknolojik düzey de aynı derecede önemli unsurlardır. Realist yazarlar için ulusal güç, uluslararası politika ve dış politikanın oluşumunda ana öğe olup, hem bir araç hem de doğrudan doğruya bir amaç olarak uluslararası politikanın temelini oluşturmaktadır. Devletler bu öğeleri dikkate alarak süper devletler, büyük devletler, orta boy devletler ve küçük devletler olarak sıralanmaktadır.[69] Oysa siber yetenekler realist yazarların tanımladığı devletleri değiştirmiştir. Küçük devletler siber uzayın sınırları içerisinde büyük devlet gibi etki veya güç sahibi olabilmektedir. Konvansiyonel savaş içerisinde çarpan etkileri olan savaş uçakları, tanklar ve diğer savaş silahları siber savaşta tam tersi bir etki yapabilir. Yani siber saldırılar ile etkisiz hale getirilen uçaklar veya uçakları düşman mı yoksa dost mu ayrımı yapan radar sistemleri kendi uçağına yapabileceği saldırılar ile hiçbir yarar sağlamayacak, hatta zarar bile verebilecektir.

Realizm ve jeopolitik teoriler güç unsurunu temel almaktadır. Bu anlamda jeopolitiğe realist anlayışın egemen olduğu söylenebilir. Her ikisinde de ulusal gücün devletlerin yayılmacı ve emperyalist politikalarının bir aracı olması, bir diğer önemli benzerliktir. Savaş, realizm gibi jeopolitiğin de bir uzantısı, bazen bir aracı bazen de doğal sonucudur. Diğer bir deyişle, jeopolitik teorilere göre de uluslararası ilişkiler bir mücadele sürecidir. Jeopolitik teoriler de realist teoriler gibi devlet merkezli paradigmayı benimseyen teoriler grubuna girmekte ve bu çerçevede devlet, uluslararası ilişkilerin temel ve tek aktörü olarak görülmektedir. Bunun sonucu olarak her iki teoride de devlet önemli bir analiz birimidir.[70]

Devlet büyüklüğü ve mesafe kavramının dışında devletlerarasındaki çatışmaları açıklamada sınır kavramı da önemli bir unsurdur. Sınırlar, devletler için bazen yeni imkânlar

---

68 Ibid, s.203.
69 ARI, op.cit., s.209.
70 Ibid, s.210.

anlamına gelmekte, bazen de dış politikasına sınırlamalar getirmektedir. Devletler arasındaki ilişkilere kısıtlama getirmesi ve bu ilişkilerin çerçevesinin belirlenmesi anlamında sınırlar oldukça önemlidir. Sınırların oynayacağı rol de diğer coğrafya faktörleri gibi durağan olmayıp dinamiktir ve zamana göre değişiklik gösterir.[71] Siber uzay da sınırların olmadığını belirtmek, teorilerin geçerliliğini de ortadan kaldırmaktadır. Ülkelerin sınırları ölçülebilen, belli uluslararası kurallara uyan somut alanlardır. Oysa siber uzay da ülkeler arasında sınırlardan bahsetmek pek mümkün gözükmemektedir. Zaman zaman devletler kendilerini siber saldırılardan korumak için sanal sınırlar belirleyerek korumak istemiştir ama teknik olarak şimdilik bu pek mümkün gözükmemektedir.

Güvenlik çalışmalarının bir diğer kırılma noktası, özgürlük-güvenlik arasındaki bağıntıyı güvenlik çalışmalarının merkezine yerleştiren Ken Booth'un öncülüğünde gerçekleşmiştir. Ken Booth, "*Security and Emancipation"* başlıklı makalesinde, realizmin entelektüel hegemonyası altında şekillenen geleneksel güvenlik düşüncesini ve üzerinde yeniden şekillenen güvenlik çalışmalarını sorgulamaya açmıştır. Ona göre güvenlik, gelecekle ilgili beklentilerin garanti altına alınabilmesi veya isteklerin gerçekleştirilmesi, önündeki engellerin kaldırılmasıdır.[72] İşte bu noktada bilgi çağının yeni güvenlik anlayışları şekillenmeye başlamış, yeni tanımlara ihtiyaç duyulmaya başlanmıştır. Siber uzayın kendisine has özgürlükçü yapısı beraberinde güvenlik açıklarını da sisteme dahil etmiştir. Siber uzayın sınırları olmadığı gibi siber savaş yeteneklerinin de sınırları yoktur. Sınır sadece insanın hayal gücünün bittiği yerdedir. Nükleer enerji elektrik enerjisi üretimi için kullanılması dışında insanlık adına unutulmayan yaralar da açmıştır. Siber uzay bütün iyi niyeti ile karşımızda durmakta ve onun fırsatlarından yararlanmamız için bizi beklemektedir. Nükleer enerjide olduğu gibi insanlık için yarar sağlayan siber uzay, kötü ellerde sonuçlarını tahmin bile edemeyeceğimiz ve kendi kanımca nükleer bomba etkisinden daha fazla yıkıcı etkisi olan sonuçlar doğuracaktır.

---

71 ARI, op.cit., s.223.

72 BOOTH Ken, "Security and Emancipation", **Review of International Studies**, Cilt 17, No 4, 1991, s. 318.

1.2.1. Uluslararası İlişkilerde Çatışmayı Açıklayan Teoriler Kapsamında Küreselleşme ve Siber Uzay Güvenliği

Küreselleşmek kelime anlamı olarak sözlükte; "*Dünya milletlerini ekonomi, siyaset ve iletişim bakımlarından birbirine yaklaşmaya ve bir bütün olmaya götürmek*[73]" şekliyle tanımlanmıştır. Genel olarak bakıldığında küreselleşme; "s*ermayenin, malların, hizmetlerin ve kültür varlıklarının, bilim ve teknoloji imkânlarının sınırları aşan bir süreci hem de oldukça karışık, karmaşık, inişli-çıkışlı, etkilediği alanlarda ne gibi sonuçlar doğuracağı ve doğacak sonuçlardan bizzat kendisinin nasıl etkileneceği bugünden asla kestirilemeyecek olan bir süreci yahut süreçler topluluğunu akla getirmiştir."*[74]

"*Güvenlik*" sözlük anlamı olarak; "*toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet*"[75] şeklinde tanımlanmıştır. Diğer taraftan tarih boyunca, üretim ilişkileri toplumların yapısını tanımlayan en önemli etmen olmuş ve insanlık "*İlkel Toplum*", "*Tarım Toplumu*" ve "*Sanayi Toplumu*" aşamalarından geçerek bugün "*Bilgi Toplumu*" aşamasına gelmiştir. 1980'li yıllardan başlayarak günümüzde tüm hızıyla süren "*Bilgi Devrimi*" ile birlikte bilginin toplanması, işlenmesi ve dağıtılması süreçleri, üretim biçimlerini, güvenlik kavramını ve bunlara ek olarak günlük yaşantımızı bütünüyle değiştirmeye başlamıştır. 1985'lere kadar, dünyada 14 yılda bir olan bilgi katlanma hızı bugün, 6,5 yılda bire düşmüştür.[76] Bilginin inanılmaz hızda katlanarak artması, aynı zamanda bilginin güvenli koşullarda saklanmasını, siber uzay da kendine ait koşullarda ilgili kişilere ve kurumlara güvenle iletilmesini gerekli kılmaktadır.

Buna karşılık günümüzde terörizm, siber uzayın olanaklarını kullanarak en büyük güvenlik endişesi ve sorunu hâline gelmiş ve küresel boyut kazanmıştır. Uluslararası terörizmin; kimyasal, biyolojik ve nükleer silâhlar gibi kitle imha yeteneği olan silâhları geliştirme, sahip olma ve kullanma peşinde olduğuna inanılmaktadır. Aynı zamanda uluslararası terörizm, bilgi teknolojilerinin olanaklarını kullanarak yanıltma haber ve psikolojik harekât vasıtasıyla kitle hareketlerini yönlendirmek suretiyle amaç ve eylemlerini

---

73 Türk Dil Kurumu, **Türkçe Sözlük**, TDK, Ankara, 2005, 10. Baskı, s.1286.

74 AYDIN Mehmet S., "Küreselleşmeye Genel Bir Bakış", **Siyasi, Ekonomik Ve Kültürel Boyutlarıyla Küreselleşme**, Mehmet S. AYDIN, Mustafa ERDOĞAN, Ali Yaşar SARIBAY, Süleyman Hayri BOLAY ve Mehmet ALTAN, 2002, Ufuk Kitapları, İstanbul, s.13.

75 Türk Dil Kurumu, op.cit., s.817.

76 TSK, op.cit., s.2.

destekleyebilecek düzeye de gelmiştir.[77] Bunun yanında siber saldırı alanında yaptıkları ulusal güvenliği ve uluslararası güvenliği etkilemektedir.

Geleceğin savaşlarının, günümüzün bilimkurgu savaş filmlerine benzeme ihtimali vardır. Günün birinde liderler, gerçek bir savaşa girmeye karar vermeden önce, aralarında siber savaş yapacaklardır. Bazı bilimkurgucular, kimin kazanacağına karar vermek için devletlerin, gerçek savaş yapmak yerine siber savaşlara yöneleceğini söylemektedir.[78]

Güvenlik kavramı, özellikle 1990'lı yıllardan itibaren eskiye kıyasla çok daha karmaşık bir hale gelmiştir. Uluslararası sisteme yeni aktörler, yeni tehditler ve bu bağlamda yeni güvenlik anlayışları hâkim olmaya başlamıştır. Düşman varlığını ortaya koymak, ispatlamak daha da önemli hale gelmiştir. Geçmiş dönemin klasik anlayışındaki düşman kavramı ortadan kalkmıştır. Düşmanı isimlendirme eğilimi geri plana kaymış, tehditlerin belirlenmesi ve onunla mücadele ön plana çıkmıştır. Bu durumun sebebi, tehdidin kaynağı olabilecek aktörlerin artık çok daha geniş bir yelpazede ve coğrafyada yer almasıdır. Eskiden tehdidin kaynağı genellikle komşu devletler olarak düşünüldüğü için düşmanı bulmak daha basit olmaktadır. Günümüzde küreselleşmenin de etkisiyle coğrafyanın anlamı değişmekte, bu kavram içerisine siber alan da dâhil olmaktadır. Böylece düşmanı bulmak ve adlandırmak giderek daha zor hale gelmektedir.[79]

Dünyanın herhangi bir yerinden, günün her anında elektronik ağlara erişim mümkün olduğu için ve elektronik ağlar artık önemli temel hizmetlerin sağlanmasında bütünüyle kullanıldığı için siber saldırılara karşı savunmasızdırlar. Siber uzayda kimliğini yâda ülkesini belki de hiç bilemeyeceğimiz, yerini dahi hiç tespit edemeyeceğimiz siber saldırı unsurları akıllı bombaları kullanarak ulusların güvenliğini veya uluslararası güvenliği tehdit edebilmektedir.

ABD İç Güvenlik Bakanlığı bu gerçekleri anladığından 2003 yılında yeni bir "*Ulusal Sanal Güvenlik Bölümü*" oluşturmaya karar vermiştir. İç Güvenlik eski Bakanı Tom Ridge bu kararı açıklarken bütüncül Amerikan alt yapısının elektronik ve fiziksel unsurları arasındaki karşılıklı bağımlılığın altını şöyle çizmiştir: [80]

---

77 SAREM, op.cit., s.XIV.

78 WALLER Douglas, "Onward Cyber Soldiers", **TIME**, 21 Ağustos 1995, http://www.time.com/time/magazine/article/0,9171,983318,00.html, (e.t. 24.01.2012), p.26–34.

79 KÜÇÜKŞAHİN, op.cit., s.. 12.

80 SAREM, op.cit., s.31, akt. Alan HEDLEY, "Bilgi Çağının Sosyal Hayata Etkileri".

"*Sanal güvenlik, kritik alt yapı muhafazasının tüm yönleri ile ilgilenmektedir. Bu ülkedeki pek çok kuruluş işin fiziksel yönünü sanal operasyonlardan ayıramaz; çünkü bunlar birbirine bağımlı hareket ederler. Bu yeni ayırım, ulusun sanal mal varlığını koruyan hayatî öneme sahip bir vazife üzerinde yoğunlaşmaktadır ki biz bu sayede ulusun kritik sanal alt yapısını en iyi şekilde koruyabilmekteyiz*."

Son dönemde gelişmiş ülkeler tarafından alt yapı muhafazasını sağlamak için tüm bu özel kurum ve birimlerin kurulması hem bu ülkelerde yaşayan herkes için bu hizmetlerin öneminin hem de söz konusu riskin, özellikle kasıtlı saldırıların büyüklüğünün anlaşıldığını göstermektedir. Karmaşık ve birbirine bağımlı elektronik sistemlerin zarar görme olasılığı, ulusal ve uluslararası alt yapılarda, özellikle ulusal savunmayı ilgilendiren kritik kurumlarda beklenmedik sonuçların doğmasına sebep olabilmektedir.[81]

Siber güvenlik sorunları konusunda çalışan ABD'nin en büyük rapor kuruluşu olan "*Bilgisayar Acil Destek Koordinasyon Merkezi (Computer Emergency Response Team) (CERT)*", genel ağdaki "*güvenlik suçlarını*" da içeren "*rapor edilen olayların*" kayıtlarını tutmaktadır. Sanal suç büyük bir oranı oluşturmaktadır. 1988 ile 2003 yılları arasında rapor edilmiş 319.992 olayın %43'ü 2003'te meydana gelmiştir. Bu sonuçlarla ilgili açıklamaların bir kısmı, CERT'in resmî ve özel kuruluşlar tarafından olayların rapor edileceği yetkili makam olarak tanınmasından kaynaklansa da, bu veriler sanal saldırılar için artmakta olan olasılıkları da göstermektedir. Bilgisayar sayısı ve genel ağ kullanımı arttıkça sadece sistem arızaları riski değil, siber güvenliğin zafiyetlerinin kendisi de artmaktadır.[82]

Siber uzay da güvenlik, en az geleneksel iş veya devlet faaliyetindeki güvenlik kadar önemlidir. İş yeri sahibi, bir pencere ya da kapının kırık olduğuna bakarak ya da pahalı bir malın kayıp olduğunu görerek bir suç işlendiğini anlayabilir. Ama bilgisayar aracılığıyla işlenen suç çok daha sinsi olabilir. Birçok durumda bir sisteme erişim daha kolaydır ve eğer becerikli bir siber güvenlik uzmanı yoksa suç tespit edilemez. Bu gibi olaylar büyük finansal kayıplarla ve bir şirketin güvenilirliğinin sarsılmasıyla sonuçlanabilir. Bu sebeple çoğu firma, bilgisayar ağları ile ilgili güvenlik tedbirlerini önemli derecede çoğaltmaktadır. Güvenlik

81 Ibid.
82 Ibid.

duvarları birkaç senedir piyasada olsa da, izinsiz giriş tespit sistemi pazarı hızla büyümektedir.[83]

Bilişimin büyük bir silah haline dönüştüğü günümüzde, devletler sanal silah üretimine de büyük önem vermektedir. Sanal âlemden kaynaklanan bu yeni tehlikenin yabana atılmaması gerekmektedir. Kimliği belirsiz bir azmettirici, sessiz bir silah ve meçhul bir tetikçi siber uzayın en çok karşılaşılan kişileridir. Siber saldırıları, bugünün en sinsi savaş yöntemi olarak nitelendirebiliriz. Geride hemen hemen hiç iz bırakmayan, fail ve azmettiricisinin siber dünyanın derinliklerinde kaybolmasını sağlayan bu soyut düşmanla mücadelenin ne kadar zor olduğunu artık devletler anlamaya başlamıştır.[84]

Güvenlik alanında teknolojik gelişmelerin en önemli sonuçlarından biri de, "*Ağ Destekli Yetenek*" anlayışını ortaya çıkarmasıdır. Bu görüşün ana hedefi, bilgi ve karar üstünlüğü sağlamaktır. Tüm millî güç unsurlarının teknolojik yeteneklerle tek bir ağda birleşmesi ve örgütlenmesi sonucu elde edilen bilgi üstünlüğü, modern orduların yeni harekât düzenleri şekillenmesini sağlayacaktır.[85]

1.2.2. Uluslararası İlişkilerde İşbirliğini Açıklayan Teoriler: Siber Güvenlik ve Kopenhag Okulu

Siber güvenliğin bir güvenlik anlayışı haline gelmesi, bilgisayar ve bilgi bilimleri disiplinleri ile başlamıştır. Siber güvenliğin bir kullanımı Computer Science and Telecommunications Board (CSTB)'nin 1991 deki, "*Computers at Risk: Safe Computing in the Information Age*" raporunda olmuştur. Burada güvenlik; "*Sistemdeki istenmeyen kapanma, modifikasyon veya bilginin yok edilmesine karşı koruma ve ayrıca sistemin kendisini koruması*" olarak tanımlanmıştır.[86] Güvenlik teknik olduğu kadar insani yönler de içermektedir ve önemli derecede prosedürel, yönetimsel, fiziksel ve kişisel araçlara sahiptir. Siber güvenlik tehditleri yalnızca istemli hareket eden taraflardan değil, sistem tehditlerinden de oluşmaktadır.[87] Bu sisteme ait tehditler, Hundley ve Anderson[88] tarafından belirtilip,

---

83 Ibid.

84 Ibid.

85 SAREM, op.cit., s.XIII.

86 CSTB (Computer Science and Telecommunications Board), 1991, "**Computers at Risk: Safe Computing in the Information Age**", Washington, DC, National Academy Press, http://www.nap.edu/openbook.php?record_id=1581&page=7, (e.t. 31.12.2011), p.2.

87 Ibid., p.17.

88 HUNDLEY Richard O., Robert H. ANDERSON, "Emerging Challenge: Security and Safety in Cyberspace", **In Athena's camp: preparing for conflict in the information age**, National Defense Research Institute, http://books.google.com.tr, (e.t. 31.12.2011), p.232.

"*Siber Uzay Güvenliği*", bilgisayar ve bilgi sistemlerinin tahmin edilemezliğinde kaynaklanmaktadır. Bu tehditler kendileri veya içinde bulundukları fiziki veya insani çevre için istenmeyen tehlikeli durumlar yaratmaktadır. Tehditler, yazılım ve donanım hatalarından oluşmakta ve dijital teknoloji ya da programları değiştirme yoluyla düzeltilememektedir. Kısaca bilgisayar sistemlerinde, ontolojik olarak bir güvensizlik vardır.

Kopenhag Okulu'na göre, "*Bilgisayar Güvenliği*" kendi kendine bir güvenlik görüşü olarak düşünülemez. Helen Nissenbaum'un[89] dikkat çektiği gibi bilgisayar bilimcilerinin büyük çoğunluğu, dışarıdan erişimi zor olacak sınırlı sayıda böcek ve sistem içeren programlar geliştirmeye odaklanmışlardır. Bilgisayar güvenliğinden siber güvenliğe geçişte, bu teknik yöntem, özel bir alan milli güvenlik için geliştirilen güvenli hale getirme yöntemi ile birleştirilmektedir. Kısaca, "*Siber Uzay Güvenliği*", "*Bilgisayar Güvenliği*" ve güvenlikleştirmenin birleşimi olarak gözükmektedir.

Siber tehditlerin potansiyel miktarını anlamak için bilgisayar sistemlerinin bağlantılı karakterine bakılmalıdır. Bu ağlar, elektrik kaynakları, trenler, boru hatları, kimyasal depo ve radarlar gibi fiziksel noktaları kontrol etmektedir.[90] Saldırı veya siber felaketler, telekomünikasyon ve elektrik dağıtımını zorlaştıracak veya imkânsız hale getirecek, ulaşımı ve taşımayı engelleyecek, büyük miktarlarda para kaybına neden olabilecek, finansal alışverişi imkânsız hale getirebilecek sistem ve ağları içerebilmektedir. Bağlantılı bilgisayarlar, devletleri koruyan geleneksel sınırları yok etmektedir. Siber uzayı oluşturan alt yapı, tasarımı ve gelişimi gereği küreseldir ve siber saldırganlar, "*kimliklerini, yerlerini ve giriş yollarını*"[91] belli etmeyecek mesafeden işlem yapabilirler.

Soğuk Savaş sonrası teknolojide ki inanılmaz değişimle beraber jeopolitik koşullar da beraberinde değişmiştir. Geleneksel güvenlik çalışmalarının dünya güvensizliklerini yansıtmakta ve çözüm önermekte yetersiz kalabildiği tespitinden yola çıkan bu araştırmacıların düşünceleri kâğıt üzerinde kalmadı; uygulamaya da yansıdı. Güvenliğin sadece askerî tehditlerin tespiti ve bertaraf edilmesinden ibaret olmadığını, güvenlik politikasının amacının da yalnızca savaşları önlemek değil aynı zamanda insanların mutluluk

89 NISSENBAUM, op.cit., p.65.
90 The White House, op.cit., p.6-7.
91 Ibid.

ve refahını sağlamak olması gerektiğini savunan "*yeni güvenlik*" anlayışı artık daha çok yerde kabul görüyor.[92]

Kopenhag Okulu güvenlik çalışmalarını, geleneksel devlet merkezli ya da ordu odaklı olmaktan çıkarmış bu alanlar dışında farklı konuları da dâhil etmesi gerekliliğini söylemektedir. Bütün bu sıralamış olduğum gerekçeler sonucu teorik açıdan Kopenhag Okulu'nun tezime temel olabileceği sonucuna varılmış ve bu temel üzerine oturtulmuştur. Bundan sonraki bütün savlarda bu düşünce temelinden hareket edilecektir.

Siber güvenlik ilk olarak 1990'ların başında ağ bağlantılı bilgisayarlar ile ilgili bir seri güvenliksizliğin altını çizmek için kullanılmıştır. Ancak dijital teknolojilerden açığa çıkan tehditlerin yıkıcı sosyal etkileri[93] olabileceği görülünce, bilgisayar güvenliği ile alakalı teknik bir görüşün ötesine geçmiştir. 11 Eylül olayları bilgisayarlara, bilgi teknolojilerine ve siber güvenliğe olan dikkati, daha az olmayacak şekilde, siber altyapının koruması, elektronik takip, teröristler tarafından saldırı ve internetin devlet üzerinden ve devletlere karşı iletişim platformu olarak kullanımına çevrilmiştir.[94] ABD dışında Çin, internetin politik ve sosyal düzeni tehdit eden kısımlarına, vatandaşlarının erişimini engellemeye çalışmışlardır. Yakın zamanda, hükümetin İkinci Dünya Savaşı'nın arşivini ortadan kaldırılmasına karşılık olarak Estonya kamu ve özel kuruluşlarına 2007'de yapılan geniş ölçekli siber saldırılar bu alandaki ilk savaş olarak görülmüştür. NATO buna karşılık, bilgi sistemlerinin korunumun, kendi güç dönüşümünün önemli bir parçası olduğunu bildirerek cevap vermiştir. [95]

Ole Waever'in Barry Buzan ile yaptığı iş birliği sürecinde Kopenhag Barış Çalışmaları Enstitüsünde gelişmeye başlayan "*Kopenhag Okulu*", 2008'de Kopenhag Üniversitesinde kurulan CAST (Center for Advanced Security Theory) ile kurumlaşmıştır. Güvenlikleştirme kuramının önemli bir katkısı Avrupa'nın İkinci Dünya Savaşı sonrasında geçirdiği dönüşüme yeni ve daha ikna edici bir açıklama getirmek olmuştur. Avrupa örneğinden hareket eden Kopenhag Okulu, sorunların ve ilişkilerin güvenlik dışına çıkarılması (desecuritization)

---

92 BİLGİN Pınar, "Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları", **Stratejik Araştırmalar**, Ocak, 2010, s. 69–96.

93 NISSENBAUM Helen, "Where Computer Security Meets National Security. Ethics and Information Technology", J. M. BALKIN, **Cybercrime: Digital Cops in a Networked Environment,** NYU Press, 2005, http://www.nyu.edu/projects/nissenbaum/papers/ETINsecurity.pdf, (e.t. 31.12.2011), p. 61–73.

94 YOULD Rachel E., "In Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security", **Beyond the American Fortress: Understanding Homeland Security in the Information Age,** , 2003, Haz. Robert LATHAM, New York, The New Press, p.3.

95 New York Times, "North Atlantic Council 2007", http://www.nytimes.com/, (e.t. 31.12.2011).

stratejisinin yaygınlaşması ve sadece devletin bekasını ilgilendiren acil konuların güvenlik konusu olarak kabul edilmeye devam edilmesini önermektedir. [96]

Kopenhag Okulunun tarihsel savı; savaşlarla anılan Avrupa'nın artık barışla anılmaya başlamasının ardında yatan dinamikleri, AB'li devlet adamlarının İkinci Dünya Savaşı sonrasında yürüttüğü güvenlik dışına çıkarma çabaları ile açıklamıştır. Waever (1998), Avrupa'da güvenlik kelimesinin telaffuz edilmesinin yarattığı gerginliklerin ve askerî reflekslerin güvenlik konuşmadan ancak güvenlik sağlamaya yönelik iş birliğinin geliştirilmesi ile aşıldığını ortaya koymuştur. [97]

Devletlerin olduğu kadar ulusların, toplumların, dinlerin ve bireylerin de güvenliğinin, uluslararası ilişkiler disiplini çalışma alanı içine girdiği görülmüştür. Bu çerçevede Barry Buzan, birey düzeyindeki güvenliğin devlet ve uluslararası sistem düzeylerindeki güvenlikle ilişkili olduğunu, dolayısıyla güvenliğin herhangi bir düzeyde ele alınarak izole edilemeyeceğini öne sürmüştür.[98]

Ulusal gücün unsurlarını coğrafya, doğal kaynaklar, sanayi, kapasite, askerî hazırlık, nüfus, millî karakter, millî moral, diplomasi olarak söyleyebiliriz. Bu unsurları kendi içerisinde değerlendirdiğimiz de birbirlerine etkilerinin kısıtlı olduğunu görürüz. Örneğin; nüfusun, güç unsurları içerisinde önemli bir etkisi vardır ama coğrafya üzerinde etkisi azdır. Siber uzay yetenekleri ise gücün bütün unsurları üzerindeki etkisi önemli bir yere sahiptir. Geçmiş yayın ve kaynaklarda da benzer şekillerde gücün unsurları içerisinde siber savunma ve saldırı yetenekleri yer almamaktadır. Bu etki geleneksel güç kaynaklarının etkisini bazen azaltan, bazen de katlayan şekilde gerçekleşebilir. Fark etsek de etmesek de özellikle son on yılda teknolojide gerçekleşen değişimler eskimiş güç teorilerini yürürlükten kaldırmıştır. Bunun yanında bilgisayar, telekomünikasyon ve medya teknolojisinde gerçekleşen patlama, güvenlik anlayışımızı iyi veya kötü yönde değiştirmiştir. [99]

Bilgi teknolojisi hem küreselleşmenin hem de gücün olmazsa olmaz koşuludur. Bilgi teknolojisi aynı zamanda küreselleşmenin ve gücün lokomotifi olmuştur. Ordu ve diğer millî

---

96 BUZAN, loc.cit.

97 WAEVER Ole, **Security Communities**, Cambridge, 1998, Cambridge University Press, p. 69–118.

98 BUZAN Barry, "People, States and Fear, An Agenda For International Security Studies in the Post Cold War Era", **Boulder**, 1991, s. 20–26.

99 NYE Joseph S., William A. OWENS, "America's Information Edge", **Foreign Affairs,** 1996, s.22.

güç kaynakları için önemi giderek artmakla beraber, dünya ekonomisini birleştirmiştir. Bu sebeple, bilgi teknolojisi hem gücü, hem de gücü yumuşatan süreci açıklamıştır.[100]

Güvenlik çalışmalarının politika konularına göre çevresel, sağlık veya siber güvenlik olarak ayrılması ve bu şekilde incelenmesi, sonuçta bu güvenlik politikalarının uygulanması problemli olacak olsa bile büyük önem arz etmektedir. Politika, medya ve bilgisayar bilimi alanlarındaki siber güvensizlikler konusundaki yaygın referanslara rağmen, siber konusunu güvenlik ile birbirine bağlayanın ne olduğu konusunda sürpriz bir şekilde çok az açık tartışma vardır.[101] Örnek olarak, yaygın olarak kullanılan "*Contemporasy Security Studies*" adlı kitap, "*Siber Güvenlik*", "*Bilgisayarlar*", "*Kritik Altyapı*" , "*Bilgi Güvenliği*" veya "*Ağlar*" için hiçbir girdi içermemektedir.[102] Güvenlik çalışmaları ile uğraşanlar, siber güvenlik ile alakalı konularda daha farklı görüşler kullanmaktadırlar. "*Siber Savaş*" , "*Ağ Savaşı*" ve "*Ağ Güvenliği*" ve "*Kritik Alt Yapı Korunması*", "*Bilgi Güvenliği*" ve "*Bilgi Savaşı*". Bu terimler siber güvenlik ile çakışmakta ancak farklı anlamlarda içermektedirler.

Lene HANSEN'a göre siber güvenlik alanını teorileştirmek için şu sorular cevaplanmalıdır: Siber güvenliği hangi tehdit ve ilgili konular oluşturmaktadır? Onu diğer güvenlik sektörlerinden farklı kılan nedir? Siber güvenliğin kalıplaşmış örnekleri nasıl analiz edilebilir? Kritik güvenlik araştırmacıları siber konuları ciddiye alarak ne öğrenebilir? [103]

1.2.3. Güvenlikleştirme Teorisi

Kopenhag Okulu iki ana teorik yol izlemektedir: Biri, güvenlik çalışmalarını geleneksel devlet merkezi, ordu odaklı halin dışına çıkarmak üzerine yapılan tartışmalar; diğeri de devlet ve güvenlik politikaları hakkındaki klasik anlayıştır.[104] Bu etiketler birleştirildiğinde, otorite üzerinde odağı, tehdit ve düşmanların yapısını, karar verme yetisi ve acil durum önlemlerinin uygulamasını gösteren "*güvenlik*" görüşü oluşmaktadır. Güvenlik politik bir güce sahiptir ve objektif ya da sübjektif bir durumda çok şeyler gerçekleştiren

---

100 GOMPERT David C., **Right Makes Might: Freedom and Power in the Information Age**, Washington, DC, National Defense University, 1998, s.5.

101 BUZAN Barry, Ole WAEVER, Jaap de WILDE, **Security: A New Framework for Analysis**, Boulder, Lynne Rienner Publishers, 1998, http://books.google.com.tr, (e.t. 31.12.2011), p.29.

102 COLLINS Alan, **Contemporary Security Studies,** 2007, Oxford, Oxford University Press, http://books.google.com.tr, (e.t. 31.12.2011).

103 HANSEN Lene, Helen NISSENBAUM, "Digital Disaster, Cyber Security, and the Copenhagen School", **International Studies Quarterly**, 2009, vol 53, http://www.nyu.edu/projects/nissenbaum/papers/Digital%20Disaster,%20Cyber%20Security%20and%20the%20Copenhagen%20School.pdf, (e.t. 31.12.2011), p.1157.

104 WILLIAMS, loc.cit.

güvenliği sağlamak, bir görüştür. Güvenlik, tehdit içeren ve acil karşılık gerektiren durumları tanımlamaktadır. Güvenlik, bir konuyu politikaların özel bir çeşidi veya politika üstü olarak görmektedir. Bu görüşe göre kamusal konuları; politize olmayan (nonpoliticized) (devletin bu konuyla ilgilenmediği), kamuyu ilgilendiren, karar yaratmayan politize olan (politicized) kamu politikacısının bir parçası, hükümet kararı olarak ayırt edebiliriz. Bu durumda politik bir soru olarak algılanmamakta, normal, kanuni ve sosyal kuralların dışına çıkılarak çözülebilmektedir. Ancak bu şekilde "*politize olmayan*" boş bir kategori olmaktadır. Tüm kamusal meseleler bir çeşit düzenlemeye maruz olduğu için, "*politize olmayan*" konuların politika ve/veya medya dikkati çekmeyen anlaşma ve teknik yollar aracılığıyla düzenlenen konular, "*politize olan*" konuların da yakın medya ve politikayı ilgilendiren, tartışma ve genellikle çoklu politika yaklaşımları oluşturan konular olarak yeniden tanımlanması daha uygundur.[105]

Kopenhag Okulu, güvenliğin aciliyet gereksinimi üzerinde odaklanmasının yanında, güvenlik konusunun devlet/ulus dışında başka objeler de içermesi ve ordu yanında başka sektörleri de dâhil etmesi gerekliliğini söylemektedir. Bu genişletme, "*sosyal güvenliği*", "*bir halkın değişen koşullarda olası ve gerçek tehditler altında kendi esas karakterinin de direnebilme yetisi*" şeklinde teorikleştirmektedir.[106] Bu şekilde milli, dini, etnik veya ırk guruplarının devlet tarafından korunmak yerine tehdit altında hissettiği yerlerde güvenlik problemleri tanımlanması sağlanmaktadır. Sosyal Güvenlik, kişilerle ilgili, büyük ölçekte ekonomik olarak düşünülmektedir. Metodolojik olarak, Güvenlikleştirme Teorisi güvenlik kelimesini karar verme kriteri olarak görmemekte, güvenli hale getirmenin yalnızca mecazi bir güvenlik referansı içermesi gerektiğini söylemektedir.[107]

Kopenhag Okulu, kişisel güvenlik görüşünü reddetme tavrını yeniden gözden geçirmiştir. Ancak, halen ortaklaşa güvenlik görüşünü önde tutmakta ve güvenlik çalışmalarını geleneksel, kişisel ve ortaklaşa güvenliği yan yana tutma durumunu kopyalamaya eğilim göstermektedir.[108]

Milli Güvenlik Görüşü, kimlik, sıralama ve otorite sorularına kuvvetli çözümler sunan devlet gücü prensibine bağlı olduğu için, büyük ölçüde sabit olduğunu kanıtlamıştır. Yine de

---

105 BUZAN, op.cit., p. 25.

106 WAEVER Ole, Barry BUZAN, Morten KELSTRUP, Pierre LEMAITRE, **Identity, Migration and the New Security Agenda in Europe**, 1993, London, Pinter, http://books.google.com.tr, (e.t. 31.12.2011), p.23.

107 BUZAN, op.cit., p.27.

108 MCSWEENEY Bill, **Security, Identity and Interests: A Sociology of International Relations**, Cambridge University Press, 1999, http://books.google.com.tr, (e.t. 31.12.2011), p. 81–93.

milli güvenliğin politik model halindeki şekli ancak devlet kadar dayanıklıdır. Ne devlet ne de güvenlik mücadele edilemez gözükmektedir. İkisi de statülerinin yeniden yapılandırılması için politik ve akademik çalışmalara dayanır. Böylece soru şu hali almaktadır: Siber güvenlik hakkındaki çalışmalar devlet/ulusu ilgili obje olarak güçlendiriyor mu? Bireysel sorumluluk, kolektif güvenliği ya da otoriteyi desteklemek ya da zorlamak için nasıl kullanılabilir? Bu güvenlik politikaları anlayışını yeniden oluşturulabilir mi? [109]

Yalnızca bağlantılar, donanım ve yazılımlar özel olarak finansal konular tarafından üretilip, sahiplenilmemekte yani yönetilmemekte, ekonomi ve siber sektörün güvenlik kısmı da önemli benzerlikler göstermektedir. Ekonomi sektörü de, bireylerden, sınıf ve devletlerden küresel piyasanın kendisine kadar sıralanan farklı objeler konusunda zengindir.[110] Siber ağlar gibi modern ekonomik sistem de sınırlar arası akışlar içermektedir. İki sektörde de bir saldırının nereden geldiğini tanımlamak genellikle zordur. Siber güvenlik, tamamen ekonomik sektörü yansıtmamakta, güvenlik potansiyeli, milli askeri güvenlikle daha fazla bağlantı oluşturacak şekilde ekonomi sektörünün güvenlik potansiyelini aşmaktadır. Siber güvenlik tamamen liberal piyasaya bırakılmamış, ancak kamu-özel sektör sorumluluğu ve hükümet otoritesinin kompleks bir karışımını göstermektedir.[111]

Yukarıdaki bireysel-kolektif çözümlemeyi doğrulayacak şekilde, hükümet ısrarcı bir şekilde, özel sektörü siber güvenlikten aynı derecede sorumlu tutmaktadır. Özel sektör, yalnızca bilgisayar ağının ana hatlarına sahip olmakla kalmayıp, aynı zamanda bilgiyi de sağlamaktadır.[112] Sivil özgürlükleri mobilize etmekle, kamu ve kişi arasında bozulmaması gereken önemli bir denge oluşmaktadır. Devletler, güvenli bilgisayar ağları oluşturmak için evlere, küçük iş yerlerine, üniversitelere ya da resmi ve yerel ajanslara veya bölümlere çok fazla müdahale etmemelidir.[113] Çünkü bu müdahaleler özgürlükçü bir anlayışla hayata geçirilen siber uzayın özüne yeni müdahaleler yapma hakkını kişilere veya kamu kurumlarına da sağlayabilmektedir. Kamu ve kişi arasında ve ekonomik ve politik arasındaki sınır arasındaki tartışmalar, "*Siber*" konusunda aynı amacı taşıyan iş hayatı ve hükümet arasındaki

109 Ibid.
110 NISSENBAUM, op.cit., p.68.
111 HANSEN, NISSENBAUM, op.cit., p.1162.
112 The White House, op.cit., p.ix.
113 Ibid., p.11.

parçalanmayı da arttırmaktadır. Aynı zamanda, politik merkez, dijital alandaki ana alanlardan halen özel sektörü sorumlu tutmaktadır.[114]

Bu akademik ve politik yöntem, finansal, ideolojik, politik veya askeri kazançları için siber stratejileri uygulayan bilgisayar korsanları, suçlular, teröristler, ticari kuruluşlar ve uluslar tarafından hükümete, iş hayatına, bireylere ve toplu halde halka karşı ciddi tehditler oluşturabilecektir.[115] Ronald J.Deibert [116] ve Diana Saco[117]'nun iddia ettiği gibi, siber güvenlik, çoklu yöntemler ve güvenliksizliklerin mücadele ettiği bir alandır. Bireysellik savunucuları ve siber özgürlükçüler kişisel güvenliğin hükümet tarafından delinmesine dikkat çekmekte, otoriter (ve yarı otoriter) rejimler, sınırlar arası bilgi akışlarını rejim/devlet güvenliğini ve kimliğini tehdit ettiği için güven altına almaya çalışmaktadır. Sorulması gereken soru; siber güvenlik yönteminin ayrı bir durum olduğu düşüncesi kaybedilmeden, bu karmaşıklığın teorik yapıya nasıl entegre edilmesi gerektiğidir. Deibart siber güvenliğin farklı objeler, tehditler, politika seçenekleri içeren dört farklı alanda düşünülmesi gerektiğini iddia etmiştir bunlar: milli güvenlik, devlet güvenliği, bireysel güvenlik ve ağ güvenliğidir. [118]

Siber güvenlik, çoklu alanların bulunabileceği bir sektör olarak teorileştirilmelidir. Ancak bu çeşitliliğin bağımsız objelerin değil, obje gruplarının mücadelesinden kaynaklandığı anlaşılırsa, sektörün, güvenlik ve politik dinamikleri daha iyi yakalanabilir. Örneğin bireysel güvenlik alanı, bireyi referans objesi olarak alır ancak bunun yanında bu alanın "*bireyi*", sosyal ve politik referans objelere bağlamaktadır.[119]

Gelecek, devletlerin güvenliği için neler getirir bunu bilemeyiz. Ancak içinde bulunduğumuz bu öngörülemez dünyada, devletler tehditlere karşı hareket tarzlarına yoğunlaşacakları kesindir. Teknolojide kaydedilen inanılmaz gelişmeler ve bilgi birikimi; dünya siyasetinin, askerî stratejisinin, ekonominin ve en önemlisi de güvenliğin yapısını önemli ölçüde değiştirmiştir. Artık, bilgi çağının gerçeklerinin farkına varma zamanı gelmiştir. Teorim; içerisinde bulunduğumuz bilgi çağında, siber uzay güvenliğinin; ulusal

---

114 HANSEN, NISSENBAUM, loc.cit.

115 HUNDLEY, loc.cit.

116 DEIBERT Ronald J., "Security in the Internet Environment. In Information Technologies and Global Politics", 2002, James N. Rosenau-J. P. Singh, **The Changing Scope of Power and Governance**, Albany, State University of New York.

117 SACO Diana, "Colonizing Cyberspace: National Security and the Internet", Jutta Weldes-Mark Laffey-Hugh Gusterson-Raymond Duvall, **In Cultures of Insecurity:States, Communities, and the Production of Danger**, 1999, Minneapolis: University of Minnesota Press, http://books.google.com.tr,(e.t. 30.12.2011), p.261.

118 DEIBERT, loc.cit.

119 HANSEN, NISSENBAUM, op.cit., p.1163.

güvenlik ve uluslararası güvenliğe etkilerinin olduğu gerçeğine dayanmaktadır. Geçmişte, Milli Güç Unsurları içerisinde adı sadece "*Askeri Güç*" içerisinde yer alan teknoloji ve siber uzaydaki kabiliyetler, artık kendi başına bir güç unsuru olmuştur. Siber uzay güvenliği ulusların güvenliğini doğrudan etkilemekte, uluslararası güvenliği koruma adına tahmin edilemez sonuçlar doğurabilmektedir.

1.2.4. Siber Güvenlik Modelleri

Kopenhag Okulu, sektörlerin spesifik yollarla tanımlandığını, bu yollar içerisindeki farklı alt formlar veya gramerlerin referans objelerini, tehditleri ve güvenlik aktörlerini birbirine bağladığını söylemektedir.[120] Bu bölümde siber sektöre özgü iki güvenlik modellemesinden bahsedilecektir.

1.2.4.1. Yüksek güvenlikleştirme

İlk görüş olan "*Yüksek Güvenlikleştirme*" Buzan[121] tarafından, "*hem tehditlerin abartılması hem de abartılı karşı önlemlerin kullanılmaya başlamasına olan eğilim*" tanımlanarak güvenliğin normal tehdit ve tehlike seviyeleri dışına çıkması olarak açıklanmaktadır. Bu tanımla "*abartılı tehditler*" tanımlanarak, abartılmayan "*gerçek*" tehditlerin olduğu doğrulanmaktadır. Ayrıca, güvenliğin abartılmış olup olmadığı sorusu, onun başarılı olduğu dereceyi gösterir.[122]

Tüm güvenlikleştirmeler karşılık vermesi zorunlu tehditler içermeleri açısından hipoteze dayalı bir element içerirler ve bu sebeple "*...sa – sonra*" mantığı kullanırlar. Ancak yüksek güvenlikleştirmeyi basit güvenlikleştirmeden farklı kılan anlık oluşumu ve birbirinin içine geçen etkiler yaratmasıdır.[123] Bu kombinasyon, ağın güvenliği için kritiktir, ancak yine de yüksek güvenlikleştirmenin gücü, yalnızca ağın kendi başına güvenliğini sağlamasından değil, zarar görmüş bir ağın nasıl sosyal, finansal ve askeri yıkımlara neden olacak ve dolayısıyla tüm diğer referans objelerini ve sektörleri bir araya getirecek olmasından kaynaklanmaktadır.[124]

---

120 Ibid., p. 1164.

121 BUZAN Barry, **The United States and the Great Powers: World Politics in the Twenty-First Century**, Cambridge, 2004, Polity Press, http://books.google.com.tr, (e.t. 31.12.2011), p.172.

122 HANSEN, NISSENBAUM, op.cit., p. 1164.

123 DENNING, op.cit., p.xiii.

124 DEIBERT, loc.cit.

Soğuk Savaş'a bakıldığında, nükleer önleme mantığı henüz gerçekleşmemiş bir nükleer değişimin yansımalarına dayanmakta, ayrıca nükleer savaşın neler olacağını gösteren Hiroşima ve Nagazaki yıkımları da bu konuda örnek oluşturmuştur. Diğer taraftan siber güvenlik, dayanak sağlayacak olaylar tarihine sahip değildir. Ancak Elektronik Pearl Harbor gibi tarihsel analojiler yaratılmaktadır. Felaketler ve daha önce bu büyüklükte bir olayın olmamış olmasının birleşimi, siber güvenlik konusunda önemli bir ikilem yaratmaktadır. Geleceğe çok fazla güvenilmesi ve tehditlerin çokluğu, konuyu "*abartmaya*" karşı açık bırakmakta, potansiyel yıkımın ölçeği, eş zamanlı olarak uyarıların göz ardı edilmesine bağlı tehditleri arttırmaktadır. [125]

Siber güvenlik içinde tüm ağın yüksek güvenlikleştirme, gezegenin kaderinin tehlike altında olduğunu iddia eden çevresel güvenlik konusuna açık bir benzerlik yaratmaktadır. Her iki konuda geriye döndürülemezlik içermektedir. Bir tür yok olduğunda ya da bir dijital sistem yok olduğunda hiçbir zaman tam olarak yeniden yaratılamazlar. Ancak, ikisi arasında önemli farklar da bulunmaktadır. İlk olarak; tehdit senaryolarının hızı, gücünü yok edici etkilerin anlık olmasından alırken, çevresel güvenlik genellikle belli bir sınıra ulaşıncaya ve olaylar hızlanıncaya kadar, tehditlerin ve tehlikelerin adım adım birikmesine izin vermektedir. Bu şekilde aciliyet için değişik modeller ve dolayısıyla politik müdahale için farklı alanlar oluşturmaktadır. İkincisi, tehditleri görüntüleme olasılığı ve buna bağlı olarak güvenlik aktörlerinin dinleyicileri ile nasıl iletişim kuracağı konularında farklılıklar vardır. Siber güvenliğin dijital, bağlantılı karakteri ve önceki felaketlerin yokluğunun imajlarla sunulması zordur.[126]

1.2.4.2. Günlük güvenlik uygulamaları

İkinci olarak, günlük güvenlik uygulamaları, özel organizasyonlar ve kurumları da içeren güvenlik aktörlerinin, normal bireylerin tecrübelerini iki yolla bir araya getirmesine dikkat çekmektedir. Bu iki yol şunlardır: Ağ güvenliğini sağlamada bireylerin ortaklığını ve anlaşmalarını güven altına almak ve felaket senaryosunun elementlerini, günlük yaşantıda olağan olan tecrübelere bağlayarak yüksek güvenlikleştirme senaryolarını daha gerçekçi hale getirmek. Hansen'e göre günlük güvenlik uygulamaları, birey güvenliği anlayışını tekrar

---

[125] BENDRATH Ralph, "The American Cyber-Angst and the Real World – Any Link? In Bombs and Bandwidth", akt. Robert LATHAM, **The Emerging Relationship Between Information Technology and Security**, , 2003, New York, The New Press, p.50.

[126] WILLIAMS, loc.cit.

oluşturmamaktadır. Kamu güvenliği yöntemlerinin kabulünün, bireyin yaşanmış ve sağlam tecrübeleri ile hızlandırabileceği gerçeğine yeterli önemi vermemektedir. [127]

Günlük güvenliğin elementlerinin başka sektörlerde de bulunabilecek olmasına rağmen, özellikle siber güvenlikte açıkça ortaya çıkmaktadırlar. Örneğin; Soğuk Savaş'taki, günlük yaşantının yok oluşuna sebep olacak nükleer felaketin askeri olarak güven altına alınmasıyla, kredi kartı dolandırıcılığı, kimlik hırsızlığı ve e-posta casusluğu olan günlük dijital hayatın güven altına alınması arasında belirli farklar bulunmaktadır. Bilgisayar sahibi olmayan ya da iş bilgisayarı bulunmayan azınlık, dijitalleşmenin sonuçlarından hiçbir zaman etkilenmeyecektir. Kopenhag Okulu'nun kabul ettiği gibi bu tehdit tecrübeleri "*kişisel güvenlik*" veya "*suç*" durumları değil, ağlara ve dolayısıyla halka karşı tehditlerdir.[128]

Günlük yaşamda siber güvenliğin sağlanması, bireyi, yalnızca güvensizlikle savaşmadan sorumlu ortak olarak değil, aynı zamanda bir sorumluluk veya bir tehdit olarak görmesi açısından farklıdır. Dolayısıyla hem kamu hem de özel kuruluşlar, güvenliği ile alakalı olarak uzman pozisyonlar oluşturmaktadır. Eş zamanlı olarak bir eğitim ve güvenlik yöntemi uygulanırken, ABD Federal Ticaret Komisyonu tarafından kurulan "*On Guard Online*" ın uyardığı gibi, örnek olarak bir dosya paylaşımı sırasında "*Telif Hakları Kanunları tarafından korunan bir dosya indirilebilir ve kanuni yaptırımlara çarptırılabilir. Bir virüs indirilebilir ya da güvenlik sızıntısı hızlandırılabilir.*" Dijitalin tehlikeli görülmesi ve sıradan bir bireyin potansiyel bir tehdit olarak görülmesi "*virüsler*" ve "*hastalık bulaşmış bilgisayarlar*" gibi "*önlem*" ve "*koruma*" gerektiğini belirten tıbbi benzetmeler oluşturmaktadır. Siber güvenlik, bir bütünün sağlığını etkileyecek şekilde sorumsuzca davranan bireyler tarafından oluşturulmaktadır. "*The National Strategy*" belgesinde belirtildiği gibi "*Siber uzaya, bilgi ağına bağlı her birey sahip oldukları ya da sorumlu oldukları alanı güven altına almalıdır.*" ayrıca FBI yetkilileri, bilgisayar sahipleri için bilgisayar ehliyeti önermişlerdir. Bir endişe de, bilgisayar sahibine hiçbir anlık etki yapmayacak saldırıları ve e-postaları yönlendirecek saldırganlar tarafından kullanıma izin veren yazılımlar tarafından ele geçirilmektir. Günlük güvenlik uygulamaları, yıkıcı senaryolarla birbirine bağlandığında, siber güvenlik kurumsal güvenlik veya tüketici güvenliği alanlarının dışına çıkaran ve milli/sosyal güvenlik içerisine sokan, bir ağ sistemi içerisindeki bu zarar verici ve dikkatsiz davranıştır. Bunların yanında yüksek güvenlikleştirme

127 HANSEN, NISSENBAUM, op.cit., p.1165.
128 Ibid.

ve günlük uygulamalar arasında bir bağlantı daha vardır. Bu da yaşanacak felaket olasılıklarının, bireylerin günlük deneyimleri tarafından kanıtlanabileceği iddiasıdır. [129]

Sonuç olarak; Hansen ve Nissenbaum'un eserinde vurguladığı üzere günlük dijital yaşamda hükümet otoritesi ve aynı zamanda özel kurumlar için güvenliğin sağlanması sırasında oluşan zorlukla oldukça önemlidir. Güvenlikleştirme Teorilerinde, güvenlik konusunun hükümetleri, radikal önlemle almak için politik yetkilerle donatması konusundaki kritik tartışmasına geri dönmek gerekirse, soru şu hali almaktadır: Bu stratejiler ve bunların devlet-ulus ilişkileri konusundaki harmonik birleşimleri hangi noktada ve nasıl tartışılabilir?[130]

Çoğu akademik alanda olduğu gibi, bilgisayar bilimcileri farklı formda atakların olma ihtimali konusuna katılmamıştır. Bu alan ayrıca askeri ve iş hayatındaki gizliliğe bağlı olduğu için, bu tartışmaların takipçileri, birçok şeyin açığa çıkartılmadığını söylemektedirler. Yıkım tahminlerinin stratejik olarak ya çok abartıldığını ya da olduğundan az gösterildiğini belirtmektedirler. Bu dalgalanmalar aynı zamanda, radikal tehditlerin "*tekno-ütopik*"[131] çözümlerle eşleşmesini hızlandırmaktadır. Gelecekte, bir bilgisayarla, internetle ya da başka her hangi bir siber sistemle çalışmak, ışıkları veya suyu açmak kadar gerekli olacaktır.[132]

Siber dünya da uzman otoriteler oluşturmak; iyi bilgi-kötü bilgi arasında ve bilgisayar bilimci ile bilgisayar korsanı arasında zayıf bir bağ oluşturmaktadır. Nissenbaum'un[133] iddia ettiği gibi, Batı politikası ve medyasında, "*bilgisayar korsanları*" kodları kırma noktasından, hırsızlık, saldırı, hatta terörist davranışlara bile varan kritik bir atlama yaşamışlardır.

Bilgisayara, siber güvenlik yöntemi içerisinde verilen öncelikli rol, güvenlikleştirmenin kendi mantığının bir ürünüdür. Eğer siber güvenlik bu kadar önemliyse benim görüşüme göre uzman olmayan personele bırakılmamalıdır. Bilgisayar kullanıcıları ve mühendisleri yalnızca uzmanlar değil, aynı zamanda teknik kişilerdir ve siber güvenliği bunların alt yapısı olarak kurgulamak siber güvenliği teknikleştirmektedir. Güvenlik gibi teknik bilgiler de düz bir şekilde tanımlayan değil, bir şeyler yapan özelliklerdir. Teknik bilgiye dayalı konular inşa eder aynı zamanda teknolojinin sağladığı politik, normatif ve

---

129 The White House, op.cit., p. 11.
130 HANSEN, NISSENBAUM, op.cit., p.1166.
131 NISSENBAUM, op.cit., p.72.
132 HANSEN, NISSENBAUM, op.cit., p. 1167.
133 NISSENBAUM Helen, **Hackers and the Contested Ontology of Cyberspace**, 2004, New Media & Society.

tarafsız konular önerirler.[134] Teknik bilgi, halkın ve çoğu politikacının sahip olmadığı bir uzmanlık gerektiren bir altyapı olarak inşa edilir. Bu bilgiye sahip teknik uzmanların, politikacı ve diğer politik aktörlerden ayrı güvenlik aktörleri haline gelmelerini sağlar. Teknik ve güvenlik birbirine karşı durumlar ya da bağlantılı modeller olarak görülmemeli, aksine karmaşık ve bağlayıcı yollarla bir araya getirilebilecekleri bilinmelidir. [135]

Kopenhag Okulu "*güvenlikdışılaştırma*"yı bir durumun güvenlik alanı dışına çıkması ve politik alanı içerisine girmesini en uygun uzun vadeli seçenek olarak açıklamaktadır. Çünkü karşı önlemlere sahip olunan tehditlerin bir anlamı olmayacağı, ancak bunları tehdit-savunma halinden çıkarıp sıradan halk çerçevesi içerisine sokmanın anlamlı olacağını söylemektedir.[136]

Çevresel güvenlik hakkındaki kamu tartışmaları ile karşılaştırıldığında, çevresel güvenlikte, dinleyicinin daha fazla şey bilmesinin beklenmesi ve bazı çevresel aktörlerin, kanıtların halka sürekli sunulması, bunları apolitik, objektif yerine politik uzmanlar yapmaktadır.[137] Bu durum bilgisayar biliminin, çevre biliminden daha teknik ya da daha az politik olduğunu göstermez. Ancak basitçe, sosyal içerikli dinleyici-uzman pozisyonlarının değişebileceğini gösterir. Bu değişim güvenlikleştirme ile nasıl mücadele edileceği ve kanunlaştırılacağını göstermesi açısından önemlidir. Bu değişimler hükümet, askerî ve akademi çevrelerinden birçok birey tarafından kabul edilmiştir. Fakat bilgiyi gerçekten faydalı kılan şey onun kullanımı ve taşınabilirliğidir. Bilgiyi dönüştürebilme, gücünü taşıma veya sergileyebilme becerisi doğrudan bilginin taşınabilirliği ile ilgilidir. Teknoloji, işte bu anlamda güç yapısını kökten değiştirmiştir. Bir zamanlar birbirinden bağımsız olan alanların birleşmesi, herkesin bilgiye ulaşmasını ve dünya çapında dağıtmasını sağlamıştır. Bu fikirler bilginin gerçek gücünü göstermesi bakımından önemlidir ve değişen de işte bu fikirlerdir.[138]

Siber tehditler gibi yeni ortaya çıkmaya, varlıklarını hissettirmeye başlayan diğer tehdit unsurları, doğal olarak güvenliğin genişlemesi ve derinleşmesini bir zorunluluk haline getirmiştir. "*Siber Güvenlik*", "*Bilişim Güvenliği*", "*Bilgi Güvenliği*", "*Sanal Güvenlik*", "*Sayısal Bilgi Savaşı*" gibi başlıklar altında yeni güvenlik alanları şekillenmeye başlamıştır. Böylesi bir değişim süreci bireylerin, devletlerin ve uluslararası yapının de güvenlik

134 HUYSMANS Jef, **The Politics of Insecurity: Fear, Migration and Asylum in the EU**, 2006, London, Routledge, http://books.google.com.tr, (e.t. 31.12.2011), p.6-9.
135 HANSEN, NISSENBAUM, op.cit., p. 1168.
136 BUZAN, op.cit., p.29.
137 Ibid.
138 KUEHL Dan, **Enformasyon Harekâtları: Yumuşak Gücün Sert Gerçeği**.

algılamalarını dönüştürmesi gerekliliğini ortaya çıkarmıştır.[139] Geleneksel olmayan bu yeni tehditlerle mücadele araçları da farklılaşacaktır. Örneğin, günümüzde bir devlet olası bir bilgisayar korsanı saldırısı ile geleneksel savaş doktrini veya savaş silahları ile mücadele edemez. Bu bağlamda askeri önlemlerin içerisine siber güvenlik önlemleri de dâhil edilmeli, dolayısıyla bilgisayar mühendisleri ya da uzmanları ilgili ülkenin ulusal savunma yapılanmasında daha etkin roller oynamalıdır. Dünya henüz siber saldırının ne zaman başladığına ve meşru savunma hakkının ne zaman başlayıp ne zaman biteceğine bir cevap bulamamıştır. Bir siber saldırı karşılığın da aynı oranda bir saldırı meşru mu sayılacak yoksa konvansiyonel bir saldırı için yeterli bir meşru savaş ortamı oluşmuş olacak mı? Bu henüz belirsizdir. Kim bilir belki de bu sorularımın cevapları gelecekte var olacak olan bir bilgisayarın tuşları arasındadır.

139 Ibid.

İKİNCİ BÖLÜM

SİBER UZAY GÜVENLİĞİNİN ULUS GÜVENLİĞİNE ETKİLERİ

Bilgisayar ağlarının artmaya başlamasıyla birlikte ağa yönelik güvenlik tehditleri de yaşanmaya başlamıştır. Bu olayların bir kısmına bilinçsiz kullanıcıların neden olmasına karşın, bir kısmına da bilerek sisteme zarar vermek isteyen kötü niyetli kişiler neden olmaktadır. 1980'li yıllarda bilgisayar haberleşmelerinde TCP/IP protokol ailesi dünya çapında kabul görmüş ve internet bu protokolü aracılığı ile yaygınlaşmıştır. İnternetin yaygınlaşması ile bilgisayar haberleşmelerindeki atakların sayısı ve çeşidi de artmıştır. Bu ataklar karşısında kimlik doğrulama, yetkilendirme, anti-virüs programları gibi güvenlik çözümleri geliştirilmeye çalışılmıştır. İlk çıkan ataklar daha çok basit kod yürütme, parola tahminleri gibi etkisi ve olasılığı düşük ataklar olmasın karşın süreç içerisinde atakların karmaşıklığı ve etkileri artmıştır. Buna karşın bu atakları kullanabilmek için gereken bilgi düzeyi düşmüştür. Çünkü bu bilgiler çoğunlukla internet üzerinden kontrolsüz olarak yayılmıştır.[140] Öyle ki siber uzayda, bomba yapımının yanında, bubi tuzağı hazırlamaya kadar her şeyi bulmak mümkün olmuştur.

Suç örgütleri, bilgisayar teknolojisini kullanarak kendilerine geniş sahalar yaratmış ve ulusların iç güvenliğini de etkileyen yeni suç alanları bulmuştur. Globalleşmenin karanlık yüzü olarak adlandırabileceğimiz bu gelişme, toplumsal barışı ve ulusal güvenliğimizi ciddi şekilde tehdit etmiştir. Güvenlik anlayışındaki bu değişim, insanları ve sınırları birbirlerine daha fazla yaklaştıran teknolojik gelişmelerin ve ortaya çıkan küreselleşmenin bir sonucu olarak ortaya çıkmıştır. Ulus güvenliğinin artık en önemli parçaları arasında sayabileceğimiz resmi internet sitelerinin bilgisayar korsanları tarafından çökertilmesi 21. yüzyılda bilişim suçlarının en önemli suç türleri arasında yerini alacağının önemli bir kanıtı olmuştur.[141]

Çalışmamızın ikinci bölümünde siber uzay güvenliğinin ulus güvenliğine etkileri üzerinde ayrıntılı olarak durulmuştur. Siber güvenliğin askeri alanda yer alan konseptler üzerinde neden olduğu değişikliklere değinilmiş ve siber saldırıların ulus güvenliğine etki eden hassas tarafları nedenleri ile birlikte açıklanmaya çalışılmıştır.

---

140 KARA Mehmet, Hayretdin BAHŞİ, "Bilişim Güvenliği Araştırmalarının Yönü", **TÜBİTAK-UEKAE**, http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html, (e.t. 06.02.2012).

141 ÖZCAN Mehmet, "Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu", www.manisabilisim.org/dokuman/siberteror.pdf, (e.t. 16.02.2012).

Kişisel bilgisayarların gelişmesi bilgi ve iletişim teknolojisinin de gelişmesine yol açmıştır. Bu gelişmeler komuta kontrol sistemleri üzerinde geniş çaplı uygulama imkânı bulmuştur. Savaşlarda kullanılan silahlardaki teknolojinin mevcut silahlardan daha etkili ve ucuz olarak yararlanılmasını sağlamıştır. Yeni imkân ve kabiliyetler sisteme adapte edilmeye çalışılmıştır. Öyle ki savaşların seyrini değiştirecek boyutlara ulaşmıştır. Öncü çalışmaların ABD'de yapıldığı savaş teknolojisi, bilginin etkin olarak sağlanması ve yerinde kullanılması konularını kapsamıştır.[142] Soğuk Savaş döneminde öncelikli olarak askeri bir teknoloji sonucu ortaya çıkan internetin, bütün dünya tarafından kullanılmaya başlanması ve internetin kendisine ait yeni teknolojileri üretebilecek bir yeteneğe ulaşması, dünya tarihindeki önemli dönüm noktalarından biri haline gelmiştir.

"*Bilgi toplumu*" terimi, Japon gelecek bilimci (futurulogist) Yoneji Masuda tarafından türetilmiştir. Masuda 1990'larda bu terimi ilk kullandığında, internet bu kadar yaygınlaşmamıştı. Günümüzde ise internet dünya çapında bir milyar kişi tarafından kullanılmaktadır. Buradan Masuda'nın öngörüsünün gerçekleşmekte olduğu sonucu çıkarılabilir. Ancak, internet sadece bir teknolojidir. İnternet, insanların özünde iyi oldukları inanışına dayanmaktadır ve bu inanış suiistimallerin ortaya çıkma ihtimaline imkân vermektedir. Bilgisayar virüsleri ve toplu elektronik postalar bunlara örnek olarak gösterilebilir.[143]

Günümüzde web bazlı virüs saldırıları internet üzerinde çok yaygınlaşmıştır ve web tabanlı tehditlerin daha karmaşık hale geldiğini ve sayısının da arttığı anlaşılmaktadır. İnternet üzerindeki güvenlik açıklarının %73 oranında web teknolojileriyle ilişkili olduğunu söyleyebilir. Web sitelerinin %83'ü, en azından bir kez ciddi bir güvenlik tehdidiyle karşı karşıya gelmiştir. Web sitelerinin %64'ü ise halen siber saldırganların ve başka kötü niyetli kişilerin saldırılarıyla karşı karşıyadır.[144] Eskiden siber saldırı gerçekleştirmek ve sistemlere girebilmek için gerekli olan teknik bilgi ihtiyacı üst seviyede olmakla beraber, günümüzde bu ihtiyaç azalmış, çok rahatlıkla temin edilebilen tehlikeli araçlar internette ücretsiz olarak

---

142 ÇOLAK H.Cahit, "Harbin Değişen Yüzü: Askeri Alanda Devrim ve Transformasyon", **Harp Akademileri Bülteni**, Mart, 2004.

143 TSUCHIYA Motohiro, "Siber Terörizm Tehdidi ve Önlemler", Küresel Terörizm ve Uluslararası İş Birliği, **II. Uluslararası Sempozyum Bildirileri**, Ankara, 10–11 Mart 2008, ss. 195–200.

144 ÜÇÜNCÜ Murat, "Siber Savunmada Mücadele Alanları ve Sistem Yönetiminin Önemi", Küresel Terörizm ve Uluslararası İş Birliği, **III. Uluslararası Sempozyum Bildirileri**, Ankara, 15–16 Mart 2010, ss. 55–61.

bulunmaktadır. Ayrıca teknoloji bağımlılığı arttıkça, verilebilecek zararlar üst seviyeye çıkmaktadır.

Siber güvenliğin ulus güvenliğini hangi noktalarda etkileyeceği, ekonomik ilişkilerin siber uzaydaki sanal malvarlıklarını ulus güvenliği içerisinde değerlendirdiğimiz de etkilerinin tahmin ettiğimiz gibi mi olacağı soru işaretleri arasındadır. AB gibi örgütlerin yasama zemininin belirlenmesinin yanı sıra sistemlerinin işleyişi hakkında daha genel anlamda karmaşık sorular akla getirmektedir. Üstelik bu anayasal ve yasal çerçeveler hem ticarî kuruluşlar gibi organizasyonlar hem de vatandaşlarla ilgili davranış sorunlarıyla doludur. Bu sorunlardan bazıları ticaretin özellikle de şimdi birbiriyle bağlantılı, küresel bir ortamda elektronik ticaretin, yapısıyla ilgilidir. "*E-ticaret faaliyetleri ulus devletin egemenliğini muhakkak aşar mı?*" sorusu özellikle geçerlidir. "*Elektronik olarak birbiriyle bağlantılı bir dünyada vatandaşlar nasıl davranıyor?*" ve "*Bu davranışlar hangi ölçüde ulus devlet egemenliğini aşıyor, hatta önemsiz kılıyor?*" gibi sorular konuyla özellikle ilgilidir.[145]

2009 yılında dünyada ortalama 2,2 saniyede bir yeni virüs siber uzaya girmekteydi. Anti-virüs şirketleri ise ancak on virüsten birini temizleyecek imkânlara sahip olabiliyordu.[146] Bunları düşündüğümüzde tehdit boyutunun ne denli büyük olduğu, buna karşın ise savunma için ne kadar hazırlıksız olduğumuz sonucu çıkabilmektedir. Klasik savaş doktrinleri ile bu düşmana karşı savaşı kazanmamız çok zor gözükmektedir. Süratle bilgi çağının yeni savaş şekillerine adapte olmamız ve buna göre ordularımızı şekillendirmemiz gerekmektedir.

Bilgisayar zararlı yazılım ve ataklarına karşı proaktif önlemler alınması ve bu sistemlerde güvenliğin sağlanması için birçok kuruluş ve ülke tarafından çok sayıda araştırma geliştirme projesi yapılmıştır ve hala da yapılmaktadır. Bu projeler sonucunda bilgisayar sistemlerinde kullanılan anti-virüs yazılımları, güvenlik duvarları, VPN (Virtual Private Network)[147] yazılım/donanımları, saldırı tespit ve önleme sistemleri, içerik kontrolcüler, merkezi yönetim yazılımları geliştirmiştir. Geliştirilen bu teknik çözümlere paralel olarak

---

145 TAYLOR John, "Bilgi Çağı ve Teknolojik Gelişmelerin Devlet Yönetimine Etkileri", **Üçüncü Uluslararası Sempozyum Bildirileri**, Genelkurmay Basım Evi, İstanbul, 12–13 Mayıs 2005, SAREM, s.110.

146 CLARK Richard A., Robert K. KNAKE, **Siber Savaş**, Çeviren Murat ERDURAN, İstanbul Kültür Üniversitesi, İKÜ Yayın Evi, 2010, s.50.

147 Sanal paylaşımlı ağ olarakta tanımlayabileceğimiz VPN, asıl çalışma mantığı aslında olamayan ama farklı hatlar üzerinden ki tüm DSL sistemleri, uydu bağlantıları, kablo net yapıları, hatlar üzerinden farklı noktada olan iki noktayı aynı ağda çalıştırmak içindir. Örnek vermek gerekirse iki farklı ülkede iki ayrı ofisimiz var ve bunlar arasında bir alt net kurmak istiyoruz işte burada devreye VPN girecektir.

bilişim sistemlerinin güvenli olarak tasarlanmasını ve yönetilmesini sağlayacak standartlar ve çerçeveler oluşturulmaktadır.[148]

Günümüzde bilişim teknolojileri (BT) güvenliği araştırma geliştirme projelerine hem çok büyük bütçeler hem de büyük iş gücü ayrılmaktadır. Çok büyük bütçe ve insan kaynağı ayrılmasının başlıca nedenleri internetin insan hayatında vazgeçilmez bir araç olması, e-devlet, e-ticaret, e-sağlık, e-eğitim, askeri, iletişim, araştırma, eğlence gibi birçok uygulama için çok etkin ve ekonomik çözümler sunmasıdır. Ülkeler ve şirketler bilgisayar güvenliği alanlarındaki uygulamaları kendi ülkelerinde kullanmanın yanı sıra diğer ülkelere satarak hem teknolojik hem de ekonomik olarak pazarda öne geçmek istemektedirler. AB 2007–2013 yılları arasında desteklenecek olan 7. Çerçeve programları kapsamında toplam bütçenin %32'sini güvenlik ve bilgi iletişim teknolojileri alanlarındaki araştırma geliştirme projelerini desteklemek için ayırmıştır.[149]

1. ULUSAL EGEMENLİK VE GENEL AĞ

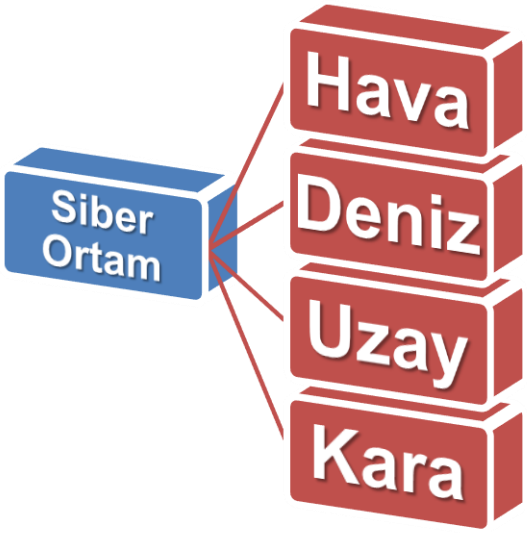
Her ne kadar ilk bakışta çelişkili gibi gözükse de internet teknolojisi çok yaygın bir şekilde paylaşılmaktadır ve birinin istemesi halinde kötüye kullanılabilme özelliğine sahiptir. Hakkında pek fazla bilgisi olmayanlara internet teknolojisi, kara kutu gibi gelebilir; ancak eğitimli bir göz için internet teknolojisi çok basittir. İnternet aynı zamanda kocaman bir kopyalama makinesidir ve bu teknoloji hızlı bir şekilde yayılmaktadır. Buna ek olarak, yayılma yöntemleri çeşitlidir ve bütün çeşitlerinin takibi hiç mümkün gözükmemektedir.[150]

İnternet birçok kişinin tahmin ettiğinden daha fazla bilgi yığını içermektedir. Örneğin, internete bağlandığınızda bilgisayarınızın IP numarası belirli aralıklarla kaydedilmektedir. IP adresi statik değildir, zaman ve yere bağlı olarak değişmektedir; ancak çeşitli kayıtlar bir araya getirilerek bir internet kullanıcısını tespit etmek imkânsız değildir.[151]

Siber ortam veya diğer bir adıyla siber uzay, Şekil -1'den de anlayabileceğimiz gibi; kara, deniz, hava ve uzay gibi ortamları da içerisinde barındırır. ABD ordusunda yapılanma bu ortamlar dikkate alınarak kendi bünyelerinde oluşturdukları siber güç kuvvetleri ile

148 KARA, BAHŞİ, loc.cit.
149 Ibid.
150 TSUCHIYA, loc.cit.
151 Ibid.

yapılandırılmıştır. ABD kara gücü kendi bünyesinde siber saldırılara karşı savunma ve aynı zamanda saldırı yapabilecek ekiplerini oluşturmuştur.[152]



Şekil 1- Siber Ortamın Kapsadığı Alan

Genel ağda, ortak dil olarak İngilizce giderek daha çok kullanılmaktadır, dolayısıyla ana dili İngilizce olmayan uluslar kendilerini bu açıdan mahrum hissedebilirler. Genel ağ, açık siyasî söylemler için bir kaynaktır ve sonuç olarak da demokrasiyi geliştirmektedir. Ancak aynı zamanda demokratik ilkeleri baltalamaya ve demokratik açıdan meşru hükümetleri devirmeye çalışan kişiler için de kaynak oluşturabilmektedir. Geleceğin dünyasında ulusların varlığında siber unsurların her çeşidinin etkisinin olacağını söylemek son derece doğru bir tespit olacaktır.

Genel ağın belirsiz yapısı onu sosyal, siyasî ve iktisadî etkinliğinin saptanması zor olan bir araç hâline gelmesine sebep olmuştur. Genel ağ, e-ticaret için büyük fırsatları beraberinde getirmektedir. Fakat bu fırsatlar beraberinde bazı durumlarda ahlâkî yönden çirkin, bazı durumlarda da ulus devlete karşı olarak nitelendirilen kötü niyetli faaliyetlere de her zaman ve her yerde erişebilmeyi mümkün kılmıştır. Diğer bir ifade ile genel ağ, pek çok meşru ve istenen faaliyetin gelişmesini sağlarken aynı zamanda da kimlik hırsızlığının çeşitli biçimlerini de içeren suç eylemleri için bir arena hâline gelmektedir. Hükümetler kendi kanunları çerçevesinde genel ağı oldukça faydalı potansiyelinden dolayı desteklerken, bazı

152 Ibid.

ticarî şirketler belli bir devletin kanunlarından kaçmalarını sağlayacak mantıklı kararlarla bu kanunlardan kendilerini muaf tutmaya çalışmaktadırlar.[153]

Terörizm ise siber uzayın olanaklarını kullanarak en büyük güvenlik sorunu hâline gelmiş ve küresel boyut kazanmıştır. Uluslararası terörizm, bilgi teknolojilerinin olanaklarını kullanarak yanıltma haber ve psikolojik harekât vasıtasıyla kitle hareketlerini yönlendirmek suretiyle amaç ve eylemlerini desteklemektedir. Genel ağın ortaya çıkmasından sonra siber uzayın kullanımı ve suiistimal edilmesiyle ilgili belirsizlikler ve ikilemler ortaya çıkmıştır. Bu düzenlemelerin hepsi genel ağın geleneksel düşünce şekillerine ve ulusal egemenliğe karşı arz ettiği büyük tehlikeleri vurgulamaktadır. Pek çok açıdan siber uzay, uluslararası etkiler doğuran fakat kendilerini yönetecek bir üst kurulu veya kuralları olmayan uluslararası faaliyetler dizisi geliştirmektedir. Hükümetler bu faaliyetleri kontrol altına almada yetersiz kalırken ticarî şirketlerin ve bireylerin düzenleyici kurallardan kaçma becerileri giderek artmıştır.[154]

Siber uzay, güvenli bir şekilde yönetilmek istenirse pek çok zorlukla karşılaşacaktır. Mesela oluşturulacak bir siber üst yönetim organizasyonu dünya çapındaki genel ağ toplumunu tarafsız şekilde temsil etmelidir. Güçlü bir ulusu, kurumu veya kişiyi desteklediği için bu üst yapı insanlar tarafından suçlanabilir. Eylemlerinden dolayı genel ağ kullanıcısı olan tüm dünya devletlerine karşı sorumlu olmalıdır. En önemlisi, genel ağda hangi davranışların ve içeriklerin kabul edilebilir olduğu konusunda dünya çapında bir tartışma başlatmalıdır. Genel uluslararası kabuller ortaya konmalıdır. Siber uzay içerisinde cevaplanmayı bekleyen çok sayıda soru vardır. İnsanlık rönesans veya reform hareketlerinden geçerek belli kararlara vardı ve insan hayatını aynı zamanda devletin varlığını sorguladı. Şimdi sıra yeniçağın artık sorun haline gelmeye başlayan sorularına cevap bulmaya gelmiştir. Siber uzayın sınırları olacak mı? Bu sınır nerede başlayıp nerede bitecek? Birey siber uzayda nasıl korunacak ve kim tarafından temsil edilecek? Siber uzaydaki sorun ne zaman uluslararası bir sorun haline gelecek? Bu sorular uzayıp gidecek ama en temel soruların yanıtları uluslararası yapı tarafından sorgulanmadığı sürece yeni sorular arkasında büyük problemler ile gelecektir.[155]

153 TAYLOR, op.cit., s.126.
154 Ibid.
155 Ibid.

2. ASKERİ ALANDA KONSEPT DEĞİŞİKLİĞİ

Bilgi çağının getirdiği değişimin askerî alana etkisi Askerî Alanda Devrim (AAD) olarak nitelendirilmiştir. Geleneksel Harp Prensipleri* ve muharebe usullerine göre tasarlanmış askerî teşkilatlar stratejik, operatif ve taktik alanda olduğu gibi onların konsept, doktrin, teşkilat yapısı, donatım, liderlik ve eğitim öğretim yapısı, insan kaynakları, tesisler ve tüm bunları yönetecek komuta kontrol sistemlerinin yapısında da değişime zorlamıştır.[156]

Bilgi ve teknoloji devrimi, bir zamanlar askerî alanda daha az önemsenen aktörler lehinde daha fazla dikkat sarf edilmesini, bunlara paralel olarak daha düşük yoğunlukta tehdit teşkil ettiği varsayılan ve olayların daha fazla önem kazanma potansiyeline sahip olabileceği düşüncesini öne çıkarmıştır. Bütün bu değişiklikler nedeniyle silahlı çatışmaların sebep, uygulama ve sonuçları üzerinde kaçınılmaz aynı zamanda önemli etkiler meydana gelebileceği gerçeği ile yüz yüzeyiz kalınmıştır. Bu husus bizi harbin değişen yüzünü görmeye itmektedir. Bundan böyle kendilerini bilgi ve teknoloji alanına iyi entegre eden orduların, elde ettikleri doğru değerlendirilmiş ve gerçek zamanlı bilgileri, uygun şekilde teşkilatlanmış kuvvetlerine ve hassas şekilde güdülen silahlarına (Precision Guided Weapons) entegre ederek gelişmiş C4I (Command, Control, Communications, Computers, and Intelligence; Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat) unsurları ile çok daha etkin bir vurucu güce ulaşacakları muhakkaktır.[157]

Körfez Savaşı'nda silah, iletişim ve bilgi teknolojilerindeki ileri düzey gelişmeler askerî yeteneklere dönüştürülmüştür. Silahlar hedeflere daha hassas bir şekilde yönlendirilmiştir. Keşif ve gözetleme sistemleri ile karşı kuvvetlerin yapısı ve yeri hakkında çok detaylı bir şekilde bilgi sağlanmıştır. Analiz ile dağıtım sistemlerinin entegre kullanılması sonucu bilginin hızlı bir şekilde dağıtılması ve kullanılması neticesinde askerî alanda devrime olan ihtiyaç kendini kanıtlamıştır.[158] Siber uzayın etkisi en fazla savaş alanındaki silahların etkili ve isabetli vuruşlarında kendisini göstermiştir.

Anthony Robbins modern dünyayı karakterize etmek için şu benzetmeyi yapmıştır; "*Modern dünya hayal edilebileceğinin ötesinde muazzam bilgi akışı ve bunun getirdiği*

---

* Harp Prensipleri, harp sanatı içerisinde taarruz, siklet merkezi gibi prensipleri olan ve harbin bu prensipler temelinde açıklandığı kavramlardır.

156 ÇOLAK, loc.cit.

157 Ibid.

158 Ibid.

değişikliklerdir. ”[159] Sanayi toplumunda ön planda olan "*maddi*" ürünlerin üretimi yerine, bilgi toplumunda, bilişim teknolojisi sayesinde bilgi üretimi önem kazanacaktır. Böylece bilgi toplumunun sürükleyici gücü ve en başta gelen kaynağı bilişim teknolojisinin ürünü olan bilgidir. Bilişim bilgisi; bilgisayar sistemleri içinde bilimsel usullerle işlenip elde edildiği için, ferdi keyfilik ve saptırmalardan uzak olması sebebiyle daha objektif bir özelliğe sahip olacaktır.[160]

Güvenlik testlerinin gerçekleştirildiği noktalarda uzmanların yetersiz kalması, yani gelişmeleri takip etmemeleri, orta ve uzun vadede eldeki bilginin eskimesine ve ihtiyaçları karşılayamamasına sebep olmaktadır. Bilgi güvenliği, doğası gereği devamlı yenilenme ihtiyacı olan bir sektördür. Ortaya çıkan açıklıkların bir iki sene sonra uygulanamaz olmasının, yeni güvenlik mekanizmalarının geliştirilmesinin bunda etkisi büyüktür. Özellikle bilgi güvenliği birimlerinde yöneticilik yapan kişiler bu konuda ileri görüşlü olmak ve personeline yatırım yapmak mecburiyetindedirler. Bu amaçla yıllık belirli eğitim hedefleri ortaya konulabilir veya test projelerinin yoğunluğu belirli oranda azaltılarak personelin literatür taraması yapabilmesine imkan tanınabilir. Kazanılan yeni test tekniklerinin birim içi eğitimlerle kurumsallaştırılması da başvurulacak etkin yöntemlerdir.[161]

Kurulan iletişim ağları ile bilgiye ulaşım, hızlanmakta ve kolaylaşmaktadır. Bilgi toplumunun iletişim altyapısı, belli merkezlere bağlı ağ sistemlerinden oluşacaktır. Diğer taraftan insanlık "*ilkel toplum*", "*tarım toplumu*" ve "*sanayi toplumu*" aşamalarından geçerek bugün "*bilgi toplumu*" aşamasına gelmiştir. İletişim ağı sistemlerinin hem bilgi bankalarına ve araştırma merkezlerine hem de kişisel bilgisayarlara bağlı olması, bilgi üretiminin; bilgi-işlem teknolojisi sistemi içinde gerçekleşmesini sağlayacaktır. Fabrikaların yerini, bilişim teknolojisine dayalı, iletişim ağ sistemleri oluşturacaktır. Bilişim bilgisi, hem bilgi toplumundaki üretim faaliyetlerinin temel girdisi hem de tüketimin en önemli girdisi olacaktır. Kısaca bilgi her türlü işin asıl kaynağı olacaktır. [162]

---

159 ROBBINS Anthony, **Sınırsız Güç**, Çeviren Mehmet DEĞİRMENCİ, İstanbul, İnkilap Kitabevi, 1992, s.6.

160 SALTÜRK Metin, “Bilgi Toplumu”, **Harp Akademileri Bülteni**, Kasım 2003, s.68.

161 TÜRKÖZ Tahsin, “Bilişim Güvenliği Testlerinde Başarının Sırları”, TÜBİTAK, UEKAE, http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/bilisim-guvenligi-testlerinde-basarinin-sirlari.html, (e.t. 06.02.2012).

162 DRUCKER Peter F., **Kapitalist Ötesi Toplum**, Çeviren: Belkıs Dişbudak ÇORAKÇI, İstanbul, İnkilap Kitapevi, 1994, s.280.

Bilgi toplumu henüz tam anlamıyla şekillenmemiş olmasına rağmen, onun en önemli özelliklerinden biri bilgisayarların yoğun olarak kullanılacak olmasıdır. Yeni toplumun şekli bilgisayar ve iletişim teknolojisi tarafından çizilecektir. Sanayi toplumunda fabrikalar, her türden malın üretildiği birer merkez olmanın da ötesinde toplumsal birer sembol olmuşlardır. Şimdi bu sembol yerini her türlü bilgiyi üreten, işleyen, saklayan ve dağıtan bilgisayar merkezlerine bırakmaktadır. Artık ilerlemenin, modernleşmenin sembolü fabrikalar değil bilgisayar merkezleri olacaktır. Bilgi toplumunda bilgisayarlar insanların bilgi üretme gücünü olağanüstü arttırarak, bilginin kitle halinde üretilmesini, işlenmesini, saklanmasını, dağıtılmasını ve tüketilmesini sağlamaktadır.[163]

Yaşadığımız bilgi çağında artık savaşlar bilgi ve bilgi sistemlerine bağımlı hale gelmiştir ve gelecekte daha da bağımlı hale gelecektir. Gelecekte savaşları kazanmak devletin sahip olduğu tesislerin bomba ile imhası şeklinde değil, sahip olduğu bilgi sistemlerini bilgi harbi araç ve vasıtaları ile etkisiz hale getirme şeklinde olacaktır. Siber savaşlar belki savaşın kazanılması noktasında esas unsur olmayacaktır ama buna sebep olacak en önemli unsur olacaktır.

Bilgi çağının savaşın sevk ve idaresi yanında tüm kuvvetlerin organizasyonu ve kullanım konseptini de değiştirmesi beklenmektedir. Endüstri çağının uygulaması olan ve harekât alanlarına yönelik olarak yürütülen savaş kavramı yerine düşmanın savaşma azmini ve harekât alanı derinliğindeki bilgi alt yapısını yok etmeyi hedefleyen yeni bir savaş türü etkili olmaya başlayacaktır. Bu savaş çeşitli türdeki bilgi harekâtı ile yürütülecektir.[164]

Bilgi çağının günümüzdeki savaş kavramına getirdiği bir yenilik; tehdidin niteliğinden çok yönü ile ilgilidir. Çağımızda bilginin kazandığı önem paralelinde bilgiyi toplayan, işleyen ve dağıtan alt yapı da tehdidin hedefi haline gelmiştir. ABD'de 15 yaşındaki bir çocuk Pentagon'un bilgisayar sistemine nüfuz ederek, çok gizli bilgilere ulaşabilmiştir. Sadece macera düşüncesiyle bir çocuk tarafından gerçekleştirilebilen böyle bir eylemin, organize bir topluluk tarafından gerçekleştirilmesi durumunda çok daha etkili olabileceği açıktır. [165]

20. yüzyılın son çeyreğinde icra edilen harekâtlar geleceğin savaş ortamına yönelik ipuçlarını vermektedir. Bilginin ve bilgi sistemlerinin son derece yoğun ve etkili olarak

---

163 SALTÜRK, op.cit., s.71.

164 **Deniz Kuvvetleri Dergisi**, EKİM, 2001, s.50.

165 Türk Silahlı Kuvvetleri (TSK), **Türk Silahlı Kuvvetleri Bilgi Harbine Nasıl Hazırlanmalıdır?**, Harp Akademileri Basım Evi, Yenilevent , İstanbul, Nisan, 1999, s. 3-4.

kullanıldığı bu harekâtlarda klasik savaş anlayışı, taktikleri, kuvvetleri kullanma şekilleri, hedefleri, etki alanları, dünya kamuoyuna yansımaları, gibi birçok yönüyle terk edilmiş ve yeni bir savaş anlayışı ortaya çıkmıştır.

Ordu her zaman savaşmaya ve kazanmaya hazır olmaya odaklanmıştır. Savaş ve savaş dışı da dâhil olmak üzere tüm askerî hareket çeşit ve safhalarında, olası her türlü göreve cevap vermek amaçtır. Bu nedenle hedef, muhasım karşısında geliştirilecek yeni konseptlerin icrasını mümkün kılan görevleri yerine getirebilecek, esnek, kıvrak bir kuvvet yapısıyla hazır olmaktır.[166]

Sonuç olarak, bilginin gittikçe daha değerli hale geldiği günümüzde, alt yapısında bilgi sistemleri bulunan her sahayı hedef alan topyekûn bir savaş türü, Bilgi Harbi ve askeri sahaya yansıması olan Bilgi Harekâtı ortaya çıkmıştır. Savaş sahasındaki bu değişim süreci bireylerin, devletlerin ve uluslararası yapının da güvenlik algılamalarını değiştirmesi gerekliliğini ortaya çıkarmıştır. Geleneksel olmayan bu yeni tehditlerle mücadele araçları, yöntemleri, savaş sahası ve en önemlisi de savaş prensipleri farklılaşacaktır. Örneğin, günümüzde bir devlet olası bir bilgisayar korsanı saldırısı ile geleneksel savaş doktrini veya savaş silahları ile mücadele edemez. Bu bağlamda askeri önlemlerin içerisine siber güvenlik önlemleri de dâhil edilmeli, dolayısıyla bilgisayar mühendisleri ya da uzmanları ilgili ülkenin ulusal savunma yapılanmasında daha etkin roller oynamalıdır.

2.1. ASİMETRİK BİLGİ HARBİ

Enformasyon yapılarına yönelik tehditler geniş ve asimetriktir; bu sebeple siber güvenliğe duyulan ihtiyaç hiçbir zaman bu kadar büyük olmamıştır. Uygun fiziksel ve personel güvenliği ve karşı istihbarat tedbirleri gerektiren dış kaynaklı tehditlerin artan seviyesine rağmen, kurumların içindeki kişiler hâlâ en büyük tehdidi oluşturmaktadır. Siber güvenlik sihirli kara kutu çözümlerinden değil; insanları, eğitimi, teknolojiyi ve kuralları kapsayan bir bütünleşmiş unsurlardan oluşmaktadır. Günümüz güvenlik ortamının düzensiz yapısı, tehditleri öngörmenin ve engellemenin çok daha zor olacağı anlamına gelmektedir. Bu asimetrik tehditler, ülkeleri ve ittifakları tahrip etme potansiyeline hâlâ sahiptir.[167]

Teorik bölümde de bahsedildiği üzere "*Ulusal güvenlik kavramı, tüm güvenlik alanı için anahtar kavramdır, ancak güvenlik birimi olarak ulus çok az incelenmiştir. Siyasi,*

166 ÇOLAK, loc.cit.
167 Ibid.

kurumsal devlet ve dolayısıyla siyasi ve askeri sektörler odak noktası olmuştur. Eğer ulusa odaklanılacak olursa, başka bir sektör daha resme dâhil olmaktadır, o da toplumsal boyuttur. Toplumsal güvenlik, siyasi güvenlikle yakından bağlantılıdır, ancak ondan farklıdır. Siyasi güvenlikle kastedilen; devletlerin örgütsel istikrarı, hükümet sistemleri ve hükümetlere ve devletlere meşruiyet kazandıran ideolojilerdir. Toplumsal güvenlik ise bir kimliğin algılanan bir tehdide karşı savunulmasıdır ya da daha açık söylemek gerekirse, bir topluluğun kimliğine yönelik algılanan bir tehdide karşı savunulması olarak tanımlanmaktadır." [168]

Bilhassa asimetrik tehditlerin önem arz ettiği günümüzde strateji, taktik, konsept ve doktrinde yaratıcılık, teşkilat, birey, eğitim sistemi, kurumsal kültür geliştirebilme yeteneği stratejik değerler olarak karşımıza çıkmaktadır.[169] 11 Eylül 2001 de ABD yaşanan asimetrik saldırı, güvenlik sistemleri ile buna ait karar mekanizmalarının kendilerini nasıl korumaları, hangi tepki altyapısıyla tehdidi nasıl bertaraf etmeleri gerektiği konusunda önemli bir uyarı oluşturmuş bu konuda güçlü sanılan devletlerin bile tam anlamıyla yeterli ve hazır olmadıkları anlaşılmıştır.[170]

Düşük yoğunluklu çatışma ve savaş öncesi, devletlerarası ilişkilerde, konvansiyonel ve balistik silahlara başvurmadan, görünmeyen saldırı ve savunma sistemi olarak internetin kullanıldığını tespit ediyoruz. Orduların operasyonel üstünlüğünün, elektronik haberleşme, görüntü alma, uzaktan algılama gibi taktiklere dayandığı günümüzde, internet temelli saldırılar için yeni savunma taktikleri geliştirilmesi gerekir. Savaş sırasında fiziki cephe açma maliyeti ve insan kaybı göz önüne alınacak olursa, savunma anlayışı olarak, elektronik saldırı ile sanal bir cephe açmak, birçok açıdan üstün bir stratejidir. [171]

Düşmanın yumuşak karnı olarak, operasyonel üstünlüğün olduğu elektronik haberleşme, uydu komuta merkezi, füze kontrol ve insansız hava araçlarının seçilmesi ve internet yoluyla elektronik savaşta ele geçirilmesi, fiziki savaş ve savunma için çok üstün bir sonuç sağlayacaktır. Neredeyse tüm cihazların internete bağlanacağı günümüzde, bilginin toplanması, stratejik olarak tasnifi, veri madenciliğiyle karar verecekler için bir destek girdisi

---

168 WAEWER Ole, "Toplumsal Güvenliğin Değişen Gündemi", **Uluslararası İlişkiler,** çev. Birgül Demirtaş COŞKUN, Cilt 5, Sayı 18, 2008, http://www.uidergisi.com/wp-content/uploads/2011/06/Toplumsal-Guvenligin-Degisen-Gundemi.pdf, (e.t. 23.12.2011), s. 153.

169 ÇOLAK, loc.cit.

170 Ibid.

171 CEYLAN Cenk, "Savaş Cephesi Olarak, Sanal Ortamda Savunma ve Saldırı", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/savas-cephesi-olarak-sanal-ortamda-savunma-ve-saldiri.html?Itemid=6, (e.t. 15.02.2012).

olarak kullanılması için, özel amaçlı olarak oluşturulmuş ücretsiz internet siteleri, arkadaşlık ve e-posta grupları, istihbaratta öne geçmek isteyen devletler tarafından örtülü olarak finanse edilecektir. Savaş öncesi keşif yapmak için, internet bir araç olarak kullanıldığında, ülkelerin işgal edilmesi için gerekli lojistik büyük ölçüde sağlanmış olacaktır.[172]

Uluslararası ilişkilerde, ülkeler arası anlaşmazlıkların çözülmesi için orduların ve silahların caydırıcı bir güç olarak kullanılması taktiğine, sanal orduların ve saldırılarında dahil edilmesinin vakti gelmiştir. Sanal orduların saldırısına, fiziksel karşılık vermek, yel değirmenleriyle savaşmaya benzediği için, sanal saldırıya, sanal cevap vermek gerekmektedir. Ülkelerin, kamu, özel sektör ve askeri haberleşmelerinin, internetten geçtiği ve bu trafiğin süzülerek bilgilerin tekrar elde edilebildiği unutulmamalıdır. Harp Akademileri'nde, sanal savaş ve savunma anlayışı konusunda bölümler açılmalı ve askeri bir taktik olarak benimsenmelidir.[173]

Savunma sanayi olarak, klasik balistik ve konvansiyonel cihazlara yapılan yatırım gibi, elektronik savunma ve saldırı için sanal savaş cihazlarına yatırım yapılmalıdır. Güçlü şifre kırıcılar, frekans karıştırıcılar, hızlı çalışan işlemciler, yüksek hassaslıkta görüntü algılayan sistemler ve yüksek güvenlikli haberleşme uyduları tasarlamak ve üretmek ülkelerin sanal savaş kabiliyetlerini ve operasyonel üstünlüklerini belirlemektedir. Süper bilgisayarla yapılmış bir sanal savunma ve saldırı harekâtı, gerçek zamanlı savaşta açılacak cephe sayısını azaltmaktadır.

2.2. SİBER SAVAŞ VE SİBER SAVAŞÇI

Günümüzde devletlerin, şirketlerin, kuruluşların ve hatta bireylerin sahip olduğu en büyük sermaye "*bilgi*" olmuştur. Bu gerçek ışığında yaşadığımız çağa da "*Bilgi Çağı*" adı verilmiştir. Ulaşılan üstün teknolojinin sağladığı haberleşme, ulaştırma ve bilişim alanındaki inanılmaz kolaylıklarla birbirine yaklaşan devletler, kuruluşlar ve kişilerle globalleşen dünyamızda bilginin önemi daha da artmıştır. Günümüzde ve gelecekte daha fazla bilgiye sahip olanlar daha fazla güce sahip olacaklar ve istedikleri zaman ve yerde sahip oldukları bu bilgiyi kullanarak arzu ettikleri etkiyi yapabileceklerdir. Olaylara yön vererek geleceği kontrol altına alabileceklerdir. "*Bilgi güçtür*." Bu cümle bilgi çağının en önemli sözü olacaktır.[174]

172 Ibid.
173 Ibid.
174 TSK, op.cit., s.5.

ABD Hava Kuvvetleri siber savaş operasyonlarını yürütmek üzere 24. Tugayı kurmuştur. Ancak bu birliğin hiç uçağı yoktur. Sadece sürdürebilir siber operasyonlarını idame etme misyonuna sahip. Bu birliğin toplamda 6.000 ile 8.000 kişilik bir kadrodan oluşan siber savaşçı mevcudu bulunduğu tahmin edilmektedir. Hava Kuvvetlerinin siber savaşa verdiği önemi Komutanları General Norman Schwartz'ın[175] sözleri vurgulamaktadır:

"*Siber savaş ABD'nin askeri üstünlüğünü sağlamak için hayati önem taşımaktadır. ABD Hava Kuvvetleri siber uzay olanaklarının tümünden yararlanmaya kararlıdır. Siber uzay alınmamış bir alandır ve bugün bu alanı ele geçirmek için kavga başlamıştır*."

Amerikan Deniz Kuvvetleri de siber uzay kapasitesi olan üç tane filo kurmuştur. Basra Körfezindeki beşinci, Akdeniz'deki altıncı ve Çin Denizindeki yedinci filolar "*siber muharebe*" yetenekleri ile teçhiz edilmiştir. Ayrıca İkinci Dünya Savaşından sonra lağvedilen 10.Filo da hiç gemisi olmamasına rağmen siber savaş için yeniden aktive edilmiştir. Bu filonun adı NETWARCOM (Donanma Ağ Savaş Komutanlığı) olarak değiştirilmiş ve 10.Filo altında operasyonlarına devam etmiştir. ABD Kara Kuvvetleri ise başta iki kuvvet kadar istekli olmasa da, kendi mütevazı siber komutanlığını NETWAR adı altında kurmuştur.[176]

Peki, kimler siber saldırıyı gerçekleştirir? Şekil-2 den anlayabileceğimiz gibi siber saldırganlar; sanal ortamdaki protestocular, organize suç örgütleri, bireysel bilgisayar korsanları, terörist organizasyonlar, içeriden gelen tehditler ve son olarak devlet destekli çalışanlar olabilmektedir. Bunların içerisinde en masumları bireysel bilgisayar korsanlarıdır. Diğerleri şekilde görüldüğü gibi bilgisayar korsanlarının farklı şemsiyeler altına girmiş halleridir. Yapılan tüm saldırılar bilgi sistemlerinin gizlilik, bütünlük ve erişebilirliğini bozmak için gerçekleştirilmektedir. Sosyal mühendislik, hizmet dışı bırakma, bilgi çalma, örün sayfalarını değiştirme gibi saldırılar hep bu üç temel unsuru hedefler.[177]

175 CLARK, KNAKE, op.cit., s.30.
176 Ibid., s.31.
177 Kara Kuvvetleri Komutanlığı Siber Savunma Şube Müdürlüğü tarafından konu ile ilgili yapılan konferanslardan derlenmiştir.



Şekil 2: Siber Saldırganlar

Dünyanın herhangi bir yerinde binlerce hedefin vurulabilme olasılığı son derece yüksek gerilimli krizlerin meydana gelmesine neden olabilmektedir. Nükleer savaşı engelleyen güç olan caydırıcılık siber savaşta yoktur. Devlet sırları arasında gömülü siber savaş olgusunun yanında Soğuk Savaş dönemi son derece açık ve şeffaf kalmaktadır.[178] Şu an için devletler siber savaş taktiklerini ve imkânlarını gizli tutarak karşı tarafa kendi durumunu belli etmemeye çalışmaktadır. Bunun yanında devlet dışı aktörlerin kendi inisiyatifi ile veya belli yönlendirmeler ile bu tespitin de yapıldığı sanal dünya da karşılaşılan olaylar ile anlaşılmaktadır. Bilinmezlikler hasım tarafı korkutmaya yetmese de siber dünyanın geniş sınırları içerisinde devletleri olduğundan daha güçlü göstermeye yetmektedir.

Dünyanın geri kalanına bu yeni silahı sergileyen ve siber uzaydaki korkunç yeni saldırı tekniğinin mucidi olan ülke, aynı zamanda gaflete düşüp o silaha karşı kendini nasıl koruyacağını planlamadıysa, siber savaşı kaybetmeye mahkûmdur.[179] Siber uzayın imkânlarını silah olarak kullanma tercihi devletlerin dışında bireylerin de imkânları dâhilindedir. İnsanlar kendi becerileri ile siber uzay da kişilere ve hatta devletlere karşı da rakip olabilirler. Bu rekabet siber uzayın kendi özelliklerinden dolayı bir artı birin iki olmadığı bir sanalsal uzayın içerisinde geçmekte ve sayısal üstünlük kabul bile edilmemektedir.

178 Ibid., s.X.
179 Ibid.

Muharebe alanının derinleştirilmesi; düşman kuvvetlerine karşı kesin üstünlük sağlanması için bir zorunluluk olacaktır. Bu da, insanlı ve insansız hedef sistemleri ile büyük doğrulukla görerek ve görmeyerek nokta ateşi yapabilen silah sistemlerinde sağlanacak büyük gelişmeler yoluyla olacaktır. Bilgi harbinin muharebe sahasında sağladığı avantajları maddeler halinde sıralamak gerekirse;[180]

- "*Muharebe alanının genişletilmesi;*
- *Düşman kuvvetlerinin dost kuvvetlerle temasa geçemeden etkisiz hale gelmesinin sağlanması;*
- *Dost birliklerin aşırı dağılmalarından doğan hassasiyetin azaltılması;*
- *Uzak mesafeli ateşler sayesinde manevranın gerçekleştirilebilmesi;*
- *Komutan, düşman kuvvetlerinin sahip olduğunun çok ötesinde yüksek bir tempoda harekât icra etme esnekliğini verebilmesi gibi farklı alanlarda düşmana karşı büyük avantaj sağlayacaktır.*"

Muharebe sahasında sağlanacak üstünlük; yüksek bir harekât temposu ile gece ve gündüz, her hava koşulunda, karadan ve havadan yapılacak sürekli harekât sayesinde başarılacaktır. Yaya ve indirilmiş birliklerin manevra yetenekleri, askerlerin taşıyacağı yükün azaltılması ve hafifletilmesi, fiziksel yeteneklerinin arttırılması, silah ve teçhizatlarının yeteneklerinin arttırılması yoluyla giderilecektir.

Bu alandaki gelişmeler geleneksel ateş ve manevra ilişkisinin gözden geçirilmesini gerektirecektir. Derin harekât ve eş zamanlı taarruz konseptlerinin birleştirilmesi; muharebe sahasının zaman, mekân ve maksat açısından uzatılmasını, harekât için geçecek sürenin kısaltılmasını düşmanın kuvvet çoğunluğu bölgesine çok boyutlu taarruzların kolaylaştırılmasını ve düşmanın mağlubiyetinin hızlandırılmasını temin eden dinamik vasıtalar yaratacaktır.

Bilgi harekâtının asıl maksadı dost bilgi sistemlerini korurken düşmanın bilgi sistemlerine taarruz etmektir. Derin ve eş zamanlı taarruzun en önemli elemanı bilgi savaşını kazanmak için alınan tedbirler olacaktır. Bu tedbirler siber uzayda konuşlu bilgi aktarımını

---

180 ÇOLAK, loc.cit.

engelleyen sistemler ve bilgisayar virüsleri olacaktır. Bir diğer taarruz metodu ise düşmanın muharebe bilgisayar sistemlerine sızarak bilgileri değiştirmek olacaktır.[181]

2.3. KÖRFEZ SAVAŞI ÖRNEĞİ

ABD, 1991'deki Körfez Savaşı'nda muharebenin tamamen yeni bir şeklini gözler önüne koymuştur. Siber uzayın imkânlarını kullanıp, Irak'ın askeri gücünü dağıtmış, dünyayı şaşırtmış ve ABD silahlı kuvvetlerinin silahlı bir çatışma standartlarındaki, performansını değiştirmiştir.

Siber uzayın imkânlarından çok iyi faydalanarak, devletler muharebeye daha önce bilinmeyen esneklik, eş zamanlılık, hız ve doğruluk derecesi kazandırmıştır. Çöl Fırtınası Harekâtı aynı zamanda siber savaşın ilk örneklerini bulabileceğimiz bir harekâttır. Bu savaşta siber savaşın taktikleri ve imkânları çok iyi kullanılarak çok daha küçük ve daha az maliyetli bir askeri gücün, bilinmezlik ve düzensizliklerle dolu savaş ortamında, neler yapabileceğinin örnekleri gösterilmiştir.

Çöl Fırtınası Harekâtı boyunca hedef ve muhabere bilgilerini dağıtmakta kullanılan en kritik bilgi sistemlerinin çoğu Irak'ın Kuveyt'i işgal ettiği gün ortada yoktu. Muhabere ve bilgisayar cihazlarının kapasite, bağlanabilirlik, kullanım sınırlamaları gibi sebeplerle kullanımlarının gecikebileceğini keşfeden teknisyenler, gerektiği anda, gerekeni yaratıp usullere aykırı ve kullanılması tavsiye edilmeyen şekillerle de olsa askeri ve sivil bilgi cihazlarını bir araya getirip harekât için gerekli ağları kurmuşlardır.

Bu bağlamda Körfez Savaşı C4I sistemleri teknolojisine sahip olma farkının büyüklüğünü ortaya koyan ilk çatışma olmuştur. Körfez savaşında kullanılan gelişmiş ve isabet ihtimali yüksek silahlar; cruise füzeleri ve akıllı bombalar düşmanın C4I sisteminin büyük ölçüde imha edilmesine ve komutanlıklar ile birliklerin irtibatının kesilmesine imkân vermiştir. Körfez savaşının geçmişteki savaşlardan farkı, sadece harekâtın daha etkin yönetilmesinde değildir. Muhabere ve bilgisayar yeteneği, bazı şeylerin yeni ve değişik bir şekilde yapılmasına olanak vermiştir. Örneğin, muharebe sahasından 10.000 km uzaktaki kaynakların, komutanlar tarafından kullanılabilmesi mümkün olmuştur. Teknoloji harekât ihtiyaçlarının karşılanması için çok çabuk uyarlanabilmiş ve sistem etkinlikleri artırılabilmiştir. Körfez savaşında zaferin kazanılmasında en önemli etkenlerden biri, koalisyon kuvvet ve birlik

---

[181] Ibid.

komutanlarının muharebe sahası resmini sürekli izleyebilmeleri, buna karşılık Irak'ın aynı resmi görmesinin engellenmesi olmuştur.[182]

İkinci Körfez Savaşı başlamadan hemen önce, binlerce Irak subayına Irak Savunma Bakanlığı e-posta sistemi üzerinden elektronik posta mesajları iletilmişti. Pentagon'un hazırladığı bu mesajlar Irak birliklerinin hiç savaşa girmeden teslim olmalarını teşvik etmek için gönderilmiştir. Tam metnin ne olduğu kamuoyuna açıklanmamıştır .[183]

ABD Başkanı, İkinci Irak Harekâtı'nda Irak ve başka ülkelerdeki banka ağlarına siber saldırılar yaparak Saddam'ın finans düzenini ele geçirmek istememiştir. Bunu yapma olanakları vardı; ancak Bush bunun başka devletler tarafından uluslar arası yasaların çiğnenmesi olarak algılanabileceğini düşünmüştür. Danışmanlar ayrıca yanlışlıkla ABD'nin yürüttüğü siber bank soygunlarının başka hesapları da etkileyip finans kuruluşlarının çökmesine neden olmasından korkmuşlardır.[184]

2.4. ESTONYA ÖRNEĞİ

2007 Nisan-Mayıs'ında, Estonya Başkanı, Parlamentosu, bir seri hükümet ajansı, haber medyası ve en büyük iki bankasının web siteleri büyük bir saldırıya uğradı. Web sitelerine, Başbakan tarafından yazıldığı söylenen sahte bir özür mektubu[185] ve Hitler bıyığı olan bir fotoğrafı konuldu.[186] The New York Times, bunu "*Siber Uzaydaki İlk Gerçek Savaş*"; Estonya Savunma Bakanı "*bir milli güvenlik durumu*" ve Estonya'nın Siber Savunma Koordinasyon Komitesi Başkanı "*bir tür terörizm*" olarak tanımladı.[187] Bu olayın başlangıcı, Estonya otoritelerinin II. Dünya Savaşı sırasında verilen Sovyet kurbanları anısına düzenlenmiş bir anıtın, Tallinn'in merkezinden, daha uzak bir alanda bulunan askeri bir mezarlığa taşınmasına karar vermelerine dayandı. Bu davranış, etnik Rus azınlığının önemli bir kısmı tarafından, kültür ve politik statülerine bir tehdit unsuru olarak görüldü. Büyük çaplı gösteriler 1300 kişinin tutuklanmasına, 100 kişinin yaralanmasına ve 1 kişinin ölümüne sebep oldu.

---

182 TSK, op.cit., s.35.

183 CLARK, KNAKE, op.cit., s.11.

184 Ibid., s. 12.

185 LANDLER Mark, John MARKOFF, "Data Assault Hits Estonia Were It Hurts", 2007, **International Herald Tribune**, May 30.

186 FINN Peter, "Cyber Assaults on Estonia Typify a New Battle Tactic", 2007, **The Washington Post**, May 19.

187 BLOMFIELD Adrian, "Estonia Calls For a NATO Strategy on 'Cyber-Terrorists' After Coming Under Attack", 2007, **The Daily Telegraph**, May 18.

27 Nisan 2007 tarihinde Estonya, başkenti Tallinn'de bulunan Rusya'ya ait meçhul asker anıtını kaldırmasından sonra Estonya'da devlete ait web mail sunucuları ve bankacılık sistemlerine ataklar gerçekleştirilmiştir. Başlangıç atakları sonucunda bazı internet siteleri kötü niyetli kullanıcılar tarafından ele geçirilmiş bazıları devre dışı bırakılmış, bazılarının içeriği değiştirilmiştir. 30 Nisan–18 Mayıs tarihleri arasında ulusal bilgi sistemleri, internet hizmet sağlayıcıları ve bankalara yönelik daha geniş katılımlı ve koordineli dağıtık servis dışı bırakma (DDOS) atakları gerçeklenmiştir. Bu ataklar sonucunda Estonya'nın ulusal bilgi sistemleri ve ev kullanıcılarına hizmet veren diğer internet sistemleri büyük zarar görmüştür. İnternet bant genişliği büyük oranda saldırılar tarafından doldurulmuş ve ülkedeki internet sistemi çökme noktasına getirilmiştir. Estonya ataklara karşı NATO'dan yardım istemiştir. Bu ataklarda botnet (köle bilgisayarlar) kullanıldığı için Avrupa, ABD ve diğer ülkelerden de çok sayıda bilgisayarın kullanıldığı görülmüştür. Bu ataklar sonucu NATO Estonya'nın başkenti Tallinn'de NATO Siber Savunma Mükemmeliyet Merkezini kurma çalışmaların başlamıştır. Bu konudaki çalışmalar hala devam etmektedir. [188]

Gösteriler sokaklardan internete yayıldıkça, Estonya otoriteleri, ağdaki bu saldırıları, Estonya'nın politik kuvvetine aynı zamanda kültürel ve milli kimliğine karşı tehdit olarak düşünce beyan etmeye başlamıştır. Estonya bilgi teknolojileri danışmanı olan Linnar Viik şöyle söylemiştir: [189] "*Bu yalnızca bir sanal dünya değil. Bu bağımsızlığımızın bir parçası ve bu saldırılar, bir ülkeyi mağaraya, taş devrine döndürmek için girişilen bir çabadır*." Hem hükümet hem de ticari aktörler, Estonya'yı dijital modernizmin ön sıralarında olarak görmekte, bu da Estonya ve Sovyet geçmişi arasındaki fark için önemli bir element olarak gösterilmiştir.[190]

Ağın çökertilmesi Estonyalıların kamu otoriteleri ile bağlantı kuramamasına (hükümetin web siteleri çökmüş durumda) sebep olmuştur. Önemli bireysel alış-verişler yapılamamıştır (en büyük iki banka vurulmuş durumda), neler olduğu hakkında bilgi alınamamıştır (medya ve web siteleri hedef alınmış durumda), veya güvenilir otoriteler tarafından internete servis edilenlere güvenememesine (Başbakan'ın web sitesinin ünü zedelenmiş durumda) neden olmuştur. Bankacılık, kamu otoriteleri ile iletişim ve online haber okuma gibi günlük merkezi uygulamalarla bağlantı kurulduğunda, "*bireysel güvenlik*" direk

188 GÖKALP Ziya, "PKI (Açık Anahtar Altyapısı) Nedir?", Vasco Data Security, http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/pki-acik-anahtar-altyapisi-nedir.html, (e.t.15.01.2012).

189 FINN, op.cit.

190 MICHAELS Jim, "NATO to Study Defense Against Cyberattacks; Computer Assault Staggered Estonia", 2007, **USA Today**, June 15.

olarak anlaşıldığı gibi sağlanmış ve Estonya dışındaki izleyiciler, siber savaşın kendi dijital rutinlerine nasıl etki edeceği konusunu hatırlamışlardır.[191]

Estonya güvenlik aktörlerinin, saldırıları "*siber uzaydaki ilk savaş*" olarak kabul ettirme ve hızlı bir şekilde dünya basını tarafından ele alınmasını sağlama becerisi en azından başarılı bir "*cybersecuritization*" durumu olarak görülebilir. Washington Times ve The New York Times durumu, "*siber savaşın gerçek bir örneği*" ve "*siber uzaydaki ilk savaş*" olarak tanımlayan birçok yazı yayınlamış ve NATO'yu "*kolektif siber güvenlik*" konusunda rol almaya itmiştir. The New York Times, bilgisayara bağımlı dünyaya daha fazla dikkat edilmesi gerektiğini savunmuş [192], bilgi savaşının birçok saldırgan formunun olabileceğini ve bunun nasıl durdurulacağını ve arkasında kimin olduğunun anlaşılmasının tam güvenlik için gerekli olduğunu söylemiştir. Bir savaş çağrısı yapmasına rağmen, Estonya otoriteleri, bir numaralı uluslararası izleyicilere, NATO'yu, saldırıların Estonya'nın politik kuvvetine yapılan bir saldırı olduğu konusunda ve dolayısıyla NATO Madde 5'in yürürlüğe sokulması konusunda ikna etmede zorluklar çekmiştir. Estonya Savunma Bakanı Jaak Aaviksoo'nun şikâyet ettiği gibi şu anda NATO siber ortakları, açık bir askeri hareket olarak tanımlamamaktadır. Ancak bu hiçbir birleşik desteğin olmadığı anlamına da gelmez. NATO, AB ve Pentagon, siber güvenlik takımları göndermiştir. NATO kuvvet dönüştürme ajandasına bilgi sistemleri eklemiş ve sonraki yıl bir siber savunma konsepti politikası oluşturmuş, bir "*Siber Savunma Yönetim Otoritesi*" yaratmış ve Estonya'nın başkenti Tallinn'de "*Kooperatif Siber Savunma Merkezi*" kurulmasını desteklemiştir. Bu olaylar, NATO'nun kendi sözleriyle, kendi şifreli yapılarının korunmasını içeren siber koruma anlayışının, üyelerinden iletişim yapıları açık olanların korunmasına bir geçiş oluşturmaktadır.[193]

Estonya "*güvenlikleştirmenin*" başarısı, "*ağ*", "*halk*" ve "*devlet gücü*" referans objelerinin bir araya gelmesi, siber sektörün, bazı olanaklar yanında zorlukları da olan özel bir alan olduğunu iyi bir şekilde örneklemektedir. Estonya otoritelerinin mücadele yönteminin tamamıyla kabul görmesine engel olan şey, saldırının kaynağını, resmi bir Rus kaynağına kadar takip edememeleridir. Saldırılar iki raund halinde düzenlenmiştir. Birinci raunda,

---

191 HANSEN Lene, Helen NISSENBAUM, "Digital Disaster, Cyber Security, and the Copenhagen School", **International Studies Quarterly**, 2009, vol 53, http://www.nyu.edu/projects/nissenbaum/papers/Digital%20Disaster,%20Cyber%20Security%20and%20the%20Copenhagen%20School.pdf, (e.t. 31.12.2011), p.1169.

192 The New York Times, "A Cyberblockade in Estonia", 2007, June 2.

193 NATO, 2008, **Defending Against Cyber Attacks**, http://www.nato.int/issues/cyber_defence/practice.html, (e.t. 10.01.2012).

Estonya resmi kaynakları, Putin yönetiminden IP (Internet Protokolü) adresine varan izler olduğunu iddia etmiştir. Estonya Dışişleri Bakanı Urman Paet; Rusya'nın bu tarz saldırıları ilk defa başka bir ülke üzerinde kullandığını ifade etmiştir.[194] Rusya resmi kaynakları, kanıt yetersizliğine ve IP adreslerinin iki ülke arasındaki ilişkileri germek için kullanacak profesyonel hackerlara açık olduğu konusuna dikkat çekmişlerdir. Yıkıcı etkileri kanıtlayan bilgisayar uzmanlarının açıklamaları ve gerçekler teknifikasyonun önemini göstermektedir: Saldırıların, ABD, Çin, Vietnam, Mısır ve Peru'yu da içeren yaklaşık 50 ülkeden geldiği ve Dünya bilgisayarlarının çeyreğine bulaştığı söylenmiştir. [195]

Botnetlerin kullanımı, günlük yaşamda ve saldırıların bağlantılı ve kötüye giden yapısında görülmüş, ancak yine de sonuç olarak, Rusya'ya varan hiçbir kabul görmüş açık dijital iz bulunamamıştır. NATO ve AB kendilerini; Estonya meselesinin bu kısmından uzak tutmaya dikkat etmişlerdir. Estonya güvenliğinin mücadele ettiği ikinci konu, saldırganların, elektrik, finans, enerji veya trafiği yöneten kritik dijital alt yapılara müdahale edememeleri ya da bu konudaki isteksizlikleridir. Bir bankayı, online hizmetlerini bir saat kapatmaya zorlamayı savaş olarak nitelemek zordur. Gerçek anlamda yıkıcı bir "*hypersecuritization*" senaryosunun sürdürülmesi zordur ve şüpheciler bu sebeple Estonya olayının da, "*siber uzaydaki ilk savaş*" tanımlamasını alan geçmiş diğer olaylar gibi, örneğin Kosova üzerindeki savaş ve Zapatista ayaklanması, hafızalardan silinmeye mahkûm olacağını savunmaktadır.[196]

Buna rağmen, siber sektörün politik özelliğine karşı çıkmayan şüpheciler, Estonya otoritelerinin sağladığı başarıyı kabul etmektedirler. İlk olarak, geçmiş 15 yılda "*hypersecuritizations"* ın sağladığı kurumsallaşmış statü, tam kapsamlı bir senaryo olmasına rağmen Estonya saldırılarına yeterli direnişin gösterilmiş olduğu görülmüş, aynı anda bu tarz yıkıcı senaryoların oluşabileceği iddiası güçlendirilmiştir. Tehdidin yerinin tespit edilememesine rağmen, saldırıları Kremlin'in planladığına dair Estonya düşünceleri, Amerika'nın, siber saldırı becerileri kazanan Çin konusundaki endişelerini açığa çıkarmıştır.

İkinci olarak, siber saldırganlar ve Rusya arasındaki bağlantının kanıtlamamış olmasına rağmen, "*siber saldırı güvenliği*", Estonya resmi kaynakları tarafından, "*terörizm*" olarak tanımlanmıştır. Sonuç olarak, "*siber tehditler*" ve "*terörizm*" terimleri arasında bağlantı kurulmaya başlanmıştır. "*Siber tehditler*" ve "*teröristlerin*" tehlikeli doğası

194 ANDERSON Robert, Daniel DOMBEY, Stephen FIDLER, Isabel GORST, Maija PALMER, "US Warns Cyber-Attacks Will Increase", 2007, **Financial Times**, May 18.
195 FINN, loc.cit.
196 Ibid.

konusundaki iddiaları desteklemiş ve saldırıların "*terörist*" karakteri, onları daha dikkate değer hale getirmiştir.[197]

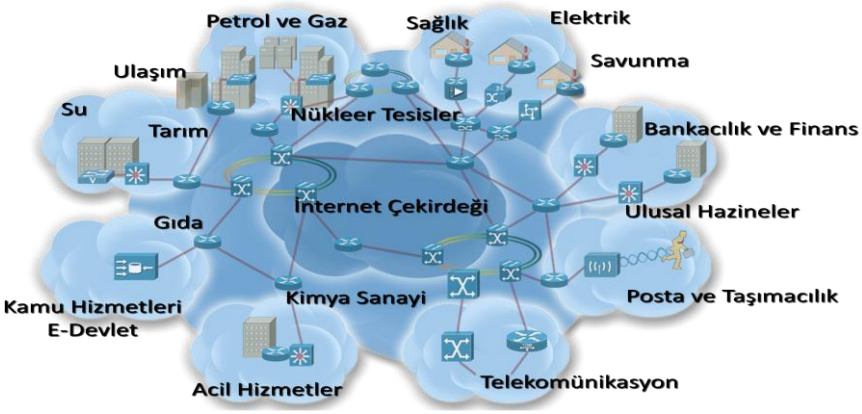
3. SİBER HEDEFLER: DEVLETLERİN SİBER SALDIRILARA KARŞI HASSAS TARAFLARI

Kritik altyapılarda kullanılan BT sistemlerinin güvenliğinin ön plana çıkmasıyla birlikte hem teknik hem de yönetimsel güvenlik önlemleri alınmaya başlanmıştır. Bu sistemler ülke için kritik öneme sahip olduğundan kurumun alacağı önlemler yanında kritik altyapıları işleten kurumların çalışmalarını düzenleyen ve denetleyen kurumlar tarafından gerekli düzenlemeler yapılmaktadır. Örneğin ülkemizde faaliyet gösteren bankalar için BDDK (Bankacılık Düzeleme ve Denetleme Kurumu) düzenleme ve denetleme yapmaktadır. Bu çerçevede BDDK bankaların bilgi sistemlerinde almaları gereken önlemleri yayınlamıştır. Sonrasında da her yıl periyodik olarak yapılan güvenlik testlerin sonuçlarını inceleyerek. Bankaların güvenliğini kontrol etmektedir. Aynı şekilde GSM operatörlerini, internet servis sağlayıcıları, elektronik sertifika hizmet sağlayıcıları düzenleyen ve denetleyen Bilgi Teknolojileri ve İletişim Kurumu bilgi sistemleri güvenliği konusunda düzenlemeler yapmaktadır. Benzer düzenlemeleri elektrik üretim ve dağıtım sistemleri, metrolar, hava limanları, hastaneler gibi kritik altyapıları düzenleyen ve denetleyen kurumların yapması gerekmektedir. Yurt dışında birçok ülkede kritik altyapıları düzenleyen ve denetleyen kurumlar altyapı BT sistemlerin güvenli hale getirilmesi için direktifler ve kılavuzlar yayınlamaktadır.[198]

11 Eylül 2001 İkiz Kule saldırılarından sonra tüm dünyada kritik altyapıların korunması ve içeriden gelen veya gelebilecek ataklara karşı önlemler geliştirme konusunda önemli çalışmalar yapılmaya başlanmıştı. Enerji santralleri, hava limanları, nükleer santraller, barajlar, metrolar, limanlar vb ülke için hayati öneme sahip kritik altyapıların fiziksel ve BT güvenliğinin sağlanması, beklenmeyen olaylar karşısında iş sürekliliğinin devam ettirilmesi, felaket planının yapılması ve uygulanması için çok sayıda proje geliştirilmeye başlanmıştır. İnternetin yaygın olarak kullanılmaya başlanmasıyla birlikte kötü niyetli internet kullanıcıları veya teröristler ülkelerin kritik altyapılarının BT sistemlerine internet üzerinden saldırarak

197 Ibid.
198 Ibid.

zarar vermeye çalışmışlardır. Hatta bu zaman zaman bir ülkenin diğer ülkenin BT altyapısına saldırmasına kadar varmıştır.[199]



Şekil 3- Siber Uzayda Stratejik Hedefler

3.1. SCADA SUNUCULARI

"*Geniş bir alana yayılmış uzak terminal birimlerinin koordineli çalışması, uzak terminal birimlerinden gelen bilgilerin yorumlanarak kullanıcılara sunulması, kullanıcıların isteklerinin uzak terminal birimlerine iletilerek kumanda fonksiyonlarının sağlanması, diğer yazılım katmanları ile entegrasyonunu SCADA sisteminde merkezi yönetim birimi yerine getirmektedir. Merkezi yönetim birimi, uzak terminal birimlerinden bilgileri alır, istenilen bilgileri düzenli olarak kayıt eder, verileri değerlendirerek operatörlerin algılayacağı sesli ve görüntülü şekle dönüştürür. Merkezi yönetim birimi; sunucu, bilgisayar destekli paket uygulamaları, insan makine iletişimi için ara yüzler, ağ anahtarları, yönlendiriciler, yazıcılar, modemler, işletme fonksiyonlarını yerine getirecek yazılımlar ve destek donanımlarından oluşur. Küçük SCADA sistemlerinde merkezi terminal birimi tek bir PC'den oluşabilir. Buna karşın daha büyük SCADA sistemleri çoklu sunucular, dağıtılmış yazılımlar ve yedekleme birimlerinden oluşur. Herhangi bir sunucu arızasında izleme ve kontrol faaliyetlerinin sürekliliğini sağlayarak sistemin bütünlüğünü artırmak için; aktif yedekleme yapısında aktif-aktif şeklinde yapılandırılan çoklu sunucular kullanılmaktadır.*"[200]

---

199 KARA, BAHŞİ, loc.cit.

200 KARA Mehmet, "Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği", http://www.bilgiguvenligi.gov.tr/siber-savunma/elektrik-uretim-ve-dagitim-sistemleri-scada-guvenligi.html, (e.t. 06.01.2012).

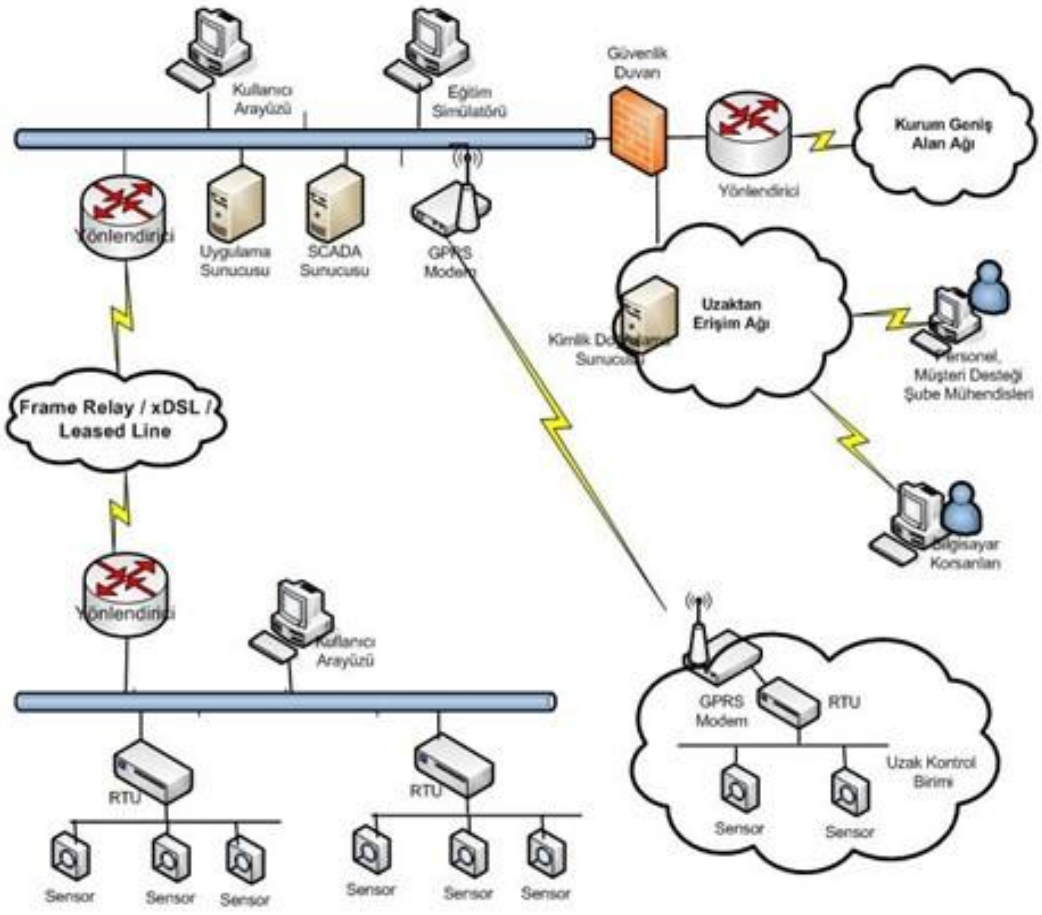
İletişim, SCADA sistemlerinin omurgasını teşkil eder. Merkezi terminal biriminin uzak bölgelerde bulunan çeşitli RTU, bilgisayar veya sistemlerle bilgi alışverişi yapması için bir iletişim hattının olması gerekir. İletişim hatlarını kablolu ve kablosuz iletişim olmak üzere iki gruba ayırmak mümkündür. Büyük SCADA uygulamalarında kablolu ve kablosuz iletişim hatlarından oluşan karma bir yapı söz konusu olabilmektedir. Direk kablo bağlantısı geniş coğrafyaya yayılmış büyük sistemler için uygulamada birtakım sorunları da beraberinde getirmektedir. Direk kablo bağlantısının mümkün olduğu kritik uygulamalarda fiber optik kablo teknolojisi, daha yüksek veri transferi ve arttırılmış güvenlik sağlaması yönünden tercih edilir. Direk kablo bağlantısının mümkün olmadığı durumlarda diğer kurumlardan hat kiralamak (Leased-line, ADSL, DSL gibi), radyo frekans (RF), uydu iletişim, GSM, GPRS, 3G hatlarını kullanmak iyi bir çözüm yoludur. SCADA sistemlerinin güvenilirliğini ve performansını etkilemede iletişim ağının çok büyük rolü vardır. İletişim ağı seçilirken iletişim hızı, güvenilirlik, maliyet gibi parametrelerin göz önünde bulundurularak titiz bir çalışmadan sonra karar verilmesi gerekir. Bazı kritik SCADA projelerinde iletişimin sürekliliğini sağlamak için yedek iletişim hatları kullanılmaktadır. Ana haberleşme hattında bir sıkıntı olması durumunda yedek olarak bekleyen hat otomatik devreye girmektedir. Ana haberleşme hattının ve yedek hattın farklı tipte olması tercih edilir (ADSL-RF, RF-GPRS, Fiber Optik-RF gibi).[201]

3.2. UZAK TERMİNAL BİRİMLERİ (UTB)

Uzak terminal birimleri fiziksel saha ekipmanları ile bağlantıyı sağlarlar. UTB'leri sistemdeki yerel ölçüm ve kumanda noktaları ile haberleşerek ya da I/O (giriş/çıkış) terminalleri yardımıyla yerel ekipmanlardan gelen sinyalleri değerlendirdikten sonra haberleşme hattı üzerinden merkezi terminal birimine bilgi verirler. UTB'leri aynı şekilde merkezi terminal biriminden gönderilen komutları değerlendirdikten sonra sahadaki ekipmanlara kumanda sinyalleri gönderirler. Sistemdeki röle, enerji analizörü, sayaç gibi cihazlarla UTB'leri haberleşerek, akım, gerilim, güç, tüketim gibi elektriksel bilgileri doğrudan alırlar. Aynı şekilde kesici, şalter, yük ayırıcı, solenoid gibi kumanda edilebilir ekipmanları kumanda ederler. Haberleşme imkânı olmayan saha ekipmanlarından bilgileri I/O modülleri vasıtasıyla alırlar. Sahadan gelen sonuçlar, cihazların çalışma durumları ve operatör tarafından girilen komutlar UTB tarafından saha ekipmanlarına iletilir. UTB'lerin programlanabilir cihazlar olması sebebiyle merkez istasyonu üzerindeki işlem yükünün bir

[201] Ibid.

kısmını üzerine alarak sistem veriminin ve performansının artmasını sağlamaktadır.[202] UTB'ler tüm alternatifleri değerlendirmek suretiyle merkezi terminal birimine bilgi vermeksizin alarm uyarıları üretebilir ve bu durumlarda ne yapılacağına anında kendileri karar vererek yerinde müdahaleler yapabilirler. Merkezi terminal birimine sadece olayın sonucunu aktarırlar. Tipik bir SCADA sistemi ağ topolojisi Şekil 4'te görülmektedir.



Şekil 4: SCADA Sistemi

Kaynak: Mehmet KARA, "Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği", http://www.bilgiguvenligi.gov.tr/siber-savunma/elektrik-uretim-ve-dagitim-sistemleri-scada-guvenligi.html, (e.t. 06.01.2012).

202 Ibid.

3.3. ELEKTRİK ÜRETİM VE DAĞITIM SİSTEMLERİ

İlk geliştirilen SCADA sistemleri hem üreticiye özel protokoller kullandığı hem de diğer ağlarla bağlanmadığı için daha çok fonksiyonellik ön plana çıkmış, çok fazla güvenlik özelliği eklenmemiştir. Fakat süreç içerisinde SCADA sistemleri için standart protokollerin yaygınlaşması sistemlerin internet ya da kapalı bilgisayar ağaları üzerinden kontrol edilmesi güvenlik risklerini de artırmaya başlamıştır. Bu riskler SCADA sisteminin internete bağlılık düzeyine göre artmaktadır. Bazı kurumlar SCADA sistemlerinin internete bağlı olmadığını öne sürerek güvenli olduklarını düşünmektedir. Siber atakların arttığı günümüzde Stuxnet zararlı yazılımı bunun doğru olmadığını açıkça göstermiştir. İran nükleer araştırmalarının yapıldığı sistemler internete bağlı olmamasına karşın Stuxnet zararlı yazılımı sisteme bulaşmıştır. Daha önceki yıllarda da birçok kritik altyapının bilgi sistemlerine saldırı yapılmış ve çok ciddi zararlar verilmiştir. Son yıllarda özellikle siber savunma kapsamında kritik altyapılara bilgisayar sistemleri aracılığıyla saldırılar geçekleştirilmektedir. İngiltere'de kritik altyapıların güvenliği konularında çalışma yapan CPNI (Center for Protection of National Infrastructure) proses kontrol ve SCADA sistemlerin güvenliği konusunda bir rehber yayınlamıştır. Yayınlanan rehberde aşağıdaki güvenlik önlemelerinin alınması tavsiye edilmiştir.[203]

- "*İş risklerinin anlaşılması*
- *Güvenli mimarinin gerçeklenmesi*
- *Olayları ele alma yeteneğinin oluşturulması*
- *Farkındalığın arttırılması ve yeteneklerin geliştirilmesi*
- *Üçüncü parti risklerin yönetimi*
- *Projelerin güvenlikle birlikte ele alınması*
- *Sürekli bir yönetişim modelinin kurulması*"

Enerji sistemlerinin bilgi ve iletişim teknolojileri ve altyapıları ile bağlantılı olması onu siber tehditlere daha açık hale getirmektedir. Tüm dünyada başta elektrik ve enerji

[203] Ibid.

sistemleri olmak üzere siber güvenlik açısından kritik altyapıları siber tehditlerden korumak üzere tüm dünyada yoğun çalışmalar ve önemli ölçüde yatırımlar yapılmaktadır.[204]

Elektrik üretim ve dağıtım sistemleri en önemli kritik alt yapılar arasında yer almaktadır. Dünyadaki gelişmelere paralel olarak ülkemizde de enerji sistemlerinin altyapı yönetimi ve izlenmesi büyük oranda BT teknolojileri ile bütünleşen SCADA sistemleri ile yapılmaktadır. SCADA sistemlerinin BT sistemleri ile bütünleşmesi birçok kolaylık ve esneklik sağlaması yanında ciddi güvenlik risklerini de beraberinde getirmektedir. Birçok ülke bu risklerin kapatılması veya seviyelerinin düşürülmesi için yönetimsel, teknik önlemler almakta ve yasal düzenlemeler yapmaktadır. Enerji sistemlerinin kesintisiz, güvenli ve istenilen kalitede hizmet vermesi tüm ülkemizi yakından ilgilendirmektedir. Bu çerçevede dünyadaki birçok ülkede olduğu gibi ülkemizde de enerji üretim ve dağıtım sistemlerinin SCADA güvenliğinin sağlanması için gerekli düzenleme ve denetim mekanizmaları oluşturulup uygulanmalıdır.[205]

3.4. KRİTİK ALT YAPILAR

Temmuz 2010'da keşfedilen ve temel hedefi İran'ın nükleer zenginleştirme programı olduğu tahmin edilen Stuxnet zararlı yazılımı en az 22 endüstriyel sisteme bulaşmıştır. Stuxnet, Siemens PCS7, S7 PLC ve WinCC sistemlerine zarar veren ileri düzey bir zararlı yazılımdır. Dört tane o güne kadar hiç görülmemiş açıklığı ve değişik yayılma yöntemlerini kullanan özel bir zararlı yazılımdır.[206]

2000 yılında meydana gelen atakta ise Avustralya'nın Moroochy eyaletinde 28 Şubat ile 23 Nisan arasında arıtma tesisinden en az 40 defa pis kanalizasyon suları parklara bırakılmıştır. Bu kirli sularla Eyaletteki marina yaşamı yok olmuştur. Yaklaşık iki ay süren ve eyalet yaşamına çok büyük zarar veren bu planlı atağın kaynağı çok uzun çalışmalar sonucunda tespit edilebilmiş ve suçlusu yakalanıp cezalandırılmıştır. Benzeri olaylardan literatürde çok sayıda bulunmaktadır. Günümüzde de bu ataklar artarak ve daha da planlı bir şekilde devam etmektedir. Siber güvenlik uzmanları, bu tür atakların ülkeler tarafından planlı olarak başka ülkelerin sistemlerine yapıldığını düşünmektedirler. Fakat görülüyor ki bunlardan yeteri kadar ders çıkarılmadığı için ataklar devam etmektedir. Bu atakların bazıları

---

[204] ATALAY Ahmet Hamdi, "Akıllı Şebekeler ve Siber Güvenlik: Akılllı Şebekelerde Bilgi Güvenliği", http://elektrikmedya.com/akilli-sebekeler-ve-siber-guvenlik-akilli-sebekelerde-bilgi-guvenligi/, (e.t. 22.10.2012).

[205] Ibid.

[206] KARA, loc.cit.

tespit dahi edilememekte bazıları ise prestij kaybı veya diğer nedenlerden kamu oyuna duyurulmamaktadır. [207]

Bütün altyapılar teknolojik gelişmelerin de etkisiyle, birbirine bağımlı hale gelmektedir. Toplumsal refah ve kamu hizmetlerinin sürdürülebilirliği açısından kritik altyapıların korunması hayati önem arz etmektedir. Bir devletin kritik altyapısında meydana gelen hasar veya arıza diğer kritik altyapılarını ve hatta diğer ülkelerin kritik altyapılarını da etkilemektedir. Kritik altyapıların korunması konusunda ulusal ve uluslararası boyutta çalışmaların yapılması gerekmektedir.[208]

Dünyadaki nüfus artışı, artan ihtiyaçlar ve kaynaklara erişim sorunu, mevcut bürokrasinin yerine güvenli e-devlet uygulamalarıyla daha hızlı ve etkili olarak çözülebilir. Devletler vatandaşlarına daha iyi bir hizmet sağlamak için sanal dünyanın nimetlerinden sonuna kadar faydalanmalıdır. İşte tam bu noktada, e-devlet uygulamaları çok stratejik hale gelmektedir.[209]

ABD, Siber Muharebe Komutanlığını USAF bünyesinde oluşturmuştur ve birimin kabiliyetlerinin sadece savunmaya dayalı değil aynı zamanda saldırıya dayalı olduğu da söylenenler arasındadır. The Defense Advanced Research Projects Agency (DARPA) (ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı) destekli bazı siber güvenlik yazılım geliştirme çalışmaları yapmaktadır. ABD'nin; açık ya da kapalı loop bilgisayar ağlarına hangi yazılım altyapısını kullanıyor olursa olsun sızma, tespit edilmeden ağda kalma, ağları (network) engelleme, hatalı bilgi üretme ve gerekirse tümüyle servis dışı bırakma amaçlı bir takım donanım-yazılım teknolojilerini geliştirmekte olduğu bilinmektedir.[210]

BBC Türkçe servisinin 17 Mart 2011 tarihli haberinde[211] siber güvenlik ile ilgili önemli konulara yer vermiştir. Pentagon'un Amerikan ordusunun ülkeyi siber saldırılardan korumak için gerekli personel ve kaynaklara sahip olmadığı uyarısını yapmıştır. ABD Ordu Komutanı Keith Alexander yaptığı açıklamada "*Sayımız çok az ve herhangi bir kriz siber*

---

207 Ibid.

208 ÜNVER Mustafa, Cafer CANBAY, Hüseyin Burhan ÖZKAN, "Kritik Altyapıların Korunması", Mayıs, 2010, http://www.cybersecurity.gov.tr/publications/CIP_Rapor.pdf, (e.t. 29.10.2012), s. 49.

209 CEYLAN Cenk, "Ulusal Güvenliğin Zayıf Halkası E-Devlet", 11.06.2009, https://www.bilgiguvenligi.gov.tr/siber-savunma/ulusal-guvenligin-zayif-halkasi-e-devlet-2.html, (e.t. 10.09.2011).

210 ÇAY Ömer, "Bilgi Harbi ve Türkiye", **Ekopolitik**, 03.11.2009, http://www.ekopolitik.org/public/news.aspx?id=4348&pid=4082, (e.t 06.09.2011).

211 BBC Türkçe, "Pentagon: Amerika Siber Saldırılara Hazırlıksız", 17.03.2011, http://www.bbc.co.uk/turkce/haberler/2011/03/110317_pentagon_cyber.shtml, (e.t. 30.12.2011).

kuvvetlerimizi zorlayacaktır." demiştir. Amerikan hükümeti, sistemlerinin her gün milyonlarca kez saldırıya uğradığını söylemektedir. Ulusal Güvenlik Bakanlığı yeni bir siber koruma sistemi talep etmektedir. ABD Ordu Komutanı Keith Alexander, ordunun Pentagon ağlarını koruma kapasitesine "*orta*" notu vereceğini söyledi, ancak son yıllarda bu konuda ilerleme kaydedildiğini de kabul etti. ABD yetkilileri, siber suçlular, teröristler ve diğer ülkelerin devlet ve özel ağlara sızmakta daha becerikli hale geldiklerini söylüyor. Siber savaş tehdidinin abartıldığını söyleyen bir grup da var. Güvenlik uzmanı Bruce Schneier, "*sivil savaş*" tehlikesi çevresinde oluşturulan duygusal dilin gerçeklerle örtüşmediğini söylemektedir. Ayrıca, "*Karşı karşıya olduğumuz bir siber savaş değil, savaş taktiklerinin gittikçe daha fazla kullanılması.*" olarak açıklık getiriyor.

"*Çin ile Batı Arasında Sanal Savaş*" isimli makalede ise NATO ve AB'nin gizli istihbarat bilgilerinin Çin'den gelen siber savaş saldırılarına karşı koruma altına alması için seferberlik ilan ettiğini bildirmiştir. Çin kaynaklı siber saldırıların ABD'deki resmi ve askeri kurumları da hedeflediği belirtilirken, siber güvenlik uzmanları AB ve NATO'nun bu saldırılara karşı etkili bir savunma sisteminin bulunmadığını ve özellikle de AB sistemlerinin savunmasız durumda olduğunu belirtmişlerdir. NATO kaynakları, İngiliz The Times gazetesine yaptıkları açıklamada, "*Çinlilerin siber saldırıları yoğunlaştırdığını herkes biliyor ve şimdi artık iç güvenliğimiz konusunda düzenli bir şekilde uyarılıyoruz*." demiştir. Çinlilerin siber saldırılarla NATO ve AB'deki önemli dairelere nüfuz etmesi, gizli istihbarat raporlarının da korunmasız halen geldiğine dair endişelere yol açmıştır. Londra'da hükümet tarafından 2009 yılında kurulan Siber Güvenlik Dairesi'ndeki kaynaklar iki tür saldırı olduğunu açıklamışlardır; bilgisayar sistemlerini aksamaya uğratma amaçlı saldırılar ve hassas bilgileri 'oltayla yakalamak' için yapılan saldırılar. İngiltere hükümeti, siber saldırılar sonucu istihbarat bilgilerinin dışarı sızmasını engellemek amacıyla bir ekip oluşturmuştur.[212]

Alman hükümeti, artan siber saldırılara karşı yeni yapılanmaya giderken, kapsamlı bir "*Siber Güvenlik Stratejisi*" hazırlamıştır. Köln'de kurulacak siber savunma merkezinde uzmanlar ve istihbaratçıların görev yapacağı belirtilmektedir. Almanya İçişleri Bakanı Thomas de Maiziere, Almanya'nın her iki dakikada bir sanal saldırıya uğradığını belirtmiştir. Ayrıca "*Alman Federal Enformasyon Güvenliği Teknolojileri Birimi*" Başkanı Michale Hange, siber güvenliğe karşı alınabilecek tedbirler ile ilgili açıklamaları çok önemlidir.

[212] GÜNEŞ Metin, "Çin ile Batı arasında sanal savaş", CNN Türk, 09.03.2010, http://www.cnnturk.com/2010/dunya/03/09/cin.ile.bati.arasinda.sanal.savas/566888.0/index.html, (e.t.24.10.2011).

"*Hangi alanların tehlikeli ve saldırıya açık olduğunu tam olarak gözlemlememiz ve belirlememiz gerekiyor. Her iki dakikada bir devreye giren zararlı yazılımlar her sistem için tehdit oluşturmaz. Ancak hangi sistemlerin tehlike altında olduğunu anlamak için çok hassas davranmak şart.*" [213]

3.5. WEB UYGULAMALARI GÜVENLİĞİ

HTTP (Hyper Text Transfer Protocol) protokolü ilk tasarlandığında sadece statik web sayfalarının gösterimi amaçlanmıştır. Sonraları dinamik sayfalar da bu protokol kapsamında iletilmiş ve günümüzde internet bankacılığı gibi karmaşık ve kritik sistemlerin üzerine bina edildiği bir protokol haline gelmiştir. Protokol baştan güvenlik düşünülerek tasarlanmadığı için birçok güvenlik açığı ortaya çıkmış ve bu açıklıkları kapatmak adına çözümler üretilmiştir. Web uygulamalarının internet üzerindeki en kritik sistemlerin temelini oluşturması ve http protokolünün güvenli olmayan altyapısı sebebiyle saldırganlar, web uygulamalarını çokça hedef almaktadır. IBM (International Business Machines)'in 2008 risk raporuna göre 2008 yılı içerisinde çıkan güvenlik açıklıklarının %55'i web uygulamaları ile ilgilidir. Web uygulamaları açıklıklarının önemli bir kısmını da siteler arası betik yazma (cross-site scripting), sql-enjeksiyonu (sql-injection) ve dosya içerme (file include) açıklıkları oluşturmaktadır. Özellikle açıklık arama ile ilgili araştırma yapanlar web uygulamaları açıklıkları üzerinde yoğunlaşmışlardır ve yoğunlaşmaya devam edeceklerdir.[214]

3.6. KABLOSUZ MOBİL SENSÖR AĞLAR

Mobil teknolojilerin kullanılması günümüzde çok yaygın hale gelmiştir. Bir yandan da mobil teknolojiler yaygın bir şekilde askerî alanda da kullanılmaktadır. Ne yazık ki çok kolay bir şekilde, mobil cihazlarda kötü niyetli yazılımların veya donanımların geliştirilmesi söz konusudur. Diğer taraftan yüz binlerce cep telefonu, hava limanlarında ya da uçaklarda unutulmakta ve bunların bazılarında kritik bilgiler bulunmaktadır.[215]

Kablosuz mobil sensör uygulamaları özellikle çevre gözleme, gözetleme, askeri aktiviteleri izleme, akıllı ev uygulamaları ve yardımcı yaşama desteği alanlarında yaygın olarak kullanılmaktadır. RFID (Radio Frequency Identification, Radyo Frekanslı Tanımlama) sistemler ise ürün tedarik zincirinin işleyiş kalitesinde, otoyol gişeleri, alışveriş merkezleri

213 http://www.dw-world.de/dw/article/0,,14872470,00.html, (e.t. 10.01.2012).
214 KARA, BAHŞİ, loc.cit.
215 ÜÇÜNCÜ, loc.cit.

gibi sürekli yoğunluk problemi olan yerlerde, kimlik ve güvenli geçiş uygulamalarında, takip uygulamalarında (öğrencilere, mahkûmlara, hayvanlara, vb.), envanter yönetimi uygulamalarında başarılı olarak kullanılmaktadır.[216]

Bu teknolojilerin her ikisi de iş odaklı geliştirildikleri için iki teknoloji için de güvenlik problemi ikinci planda kalmıştır. Kablosuz mobil sensör ağlarının güvenliği, sensör ağların güvenlik engelleri, sensör ağların gereksinimleri, ataklar ve savunma önlemleri olmak üzere üç kategoride ele alınmaktadır. [217]

- "*Sınırlı güç tüketimi, bellek ve saklama alanı,*
- *Genel yayın olması, çarpışma ve gecikmeden dolayı güvenirliği düşük haberleşme,*
- *Merkezi olarak yönetilse bile fiziksel tehditlere açık olması*"

Kablosuz mobil sensör ağlarda yukarıda saydığımız ataklara karşı önlem almak için ve güvenlik gereksinimlerini karşılamak için kriptografik protokollerle* savunma mekanizmaları kullanılmaktadır. Fakat işlemci gücü, saklama, alanı, enerji sınırlılığından dolayı etkin güvenlik protokolleri kullanmak kolay değildir. Son yıllarda ekonomik, kaynakları etkin kullanacak güvenli haberleşebilecek kablosuz mobil senör ağlar ve RFID sistemler konusunda projeler geliştirilmektedir. [218]

3.7. VERİ GÜVENLİĞİ

Günümüzde kişilere, kurumlara hatta ülkelere ait verilerin büyük bir kısmı disk sistemi, sabit disk, usb bellek, flash disk, CD, DVD gibi sayısal saklama ortamlarında saklanmaktadır. Bu saklama ortamlarında saklanan bilgilerin tamamı aynı gizlilik seviyesinde değildir. Bazı verilerin ortaya çıkması kişileri veya kurumları para, zaman, prestij kaybı gibi önemli kayıplarla karşı karşıya bırakabilmektedir. Bilgilerin önemlerine uygun olarak güvenliğin temel üçayağı olan gizlilik, bütünlük ve sürekliliğinin sağlanması çerçevesinde

---

216 KARA, BAHŞİ, loc.cit.
217 Ibid.
* Bir çeşit şifreleme sistemi
218 Ibid.

gizliliğin korunması adına gerektiğinde güvenli olarak silinmesi ya da imha edilmesi de büyük önem taşımaktadır.[219]

Bilgilerin ilgisiz kişilerin eline geçmemesi için cihazlar kullanıldığı sürece şifreleme, kimlik doğrulama, yetkilendirme gibi birçok güvenlik önlemi alınmaktadır. Fakat silindiği düşünülen dosyalar, saklama ortamının uygun bir şekilde silinmemesi durumunda sayısal adli analiz araçlarıyla ya da basit yazılım araçlarıyla kolayca geriye döndürülebilmektedir. Hatta bu saklama ortamları zaman zaman kontrolsüz bir şekilde elden çıkarılabilmektedir. Örneğin çok kritik bilgileri bulunan bir kurum veya kişi eskiyen bilgisayarını herhangi bir işlem yapmadan başka bir kuruma bağışlayabilmekte, hurda olarak satabilmekte ya da doğrudan çöpe atabilmektedir. Bozulan veya çok eskiyen bilgisayarlar disklerinin uygun bir şekilde silinmemeden veya elden çıkarılması çok önemli bilgilerin ilgisiz kişilerin eline geçmesine neden olmaktadır. Hatta bu bilgisayarlara ait saklama ortamları yeterince güvenli olmayan yöntemlerle silinmesi durumunda verilerin büyük bir bölümünün veya tamamının geriye döndürülmesi mümkün olmaktadır. Bu yetkisiz geriye döndürmelerin ortadan kaldırılması için veriler önemlerine uygun olarak silinmelidir.[220]

Veriler bilgisayar ortamlarında saklanırken işletim sistemleri ve uygulama yazılımları aracılığıyla ilgisiz kişilerden kimlik doğrulama ve yetkilendirme güvenlik önlemleriyle korunurlar. Örneğin bilgisayarımız çalışırken başından ayrıldığımızda ya bilgisayarı kapatırız ya da kilitleyerek ilgisiz kişilerin çalışma ortamımıza erişmesini engelleyebiliriz. Eğer çok sayıda kullanıcının dosyasının bulunduğu bir ortamda çalışıyorsak o zamanda yetkilendirme mekanizmasını kullanarak hangi kullanıcının hangi dosyalara erişim yapabileceğini belirleriz ve her kullanıcı kendi yetkileri çerçevesinde dosyalara ulaşabilir. Tabi ki bilgisayardaki verileri şifreli olarak tutmuyorsak bu çözüm yeterli olmaz çünkü bilgisayar çalıştırılabilir bir CD ile açılarak sabit disk üzerindeki veriler okunabilir, bilgisayarın sabit diski çıkarılıp başka bir bilgisayara takılarak içindeki veriler kolayca görülebilir. Çok önemli bilgilerin bilgisayarda açık olarak saklanması uygun değildir. Birçok düzenleme ve yasa önemli verilerin saklanması ile yakından ilgilenir.[221]

İnsanlar verilerini kaybetmemek için değişik yöntemlere başvurmaktadırlar. Uzmanlar tarafından kabul edilen gerçek, sanal ortamda güvenliği yüzde yüz sağlamanın mümkün

---

219 KARA, loc.cit.
220 Ibid.
221 Ibid.

olmadığıdır. Her geçen gün konuyla ilgili yeni teknolojiler üretilmekte, söz konusu teknolojilerin belirli kişi ya da kuruluşların elinde bulunması verilerin güvenli bir şekilde korunmasını zorlaştırmaktadır.[222]

Kişilere ait bilgilerin büyük bir kısmı bedava e-posta hizmeti sunan Hotmail, Yahoo, Gmail gibi eposta sitelerinde, Facebook, Twitter, Netlog, MySpace gibi sosyal paylaşım sitelerinde, Youtube gibi video paylaşım sitelerinde, Msn, Skype gibi mesajlaşma sitelerinde tutulmaktadır. Bu verilerin nerede tutulduğunu biz sildiğimiz zaman gerçekten silinip silinmediğini bilmiyoruz. Hatta bize ait verileri zaman içinde silemez duruma bile düşebiliyoruz. Örneğin size ait özel bir resmin başkaları tarafından kopyalandığını ve farklı bir ülkedeki internet servis sağlayıcı üzerinden yayınlandığını düşünün. Bu resminizin yayından kaldırılmasını sağlamanız aylar sürebilir belki de mümkün olmayabilir. O yüzden bu tür kontrolü bizde olmayan sitelere bilgi yüklerken iki defa düşünmemiz gerekir. Televizyon haberlerinde, gazetelerde, internette bu tür sitelerin olumsuz sonuçlarına ait her gün onlarca haber görülmektedir. Bu haberlerin en önemlilerinden biri Google yöneticisi Eric Schmidt'in "*İleride gençler belki de twitter, facebook gibi sosyal paylaşım sitelerine yazdıklarından kurtulmak için isimlerini değiştirmek zorunda kalacaklardır.*" açıklamasıdır. Uzaktan baktığımızda tamamen bizim kontrolümüzde gibi görülmesine rağmen oraya yazdığımız bilgilerin ya da koyduğumuz dokümanların kimlerin eline geçtiğini bilemiyoruz.[223]

Getirdiği yeniliklerle hayatımızı kolaylaştıran bilgisayarlar, en değerli verilerimizi işleme, saklama ve iletme işlemlerini de yerine getiriyor. Bilgisayarlar verilerin gizliliğine uygun olarak saklanması ve gerektiğinde silinmesi ya da saklama ortamının tümden imha edilmesi büyük önem arz etmektedir. Bu yüzden kurumlar ya da kişiler verilerini saklarken güvenli saklama ve silme yöntemlerini kullanmalıdırlar. Özellikle internet ortamında kullanılan ve verileri nerede sakladığını bilmediğimiz uygulamalara minimum güvenlik düzeyindeki verileri yüklemeliyiz.[224]

3.8. MOBİL SİSTEMLER

Günümüzde cep telefonları, mesaj atmak ve konuşmak gibi basit iletişim aracı olarak kullanılmaktan öteye giderek medya, oyun, internet ve doküman yönetimi için kullanılan

---

222 AL Umut, "İnternet'te Veri Güvenliği", http://yunus.hacettepe.edu.tr/~umutal/publications/datasecurity.pdf, (e.t. 22.10.2012).

223 Ibid.

224 Ibid.

cihazlara dönüşmüştür. Akıllı cep telefonları denilen bu cihazların çeşidi ile beraber sayıları da artmaya devam etmektedir. Cep telefonlarında kullanılan işletim sistemlerinin çoğu iPhone OS, Android ve RIM OS gibi gelişmiş mobil işletim sistemlerinden oluşmaktadır.[225]

Virüsler ile ilgili genel duruma bakıldığında bilgisayar virüslerinin sayısı yarım milyar, mobil virüs sayısı da 1227 dolayında ve bu virüsler her geçen yıl katlanarak artıyor. Cep telefonları arasında yayılan virüsler, kullanıcıdan habersiz, telefonda bulunan iletişim bilgilerini de kullanarak mesajlar yollayabiliyor ya da telefonda kayıtlı bulunan banka bilgileri ya da şifreleri gibi önemli bilgileri mesaj yoluyla çalabiliyor, hatta telefonda bulunan kayıtlı bilgileri silebiliyor. Kullanıcının haberi olmadan günde 10 tane uluslararası telefon numarası arayarak bedeli yüksek faturalara neden olabiliyor. Diğer yandan bu gibi olaylarda aynen kişisel bilgisayarlarda olduğu gibi cep telefonu üzerinden yasal olmayan işlemlerin yapılmasına da olanak tanıyor. Cep telefonlarında virüslere karşı koruma sağlamak için şu gibi basit önlemler alınmalı, Bluetooth sürekli açık olmamalı, Bluetooth şifreleri kırılması zor güçlü şifreler olmalıdır. Ayrıca bilinmeyen, güvenliğinden emin olunmayan sitelere girilmemelidir. Telefonlara kurulan uygulamalardan gelen tehlikelere bakıldığında, kaynağı bilinen ve güvenilen uygulamalar dışında kaynağı çok da tanınmayan birçok uygulama bulunmaktadır. Kullanıcıların, uygulamaları telefonlarına kurmadan önce dikkat etmeleri gereken bazı hususlar vardır. Telefona bir uygulama kurarken uygulamanın yetkili bir otorite tarafından kontrol edilmiş olmasına veya uygulama üreticisine dikkat edilmelidir.[226]

3.9. ENDÜSTRİYEL SİSTEMLER

Enerji santralleri, nükleer santraller, barajlar, petrol istasyonları gibi modern endüstriyel sistemler büyük karmaşık sistemlerdir. İşletim esnasında bu sistemlerin değişik kısımlarının operatörler tarafından gözlenmesi ve kontrol edilmesi istenir. Günümüz ağ teknolojileri bu izleme ve kontrol işlemini mümkün kılmaktadır. Önceki ağ kontrol uygulamaları noktadan noktaya bir parçayı ya da cihazı kontrol edebilecek yapıda tasarlanmıştır. Bu yapılar zaman içerisinde merkezi kontrol ünitesi ve birçok uzak birim arasındaki haberleşmeyi ortak veri yolları ile haberleştirecek şekilde geliştirilmiştir. Bu ağlardaki uzak birimler belli amaçlar için geliştirilmiş gömülü sistemleri içeren sensörler, harekete geçiriciler ve PLC (Programmable Logic Control) gibi parçalardan oluşmaktadır.

---

225 ÇERİ Yusuf, "Mobil Güvenlik", TÜBİTAK-UEKAE, http://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-guvenlik.html, (e.t. 06.02.2012).

226 Ibid.

Üstelik bu sistemler birbiri ile uyumlu değildir. Günümüzde bu endüstriyel komuta kontrol ağlarının gelişmiş hali SCADA (Supervisory Control and Data Acquisiton) olarak adlandırılmaktadır.[227]

Günümüz rekabetçi ortamında endüstriyel ortamların düşük maliyeti ve etkin üretimi yakalaması için kendi SCADA sistemlerini modernize etmeleri gerekmektedir. Günümüz SCADA sistemleri kurum ağlarına ve internete bağlanabilmektedir. Bu bağlantı üretimi ve dağıtık veri işlemeyi kolaylaştırmasına karşın sistemi internetin güvenlik problemleri ile karşı karşıya bırakmaktadır. Eğer cihazlar internet üzerinde kontrol edilirse SCADA sistemine yapılan bir atak tüm sistemi etkileyebilmektedir. Bu atak sonucunda fiziksel ve ekonomik kayıplar yanında insanlar diğer canlılar ve çevre zarar görebilmektedir. Bu sebeple SCADA sistemlerin güvenliğinin birincil öncelikli olması gerekmektedir. [228]

TCP/IP protokolünün açık yapısı ve internet uygulamalarının yaygınlaşması ile birlikte ilk önceleri seri arabirimler aracılığı ile PLC gibi sistemler, bilgisayarlar aracılığı ile kontrol edilmeye başlanmış sonra ise SCADA sistemleri doğrudan Ethernet arayüzünü kullanılarak bilgisayar ağlarıyla haberleşmeye başlamıştır. Bu haberleşme bilgisayarın gelişmiş yazım yeteneği ve grafik arayüzünün SCADA sistemler tarafından kullanılmasını sağlamıştır. SCADA sistemlerin bilgisayar ağları ile haberleşmesi için çeşitli kuruluşlar tarafından Ethernet/IP, DeviceNet, ControNet, PROFIBUS, MODEBUS TCP/IP, DNP3, Foundadion Fieldbus gibi protokoller geliştirilmiştir. İç tehditlerin, siber atakların arttığı günümüz internet yapısında çok kritik altyapıları işleten SCADA sistemlerin güvenliğinin sağlanması için erişim kontrolü, güvenlik duvarı, saldırı tespit sistemi, VPN gibi güncel sınır güvenliği önlemleri yanında protokol güvenlik analizi, SCADA sistemlerin işletim sistemleri güvenlik analizi gibi konularda çok sayıda proje geliştirilebilir.[229]

Günümüzde, bilgi teknolojilerinin gelişmesine paralel olarak, casusluk araç ve teknikleri de farklılaşmıştır. Rakip bir şirketin, ARGE (araştırma geliştirme) laboratuarındaki Nano teknolojiyle ilgili araştırma sonucunu çalmak için içeriye casus olarak insan göndermek en son çare olarak düşünülebilir. İş süreçlerinin tüm aşamalarında kullanılan bilgisayarlar, bu iş için en yetkin casuslar, fiziksel olarak kapılarına güvenlik görevlisi, X ışınıyla tarama sistemleri, biyometrik kimlik doğrulama sistemleri koyduğumuz çalışma alanlarındaki

227 KARA, BAHŞİ, loc.cit.
228 Ibid.
229 Ibid.

bilgisayarlara görünmeyen 65 bin kapıdan (port) erişilmesi, kontrol edilmesi ve uzaktan yönetilmesinin sanayi casuslarınca tercih edildiği bilinmektedir.[230]

Barack Obama (ABD Başkanı) seçilir seçilmez, elindeki BlackBerry telefon alınıp, yerine NSA siparişi ile General Dynamics tarafından üretilen Sectera EDGE modeli yeni bir telefon verilmiştir. ABD Başkanı için tercih edilmesinin nedeni güvenlik standartlarının yüksek olmasıdır. ABD Ulusal Güvenlik Ajansı NSA'in onayından geçen ürün güvenli kablosuz internet bağlantısı, dâhili Common Access Card (CAC) desteği, Type 1 şifrelenmiş veri saklayabilme gibi özellikler sunabilmektedir. AR-GE ve çok gizli çalışmaların yapıldığı kurumlarda, içeriye alınan tüm BT cihaz ve malzemelerinin, aynı şekilde dışarıya çıkarılırken, gizlik ve risk değerlerine göre imhası, hurdaya çıkarılması çok önemlidir.[231]

Bilişim sistemleri güvenliği konusunda yapılan araştırmalar ve projeler internetin askeri, e-devlet, e-sağlık, e-ticaret, e-öğrenme, gibi konularda tüm dünyada yaygın olarak kullanılmaya başlamasıyla birlikte hız kazanmıştır. Günümüzde de bilişim sistemleri güvenliği alanındaki araştırmalar devam etmektedir. Bilgisayar ağlarında taşınan, işlenen ve saklanan bilgilerin artmış olması, güvenliğin dolayısıyla da güvenlik araştırmalarının önemini daha da artırmıştır. [232]

Bilgisayar ağlarında gizlilik, bütünlük ve sürekliliğin sağlanması için hali hazırda geliştirilmiş bilişim teknolojileri projeleri yanında son yıllarda iç tehdit, kişisel gizlilik, güvenli yazılım geliştirme, web uygulaması güvenliği, kablosuz mobil sensör ağları, RFID güvenliği, siber ataklar ve endüstriyel sistemler BT güvenliği konularında yeni projeler geliştirilmektedir. AB çerçeve programları, ülkelerin çeşitli destekleme programları ile bu alanlarda yapılan projeler hız kazanmıştır. Bilişim sistemleri güvenliği alanında yeni çözümlerin geliştirilmesi daha güvenli bir iletişim ortamı sağlanmasına ve geliştiren kurum veya ülkenin teknoloji pazarında ön plana çıkmasını sağlayacaktır. Türkiye'de bu konularda geliştirilecek projelere, AB Çerçeve Programları başta olmak üzere TÜBİTAK'ın SAVTAG, KAMAG ve diğer programlar çerçevesinde destek bulunabilir. Ayrıca sadece BT güvenliği alanlarında bilimin ve ülkenin önceliklerine göre istenilen çözümlerin detaylı tanımlandığı

---

230 CEYLAN Cenk, "Savaş Cephesi Olarak, Sanal Ortamda Savunma ve Saldırı", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/savas-cephesi-olarak-sanal-ortamda-savunma-ve-saldiri.html?Itemid=6, (15.02.2012).

231 Ibid.

232 KARA, BAHŞİ, loc.cit.

destekleme ve iş birliği programlarının oluşturulması söz konusu alanlarda etkisi yüksek projeler geliştirilmesinde faydalı olacaktır.[233]

4. İÇ TEHDİT

Bilgi güvenliği tehditleri arasında, organizasyon bünyesinde çalışan kişilerin oluşturabileceği bilinçli veya bilinçsiz tehditler olarak tanımlayabileceğimiz iç tehditler çok önemli bir yer tutmaktadır. Bilinçli tehditler iki kategoride ele alınabilir. Birinci kategori, organizasyonda çalışan kötü niyetli bir kişinin kendisine verilen erişim haklarını kötüye kullanmasını içermektedir. İkinci kategori ise bir kişinin başka birine ait erişim bilgilerini elde ederek normalde erişmemesi gereken bilgilere erişerek kötü niyetli bir aktivite gerçekleştirmesini kapsamaktadır. Veritabanı yöneticisinin, eriştiği verileri çıkar amacıyla başka bir firmaya satması ilk kategoriye verilecek örnektir. Veritabanı yöneticisi olmayan ve normalde veritabanına erişim hakkı bulunmayan birisinin erişim bilgilerini bir şekilde elde etmesi ve bunu çıkarı için kullanması ikinci kategoriye örnektir. CSI (Computer Security Institute) tarafından yapılan ankete göre katılımcıların %44'ü 2008 yılı içerisinde iç suiistimal yaşamışlardır. Söz konusu oran, iç suiistimallerin %50'lik virüs tehdidinden sonra ikinci büyük tehdit olduğunu göstermektedir. Bu tür suiistimallerin tespitinin zor olduğu ve çoğunlukla organizasyon dışına bu konuda çok bilgi verilmek istenemeyebileceği de düşünülürse aslında %44'lük oranın daha büyük olduğu düşünülebilir. Anket çalışmasında, suiistimal tabiri ile sadece bilinçli oluşan iç tehditlerin kastedildiği anlaşılmaktadır.[234]

5. KİŞİSEL GİZLİLİK

Kişisel gizlilik, bir kişinin ya da bir grubun kendilerine ait bilginin kimlere ve hangi şartlar altında iletileceğinin bizzat o kişilerin/grubun onayı ile gerçekleştirilmesi anlamında kullanılmaktadır. Kişisel gizliliğin sağlanması iki farklı durumda da gerçekleştirilmelidir. İlk durum, kişisel verilerin kişilere ait bilgi sistemlerinde bulunduğu esnada tüm tehditlere karşı korunmasıdır ki bu anlamda herhangi bir bilginin korunması için geçerli tedbirler uygulanır. Bu tedbirler, erişim denetimi, yetkilendirme, sürekliliğin sağlanması gibi konuları içerir. İkinci durum ise kişisel verinin bir başka sistemle ihtiyaç dahilinde paylaşılmasında uygulanacak güvenlik tedbirlerini kapsar. Bu tedbirler, verinin içeriğinin kişi tarafından paylaşılması onaylanmamış kısmının filtrelenmesi, filtrelenmiş verinin ilgili sisteme güvenli

233 Ibid.
234 Ibid.

aktarımı ve söz konusu verinin sadece veri sahibi kişiler tarafından onaylanmış organizasyonlarla paylaşılmasını içerir. [235]

Kişisel gizlilik ile ilgili çalışmalar literatürde verinin kişisel gizliliğinin korunarak yayınlanması (privacy preserving data publishing) adıyla ele alınmaktadır. Bu metodlar, verilerin hiç bir şekilde sahibi ile sahibinin kritik bilgilerini eşleştirmeyecek şekilde anonimliğini sağlayarak iletilmesini gerçekleştirmeye yöneliktir. Örneğin, hastaneler araştırma projeleri için araştırma merkezleri ile hasta verilerini paylaşabilmektedirler. Burada paylaşılan bilgilerden, spesifik olarak herhangi bir kişinin hangi hastalığa sahip olduğuna araştırma merkezinin ulaşamaması beklenmektedir. Bu soru, sadece veri içerisinde kişiyi tekil olarak belirleyebilen TC. kimlik numarası, isim ve soyadı gibi bilgilerin çıkarılması ile çözülememektedir. Kişilere ait cinsiyet, adres gibi veriler de çoğunlukla spesifik olarak bir kişiyi tespit etmede yardımcı olmaktadır. Yapılan çalışmalarda, bu tip veri kısımlarının da kişisel gizliliği sağlayacak şekilde genelleştirilmesi ya da silinmesi sağlanmaktadır. Aslında verilerde bu tür işlemler, veri kalitesini düşürmektedir. Şu andaki ve gelecekteki çalışmalar çoğunlukla kişisel gizlilik ölçüm metriklerinin belirlenmesi, bu metriklere uyacak şekilde verinin olabilecek maksimum kalitede paylaşılabilmesine olanak sağlanması üzerinde yoğunlaşacaktır. Söz konusu metriklerin belirlenmesinin, sadece bilgisayar mühendislerinin değil, sosyoloji, psikoloji, hukuk alanlarında çalışanlarla yapılabilecek disiplinler arası çalışmalarla mümkün olabileceği değerlendirilmektedir. Bilgi güvenliği araştırmalarında en önemli problemlerden birisi, araştırmacıların yeterli ve gerçek test verisi bulamamalarıdır. Bu durum, sistem işleten organizasyonların kurum mahremiyeti açısından sistem verilerini paylaşmaması sebebiyledir. Verilerin kurum mahremiyetini de sağlayarak paylaşılabilmesi için ortaya konabilecek araştırmaların yakın gelecekte artacağı ve bu çalışmaların bilgi güvenliği alanının geneline de çok fayda getireceği öngörülmektedir.[236]

6. VERİLERİN SAKLAMA ORTAMLARINDAN SİLİNMESİ VEYA SAKLAMA ORTAMLARININ İMHA EDİLMESİ

Verilerin güvenli olarak silinmesi güvenli saklanması kadar önemli bir konudur. Çünkü verilerin etkin bir şekilde silinmemesi durumunda basit adli analiz araçları ile veriler kolay bir şekilde geriye döndürülebilmektedir. Verilerin güvenli olarak silinmesi verilerin gizlilik dereceleri ve daha sonra saklama ortamının hangi amaçlar için kullanılacağı ile

235 Ibid.
236 Ibid.

yakından alakalıdır. Örneğin özel verileri içeren bir saklama ortamındaki verileri sildikten sonra aynı gizlilik derecesine sahip verileri saklayacaksak basit silme yöntemlerini kullanmamız yeterli olabilir. Buna karşın gizli seviyesindeki bilgileri tuttuğumuz bir saklama ortamında açık verileri saklayacaksak bu saklama ortamı herkes tarafından görülüp incelenebileceği için içindeki verilerin güvenli yöntemlerle silinmesi gerekmektedir. Saklama ortamlarından verilerin silinmesi ve yeniden kullanılması konusunda aşağıdaki maddeler yaygın olarak kullanılmaktadır.

- "*Hassas bilgi içeren saklama ortamları fiziksel olarak imha edilmeli ya da her bir silmeden sonra saklama ortamının rastgele karakterlerle doldurulduğu güvenli silme programları ile üç defa silinmelidir.*
- *Tüm saklama ortamları, elden çıkarılmadan (devir, satış, çöpe atma vb.) önce hassas veri açısından kontrol edilmeli. Hassas veri içeriyorsa güvenli olarak silinmelidir.*
- *Şifrelenmiş verileri saklayan diskler doğrudan elden çıkarılmamalı basitte olsa silme işlemine tabi tutulmalıdır.*
- *Hassas bilgi içeren saklama ortamları tamir edilemiyorsa imha edilmelidir.*
- *Kurum kendisi için güvenli silme prosedürü oluşturmalı ve veri silmede onu kullanmalıdır.*
- *Aynı gizlilik seviyesinde kullanılacak saklama ortamlarının bir defa silinmesi yeterli olabilir."* [237]

7. SİBER SALDIRILARIN MALİYETİ

Günümüzde internet kullanımının yaygınlaşması özellikle elektronik bankacılık ve elektronik ticaret sistemleri ile elektronik haberleşme ve elektronik eğitim platformlarının kullanıma alınmasını beraberinde getirmiştir. İnsanların evden veya işyerlerinden tüm ihtiyaçlarını elektronik platform ve uygulamalar ile yürütmesi kullanım açısından çok büyük kolaylıklar sağlıyor olsa da bu uygulamaların varoluşu yine beraberinde çeşitli güvenlik açıklarını doğurmuştur. [238]

Özellikle elektronik bankacılık ve elektronik ticaret platformlarındaki güvenlik açıkları neticesinde ortaya çıkan kayıplar (ticari casusluk, para aktarımı, yetkisiz erişim v.s.) milyon dolar mertebesine ulaşmıştır. Alınan önlemler her defasında yine hem insana hem de

237 Ibid.
238 GÖKALP, loc.cit.

teknolojiye bağımlı olarak kırılabilir olmuştur. Özellikle bu uygulamalarda kullanılan statik şifreler ile buna benzer statik kimlik tanıma yöntemleri güvenliğin sağlanmasında aktif rol oynasa da gerçek bir kimlik tanıma işlevi sağlamamaktadırlar. Bu nedenle örneğin bankacılık işlemlerinin tam ve güvenli olarak elektronik ortamda yapılabilmesi için onay ve yetki güvenliğinin sağlanması, giderilmesi gereken eksikliklerin başında yer almaktadır. [239]

8. SİBER GÜVENLİĞİN SINIRLARI

Elektronik iletişimin bazı çeşitleri eşzamanlıdır. Telefon konuşmaları, masaüstü ağları, gerçek zaman işitsel ve video görüşmeleri, elektronik toplantı sistemleri ve elektronik ekranlar liderler ve takımları arasında eş zamanlı olarak gerçekleşir. Telefonla mesajlaşma, elektronik mektup, grup programları ve takvimleri, elektronik ilân tahtaları, iş akışı uygulamaları ve gerçek zaman dışı veri tabanı bölüşümü gibi diğer elektronik iletişim şekilleri eş zamanlı değildir. Yorumlara ve sorulara verilen cevaplar anında gelmez. İletişim ABD ve Japonya gibi değişik zaman bölgeleri arasında yapılıyorsa sorunlar daha da artmaktadır. Ancak 35 sanal takımla yapılan denemeler zaman uyumunun bu tür sorunların olumsuz etkilerini azalttığını göstermiştir. Zaman uyumu takımların İngiltere, Hindistan, Japonya ve ABD gibi zaman bölgelerindeki takımlarda olduğu gibi işi kendi çalışma nöbetlerinin sonuna doğru başkasına devrederek işin günde 24 saat sürdürmelerini sağlayarak yazılım gelişiminin sürekli olmasını mümkün kılar.[240]

Elektronik iletişim süreksizdir. Elektronik mesajlaşma, kendiliğinden iletişime en yakın haberleşme biçimidir. Genellikle, gönderici ve alıcı arasında sadece bir anlık fotoğraf gönderilir. Doğal ve sözsüz etkileşim yoktur. Toplumsal statü ile gönderici ve alıcıların çeşitliliği çok belirgin değildir. Kişilikle ilgili ipuçları yoktur. Davranışların görünmezliği söz konusudur. Geleneksel denetim ve kontrol şekilleri mevcut değildir. İkincil çabalar gözlenemez. Bireyler aldatıcı olabilir, takım çıkarlarını göz ardı edebilir ve diğerlerinin eylemlerini önceden sezemeyebilirler.[241]

9. SİBER GÜVENLİK VE ÖZEL SEKTÖR

BBC'in 4 Mayıs 2011 tarihli haberinde Çin'in "*Devlet İnternet Enformasyon Dairesi*" adlı kurum ile internette bilgi akışını denetleyecek yeni bir hükümet kurumu oluşturduğunu

239 Ibid.
240 Ibid.
241 Ibid.

bildirmektedir.[242] Devletler bir taraftan dışarıdan gelebilecek saldırılara karşı savunma tedbirleri oluştururken diğer taraftan da kendi iç güvenlikleri adına ulusal internet ağı içerisindeki veri akışını kontrol etmeyi kimi zaman kısıtlamaya çalışmaktadırlar. En güzel örnekleri İran ve Kuzey Kore'dir. Bu devletlerde internetin uluslararası ulaşımına kısıtlamalar getirilmesi söz konusudur.

Estonya atağı ülkeler arasında, ilk siber savaş denemesi olmamıştır. Gürcistan ile Rusya arasında Güney Osetya bölgesinden dolayı yaşanan politik çekişmeler sonucu 11 Ağustos 2008 tarihinde çıkan savaştan önce siber savaş başlamıştır. Rusya kaynaklı gerçekleştirildiği düşünülen siber saldırılar, askeri birliklerin savaşa girmesinden önce, 20 Temmuz 2008 tarihinde Gürcistan Devlet Başkanı Mihail Saakaşvili'nin internet sitesi olan www.president.gov.ge adresini hedef alarak başlamıştır. Ülkedeki birçok internet sitesi çökertilmiş ya da içeriği değiştirilmiştir. Bu ataklar dağıtık servis dışı bırakma (Distributed Denial of Service) türü ataklar olarak gerçekleştirilmiştir. Ataklarda çok sayıda köle bilgisayar kullanıldığı için atakları durdurmak ve kaynağını tespit etmek kolay olmamıştır. [243]

4 Temmuz 2009 tarihinde ABD ve Güney Kore'ye ait çeşitli sitelere siber ataklar yapılmıştır. Güney Kore'de başta Ticaret ve Maliye bakanlığı sistemleri olmak üzere birçok kamu kurumu hedef alınmıştır. Ataklarda yaklaşık 50000 köle bilgisayar kullanılmış ve 20-40 Gbps'lık bir trafik oluşturulmuştur. Güney Kore yetkilileri atakların Kuzey Kore veya onun sempatizanları tarafından organize edildiğini ifade etmişlerdir.[244]

NATO başta olmak üzere birçok organizasyon ve ülke siber atakları tespit etmek, önlemek ve atak sonrasında sistemleri normale dönüştürmek için organizasyonlar kurmakta ve projeler geliştirmektedir. Bu konudaki çalışmaların artarak devam etmesi beklenmektedir.[245]

Wikileaks belgeleri Kasım 2010 sonlarında yayınlandığında, Amerikan diplomasisi bundan etkilenmiştir. Hatta bu olay için "*Amerikan diplomasisinin 11 Eylül'ü*" yakıştırması dahi yapılmıştır. Aslında bu belgeler ABD gibi küresel bir güç yerine, daha küçük bir devlette ortaya çıksaydı toparlanması pek kolay olmazdı. Ama ABD yöneticileri, saklayamadıkları bu

---

242 BBC, "Çin'de İnternet Denetimi İçin Yeni Kurum", http://www.bbc.co.uk/turkce/haberler/2011/05/110504_china_censor.shtml, (e.t. 22.10.2012).

243 KARA, BAHŞİ, loc.cit.

244 Ibid.

245 Ibid.

sırlar, mücadelede kaybettikleri bu siber saldırılar karşısında, tüm dünyaya "*af edersiniz*" (sorry) diyerek geçiştirmiştir.[246]

CNN'in 18 Mayıs tarihli haberinde[247]; İspanya'da "*Hemen Gerçek Demokrasi*" adlı sivil toplum örgütünün internet üzerinden yaptığı çağrı sonucu halk gösterileri olmuştur. Madrid ve Barcelona başta olmak üzere İspanya'nın birçok büyük kentinde meydanlarda toplanan halk, ülkedeki ekonomik, siyasi ve sosyal sistemin "*demokratik olmadığını*" savunarak, değişim istemini sürdürmüştür. Çoğunluğunu gençlerin oluşturduğu göstericiler tamamen internet ortamındaki sosyal paylaşım sitelerinde yapılan çağrılar sonrasında bir araya gelirken en büyük katılım başkent Madrid'de gerçekleşmiştir.

Mısır'da eski Cumhurbaşkanı Hüsnü Mübarek karşıtı gösterilerin başlatılmasında önemli payı bulunan internet eylemcileri ile ilgili verdiği haber sosyal medya adına ilgi çekicidir. Ayrıca, Google şirketinin Mısır'daki halk ayaklanmasının sembolü haline gelen çalışanı Vail Gonim ve blog yazarı Amr Selam, demokrasi yanlısı bir internet sitesinde, "*Silahlı Kuvvetler Yüksek Konseyi ile Randevu*" başlıklı yazılarında, "*görüş açılarını anlamak ve kendilerininkini anlatmak için komutanlarla bir araya geldiklerini*" belirttiler. Bu haberler siber uzayda sosyal medyanın ne kadar etkili olabileceği halk kitlelerini harekete geçirme adına neler yapılabileceğinin en güzel örneklerini ve Bilgi Çağı'nın en büyük nimetleri olarak yaşamaktayız. [248]

10. ABD'NİN SİBER GÜVENLİK ÖNLEMLERİ TEŞKİLATLANMASI

Çağımıza damgasını vuran teknolojik buluşlar, özellikle bilgisayar alanında inanılmaz boyutlara ulaşmıştır. Bilgisayar teknolojisini bütün birimlerine yerleştiren Amerikan Ordusu, klasik savaş anlayışını kökünden değiştirmiştir. Amerikan Savunma Bakanlığı (Pentagon), yeni Bilgi Harbi teknolojisinden yararlanarak düşmanın haberleşme, komuta kontrol merkezlerini, askeri, sosyal, ekonomik sistemini tek bir kurşun sıkmadan, belki de kan akıtmadan, işlemez hale getirme planları yapmaktadır.

25 Kasım 2002 tarihinde ABD Başkanı Bush, Yurt Güvenliği Bölümü'nün (Department of Homeland Security, DHS) oluşturulması kararını imzalamıştır. Yeni bölüm 22

---

246 YAVUZ Celalettin, "Wikileaks'in Tunus'tan Mısır'a Domino Etkisi Ve Türkiye, Ortadoğu ve Afrika", 28 Ocak 2011, http://www.turksam.org/tr/a2313.html, (e.t. 08.01.2012).

247 http://www.sondakika.web.tr/263093/internetten-dogan-guc-ispanya-yi-salliyor.html. (e.t. 08.01.2012).

248 Anadolu Ajansı (AA), "Mısır - Siber Militanlar: Ordu İle Demokratik Reformları Görüştük", www.aa.com.tr, (e.t. 24.01.2012).

kabine seviyesinde alt unsurlardan oluşmakta ve amaçları arasında siber güvenlikte bulunmaktadır. Bu sorumluluklar şunlardır;[249]

1. "*ABD alt yapısı ve kritik temel kaynakları korumak için kapsamlı bir ulusal plan geliştirmek.*
2. *Kritik bilgi sistemlerine yapılacak saldırılara karşı kriz yönetimi sağlanması.*
3. *Özel sektör ve diğer kamu kuruluşlarına, kritik bilgi sistemlerinin yok olmasına karşı geri kazanım veya kurtarma planları yönünde teknik yardım sağlanması.*
4. *Diğer yetkili kamu kuruluşlarına, yerel unsurlara, sivil toplum kuruluşlarına, özel sektöre, akademi çevresine uyarı ve bilgi sağlama noktasında, uygun koruma tedbirleri ve karşı tedbirleri sağlamak.*
5. *Araştırmaları desteklemek ve diğer kurumlar ile çalışmak, yeni bilimsel ve teknolojik kazanımların sistemi iyileştirmesini sağlamaktır*."

Aynı belge içerisinde "*Güvenli Siber Uzay Stratejisi*" [250] içerisinde 5 ulusal öncelik belirlenmiştir.

1. "*Ulusal Siber Güvenlik Yanıt Sistemi*
2. *Ulusal Siber Güvenlik Tehdit ve Güvenlik Açığı Azaltma Programı*
3. *Ulusal Siber Güvenlik Farkındalık ve Eğitim Programı*
4. *Kamu Kurumlarının Siber Güvenliği*
5. *Ulusal Güvenlik ve Uluslararası Siber Güvenlik Koordinasyonu*"

Bazı devletler siber saldırılara karşı nasıl davranacaklarını müşterek bir çalışma ile ve belli başlı hedefler belirlemek suretiyle çözme yöntemine gitmektedirler. Amerikan Adalet Bakanlığı'nın bu anlamda belirlediği prensipler şunlardır; [251]

1. "*Devletlerin siber hassasiyet ve tehdit ile ilgili acil uyarı ağları olmalıdır.*
2. *Devletler, kritik bilgi altyapılarının niteliğini ve kapsamını paylaşan ülkelerin bilinçlendirilmesini arttırmalı ve her bir ülkenin rolü bu kritik bilgi altyapılarının niteliğini korumak olmalıdır.*

---

249 Ibid.
250 Ibid., p. X.
251 G8 Principles for Protecting Critical Information Infrastructures (Adopted by the G8 Justice & Interior Ministers, May 2003), http://www.justice.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf, (e.t. 14.05.2011).

3. Devletler birbirlerinin alt yapılarını, kendi aralarında ki bağımlılığı belirlemek için incelemeli, bu sayede de bu tür alt yapıların korunmasını arttırılmış olacaklardır.

4. Devletler siber saldırıları önlemek, araştırmak ve bu tür kritik alt yapılara saldırı veya zararlara yanıt vermek için, kendi içinde hem kamu sektörü hem de özel sektörde bilgi paylaşımlarını teşvik etmelidir.

5. Devletler, kriz anında kullanmak için iletişim ağlarını oluşturmalı ve bu ağları korumalı, acil durumlarda güvenli ve hazır olacaklarına emin olmak için bu sistemlerini test etmelidirler.

6. Devletler, veri kullanılabilirliği politikalarının kritik bilgi altyapılarının korunmaya ihtiyaç duyacaklarını dikkate alındığından emin olmalıdırlar.

7. Devletler, kritik bilgi altyapılarına saldırıların takibi noktasında birbirlerine kolaylaştırıcı ve yardımcı olmalı, tam zamanında ve yerinde bu bilgileri diğer ülkelere vermelidirler.

8. Devletler tepki yeteneklerini geliştirmek için alıştırmalar ve eğitimler yapmalıdır. Süreklilik gerektiren ve acil durum planlarını, bilgi alt yapısı saldırı durumunda test etmeli ve diğer ortak ülkeleri de benzer faaliyetleri yapmaya teşvik etmelidir.

9. Devletler, 23 Kasım 2001 tarihli Avrupa Konseyi Siber Suç Sözleşmesi'nde belirtildiği gibi yeterli maddi ve usul yasalarına sahip olduğundan emin olmalı ve personelini kritik bilgi alt yapılarına saldırıları araştırmak ve yargılamak konusunda eğitmeli, bu araştırmaları ve yargılamaları diğer uygun ülkelerle koordine etmelidir.

10. Devletler kritik bilgi alt yapılarını koruma, acil bilgi sistemlerini geliştirme ve koordine etme, tehditleri, açık noktaları ve olayları çözümleme ve paylaşma, bu tür saldırıları yasalara uygun olarak araştırmayı koordine etmek noktasında uluslar arası işbirliği içinde olmalıdır."

Diğer bir değişle bilgisayar teknolojisinin sağladığı bütün olanakları kullanan Amerikan ordusu, her hangi bir savaşı sadece video ekran, klavye ve fare (mouse) ile kazanmayı hedeflemektedir. Pentagon yetkilileri, bilgisayar savaşlarının en büyük zaafının, kendi sistemlerinin de başka ülkeler tarafından yok edilebilmesi ihtimali olduğunu belirtmektedirler.[252]

ABD'de bilgisayarların, iletişim şebekelerinin ve veri tabanlarının, askeri çıkarlar için kullanılması esasına dayanan bilgi harbi üzerine artan bir şekilde çekilen dikkatlerin, başlıca iki

---

[252] WALLER Douglas, "Onward Cyber Soldiers", **TIME**, 21 Ağustos 1995, http://www.time.com/time/magazine/article/0,9171,983318,00.html, (e.t. 24.01.2012).

sebebi bulunduğu düşünülmektedir. Birincisi; Birleşik Devletlerin Bilgi Harbi taarruzlarından kendi bilgi sistemlerinin alacağı tahribat derecesinin tespiti, ikincisi ise bilgi teknolojilerinin temin edeceği öngörülen yeni sistemler için yeni askeri stratejilerin geliştirilmesi fırsatlarının ortaya çıkaracağı hususlardır. Bu konudaki çeşitli sorular, senaryolar, tarihsel deneyimler ve güncel konular göz önüne alındığında bilgi harbine karşı savunmanın zorluğu yanında, caydırıcılık için etkili bir planın ortaya çıkarılmasının da çok zor olduğu düşünülmektedir.[253]

Bütün bunların ötesinde en büyük mücadelenin, stratejik düşünme ile ilgili gelişmekte olan bilgilerin, devlet sırrı ve açık demokrasi gerçeği ile bağdaştırılması alanında olacağıdır. Geçmiş elli yıl içinde en iyi geliştirilen teorilerin hepsi, klasik ve nükleer caydırıcılık konusunda toplanmış ve Yıldız Savaşları'na kadar gelinmiştir. 1947 yılında nükleer taarruza karşı savunmanın zorluğu nedeni ile nükleer taarruzu durduracak stratejinin misli ile mukabele olması düşünülerek, caydırıcılık temini öngörülmüştür. Ne yazık ki günümüzde Bilgi Harbi'ne karşı savunmanın güçlüğü eski stratejilere göre iki kat daha fazladır. Bilgi Harbi savunmasının güçlüğü yanında caydırıcılık için etkili bir planın ortaya çıkarılması da oldukça güç olacaktır. Caydırıcılıkta en büyük güçlüklerden biri de Bilgi Harbi tehdidinde taarruz edenin belirsiz olabilmesidir.

Devletler, ulusal ve uluslararası araştırma ve geliştirmeleri teşvik etmeli ve uluslararası standartlara uygun sertifikalı güvenlik teknolojilerinin kullanılmasını zorunlu kılmalıdır. Amerikan hükümeti *"Amerika'nın Sesi*" internet sayfasında Amerika'nın Siber Uzay Stratejisi açıklanmıştır. "*Amerikan hükümeti interneti daha açık, güvenli ve güvenilir hale getirmek amacıyla yeni bir strateji hazırladı..."* "*Uluslararası Siber Uzay Stratejisi*" adlı girişime önsöz yazan Başkan Barack Obama, siber güvenliğin devletler ve toplumlar tarafından gönüllü üstlenilmesi gereken bir yükümlülük olduğunu, bu şekilde yeniliklerin artacağını, piyasaların yönlendirilebileceğini ve yaşam kalitesinin yükseleceğini belirtmiştir. Obama, Amerika'nın ilk kez internet güvenliği konusunda böyle bir yaklaşım benimsediğini, uluslararası ortaklarla birlikte sorumluluk aldığını kaydetmiştir. Yeni siber uzay stratejisi, internet kapasitesinin arttırılması, internet yönetiminin geliştirilmesi, siber ağların saldırılardan korunması için askeri işbirliğinin teşvik edilmesi gibi öncelikler içermektedir. Yeni strateji ayrıca internette temel özgürlüklerin ve özel hayatın korunması çağrısında da bulunmuştur. Amerika'nın yeni internet stratejisi, Dışişleri Bakanı Hillary Clinton ve üst düzey hükümet üyeleri tarafından açıklanmıştır. Clinton, internetin geleceği için ortak bir

[253] The White House , op.cit., p.ix.

vizyon çevresinde küresel bir görüş birliği oluşturulmasının önemini vurgulamıştır. Dışişleri Bakanı Clinton, bu şekilde internetin, halkların sosyal, ekonomik ve siyasi arzularını bastırmaktan çok hizmet etmeye yarayacağını söylemiştir.[254]

31 Mayıs 2011 tarihinde Pentagon, ABD'ye internet üzerinden saldırı düzenlenmesi durumunda askeri tedbirler de dahil tüm seçeneklerin değerlendirileceğini bildirmiştir. Amerika Savunma Bakanlığı sözcüsü Albay David Lapan, siber saldırılara aynı yoldan misilleme yapmak zorunda olmadıklarını açıklamıştır. Albay Lapan internet üzerinden düzenlenen her saldırıya Amerika'nın her türlü yanıt hakkına sahip olduğunu belirtmiştir. Pentagon, bilgisayar sistemlerini hedef alan olası saldırılara karşı yapılacak misillemeler konusunda ki kararını açıklamıştır. Bu açıklamalarda Pentagon sözcüsü Lapan, belli saldırıya karşı belli misillemeler yapılacağı şeklinde bir liste içermeyeceğini kaydetmiştir. [255]

[254] http://www.voanews.com/turkish/news/Amerikan-Hukumetinden-Yeni-internet-Stratejisi-121969104.html, (e.t. 15.01.2012).

[255] http://www.voanews.com/turkish/news/Washingtondan-Sanal-Saldirilara-Karsi-Silahli-Misilleme-Uyarisi-122917363.html, (e.t. 15.01.2012).

ÜÇÜNCÜ BÖLÜM

SİBER UZAY GÜVENLİĞİNİN ULUSLARARASI GÜVENLİĞE VE TÜRKİYE'YE ETKİLERİ

21. yüzyılın en önemli güç kaynağı hiç şüphesiz 'bilgi'dir. Bilgiyi elinde tutan gücü de elinde tutmuş olmaktadır. Bilginin gücüyle teknolojik alandaki gelişmeler tüm yaşamımızı olumlu yönde etkiliyor. İnternet, bilgisayar, uydular, cep telefonları vs. bunlar sadece günlük yaşamımıza giren teknolojinin ürünlerinden bazıları. Yine bilginin gücünü kullanarak aynı araçlar birer silaha dönüşebilmekte ve karşımıza siber savaş ve siber terör kavramları çıkmaktadır.[256]

DARPA (Amerikan Savunma Bakanlığı İleri Araştırmalar Merkezi) projesi olarak, 1966 yılında olası bir nükleer savaş sonrası askeri birliklerin haberleşmesi amacıyla oluşturuldu. Daha sonra üniversiteler ve günümüz de tüm dünyada kullanıma sunulan, ağlar arası ağ projesi internet ilk çıkış amacına adeta geri bildirimde bulunurcasına, saldırı ve savunma amacıyla kullanılır hale geldi.[257]

Günümüzde, bilgisayarların giremediği kamu ve özel sektör kurumu kalmadı. Askeri tesisler, kamu kaynakları, ülkelerin en önemli yönetim merkezleri hep bilgisayarlar ile bağlıdır. İnternetten gelecek saldırılar karşısında, savunma yapabilmek için, ağda dolaşan verilerin içeriğiyle saldırıları sezmek ve önlemek mümkündür. [258]

2009 yılı sonu itibariyle ABD Gizli Servisi ülke genelinde ve Roma'da olmak üzere toplam 28 "*Elektronik Suçlarla Mücadele Birimi*" oluşturmuştur.[259] Başta ABD olmak üzere, birçok ülke siber güvenlik konusundaki yapılaşmasını sadece ülke içerisinde değil, uluslararası alana da taşıyarak çok yönlü bilgi paylaşımı şeklinde yapmaktadır. Özellikle siber suç örnekleri tehdidin sadece tek taraflı olmayacağı, çok kapsamlı düşünülmesi ve özellikle diğer devletler ile bu konularda bilgi paylaşımının çok önemli olduğu gerçeğini ortaya çıkarmıştır.

---

256 ÖRGÜN Faruk, **Küresel Terör**, Okumuş Adam Yayınları, İstanbul, 2001, s.34.

257 CEYLAN Cenk, "İnterneti Durdurmak için Siber Savaş Aracı olarak DDoS Saldırıları", Turkish Forensic, 23.08.2011. http://www.bilgiguvenligi.gov.tr, (e.t. 03.01.2012).

258 Ibid.

259 Unites States Secret Service, Fiscal Year, 2009, **Annual Report**, p.38.

Kasım 2001 de Asya Pasifik Ekonomik İşbirliği Topluluğu üyesi 30 devlet, Avrupa Siber Suç Sözleşmesini imzalamıştır. Bu sözleşme siber suçlarla mücadele konusunda o zamana kadar hazırlanmış en kapsamlı ve çok taraflı bir sözleşme olma özelliğindedir. Üye devletlere ekonomik alt yapılarını bu sözleşmedeki en alt seviyedeki yasal yapılanmalar ile korumaları ve uluslar arası iş birliği içinde olunması gerektiği tavsiye edilmiştir.[260] Sözleşmenin detaylarında devletlerin özellikle yasal ve politik yapılanmalar ile sözleşmenin gereklerini en kısa sürede yerine getirmesinin önemli olduğu vurgulanmıştır.

Siber uzayın genişliği düşünüldüğünde saldırıların her yerden gelebileceği unutulmamalıdır. Bu sebeple özel ve kamu sektörünün, devletlerin bu anlamdaki güvenlik yapılanmalarının ve uluslararası yapılanmaların, sürekli bilgi paylaşımında bulunması suçluların en kısa sürede yakalanması konusunda önemlidir. Siber uzay her an canlı bir yapı olması sebebiyle güvenliğin ve kontrolün bir an bile bırakılmaması gerekmektedir.

Siber uzay kullanıcılarının da bu alanda gezinirken uyması gereken kurallar olacaktır. Siber uzayın kuralları, siber uzayın faydalarının yanında ne gibi sorumluluklar da getirdiği, olası yanlış kullanımdan doğabilecek sorumluluklar konularında bilgilendirilmeleri gerekecektir.

Bilgisayar ve bilgi teknolojilerindeki inanılmaz gelişme beraberinde e-ticaret, e-devlet, e-finans gibi birçok alanda kendini göstermiştir. Bu inanılmaz genişleme ve özellikle ekonomik faaliyetler üzerindeki büyük potansiyel, siber güvenlik ve bu anlamda oluşabilecek suçlara karşı ülkelerin iş birliği içinde çalışmasını zorunlu kılmaktadır.[261]

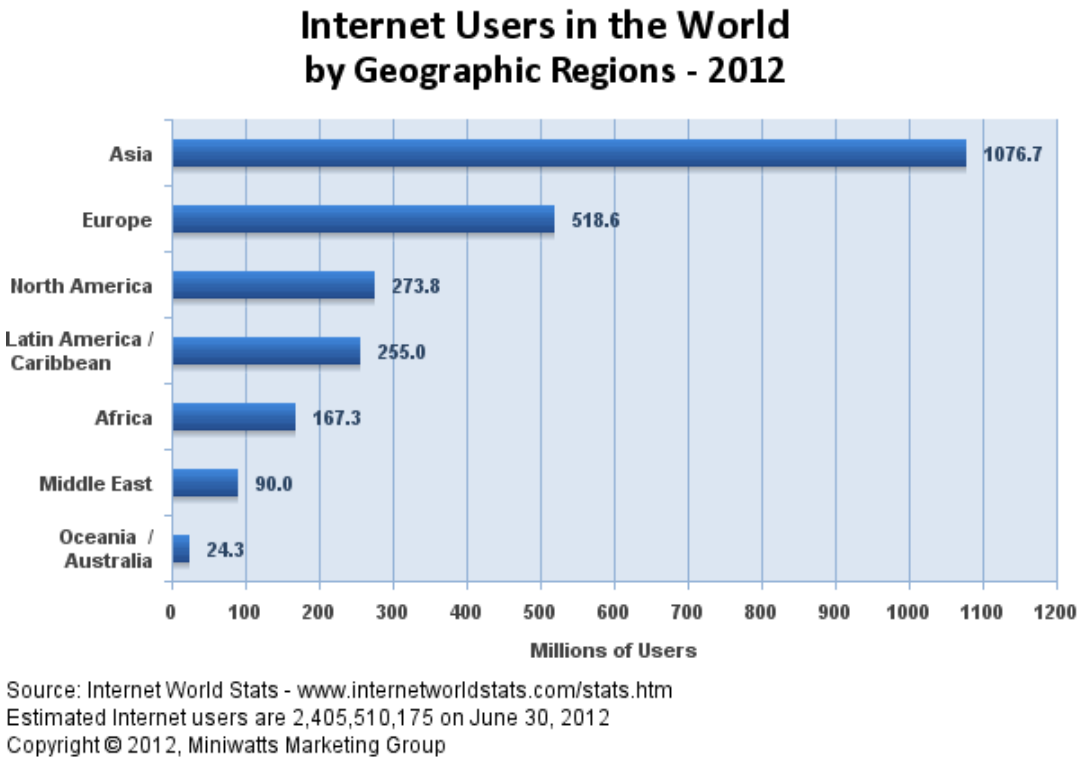
30 Haziran 2012 itibariyle dünyada yaklaşık 2,5 milyar internet kullanıcısı bulunmaktadır. Dünya nüfusunun yaklaşık % 34'ü internete erişim sağlayabilmektedir. Son 12 yılda internet kullanımı % 600 artmıştır. Türkiye'deki internet kullanıcı sayısı da her geçen gün artmış ve 2010 yılı itibariyle yaklaşık 35 milyona ulaşmıştır. Türkiye nüfusunun yaklaşık % 45'ine karşılık gelmektedir. [262]

---

260 **APEC Cyber Security Strategy**, "APEC Telecommunications and Information Working Group 26th Meeting", 19-23 Ağustos 2002, Moskova, Rusya, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan012298.pdf, (e.t. 22.04.2011).

261 Ibid.

262 http://www.internetworldstats.com/eu/tr.htm, (e.t. 23.10.2012).



Şekil 5: 2012 İnternet Kullanıcıları Sayıları (Milyon)

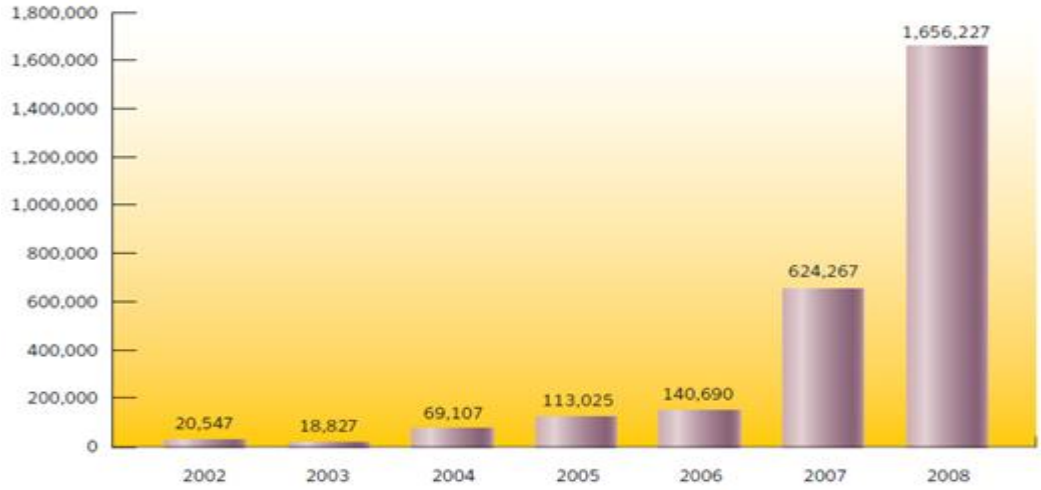
Kaynak: http://www.internetworldstats.com/stats.htm (e.t. 23.10.2012)

Bilgi devrimi ile beraber gelişen küreselleşme uluslararası siber suçları doğurmaktadır. ABD Gizli Servisi özellikle finans sektörüne ve önemli alt yapılara yönelik siber saldırılara karşı çalışmalarına ağırlık verdiğini belirtmektedir. Gizli Servis bu suçlara karşı kendi personelini siber suçlara yönelik özel eğitim programlarına almaktadır. ABD Gizli Servisi Temmuz 2005'te bir siber suç örgütünü takibe aldı ve araştırmalar sonucu örgütün 40 milyondan fazla kredi ve banka kartı bilgisini ele geçirdiğini tespit etmiştir. Örgütün ABD, Estonya, Belarus ve Çin Halk Cumhuriyeti'ne mensup kişilerden oluşan uluslararası bir örgüt olduğu ortaya çıkmıştır. Üç yıllık bir çalışma ile örgüt mensuplarının bilgileri kablosuz internet ağlarına yükledikleri casus yazılımlar ile elde ettikleri anlaşılmıştır. Ocak 2009'da bu kişiler ABD Gizli Servisi tarafından yakalanmıştır. [263]

Diğer bir istatistik de Symantec firması tarafından 2009 yılı ortalarında yayınlanan Güvenlik Tehdit Raporu'nda yer almaktadır. Şekil 6'da gösterilen veriler 2002 yılından bu

263 Unites States Secret Service, op.cit., p.35.

yana tespit edilen zararlı yazılım tehditlerini yıllara göre ortaya koymaktadır. Özellikle son iki yılda ciddi oranda yükselen zararlı yazılım tehdidi 2008 yılında 2002 yılına göre yaklaşık 80 katına çıkmıştır. [264]



Şekil 6. Symantec firması tarafından yıllara göre tespit edilen zararlı yazılımlar

Kaynak: Symantec Security Technology and Response, Symantec Global Internet Security Threat Report Trends for 2008 (2009).

Açık Güvenlik Kuruluşu DataLossDBson yıllarda tespit edilen veri kaçağı vakaları hakkında detaylı bilgiler sunmaktadır. Bu veritabanında yer alan "*Heartland Ödeme Sistemi*" örneği günümüze kadar yaşanmış en büyük veri kaçağı vakası olarak bilinmektedir. 2009 yılı başlarında meydana gelen olayda saldırganlar ABD çapında en büyük 5. kredi kartı ödeme firması olan Heartland'ın sistemlerine girmeyi başarmışlar ve yaklaşık 130.000.000 kullanıcının kredi kartı bilgilerini elde etmişlerdir. Firmanın Finansal İşler Başkanı Robert Baldwin yaptığı açıklamada saldırganların haftalarca sistemlere bağlı kalmayı başardıklarını ve bu süre içerisinde gerçekleştirilen tüm finansal işlemlerin kayıtlarını elde ettiklerini itiraf etmiştir. Analistler ifşa olan kredi kartlarının yenileri ile değiştirilme durumunda oluşacak mali kaybın, yükümlülüklerden dolayı ödenecek cezalardan fazla olacağı tespitinde bulunmuşlardır. [265]

---

[264] Symantec Security Technology and Response, **Symantec Global Internet Security Threat Report Trends for 2008 (2009)**.

[265] http://datalossdb.org/statistics, (e.t. 13.02.2012).

BM internetin "*temel bir insan hakkı*" olduğunu açıklamıştır. Örgütün İnsan Hakları Konseyi tarafından yayınlanan son raporunda, internet bağlantısının korunmasının özellikle bir ülkede gerçekleşen siyasi karışıklıklar süresince önemli olduğuna dikkat çekilmiştir. Konseyin raportörü Frank La Rue, "*İnternet erişimini ülkedeki her birey için mümkün olan en az miktarda kısıtlama gerçekleştirerek sağlamak her hükümetin önceliği olmalıdır. İnternet bireylerin anında bilgi alışverişinde bulunmasını, bilginin dağıtımını, organize olmayı ve dünyayı bir ülkede yaşanabilecek olası adaletsizlik ve eşitsizliklerden haberdar etmeyi sağlar.*" diye ekleyerek internetin önemine vurgu yapmıştır. Birçok ülkede internetin filtre koyularak engellendiği hatırlatılarak BM tarafından hükümetler "*internet bağlantısını engelleyecek bir yasa oluşturmamaları*" konusunda uyarılmıştır. [266] İnternetin uluslararası bir ağ olarak tüm dünyada etkisini kanıtlaması, onun devletler nezdinde daha ciddi olarak önemsenmesine sebep olmuştur.

Gelecekte BM örgütünün en önemli konuları arasında devletlerin internet yasakları olacağını öngörmek yanlış olmayacaktır. Devletlere internet konusunda tavsiyelerde bulunan örgüt, internet erişim yasaklarının artması ile birlikte baskılarını arttıracaktır. Yasakçı devletlere karşı uluslararası bir müdahale nasıl olacak? Şekil ve yöntem olarak neler benimsenecek? Bu müdahale şekilleri sanal mı olacak yoksa çok daha sert bir fiziksel yöntem mi tercih edilecek? Bütün bu sorularımızın yanıtlarını zaman gösterecektir.

Çalışmamızın üçüncü ve son bölümünde siber uzay güvenliğinin uluslararası güvenliğe ve Türkiye'ye olan etkileri üzerinde durulmuştur. Siber uzayda özellikle uluslararası güvenliği etkileyen siber terör üzerinde detaylı anlatımda bulunulmuştur. Çalışmamı son olarak, Türkiye'nin siber güvenlik alanındaki mevcut durumu ve TSK'nin siber uzay güvenliği alanında gelecek için yapılanmasına örnek oluşturması için Siber Kuvvet Komutanlığı yapılanması anlatılarak sonuçlandırılmıştır.

---

266 http://gundem.milliyet.com.tr/bm-internet-temel-bir-insan hakki/gundem/gundemdetay/06.06.2011/1398967/default.htm, (e.t. 06.02.2012).

1. SİBER TERÖR

"*Siber terörizm çok kullanılan bir terim olmasına rağmen bu terime çok geniş anlamlar yüklenmektedir. Çeşitli sayıdaki benzer kavramlar arasındaki farkı ortaya koyabilmek amacıyla biri yatay, diğeri dikey iki eksen ile dörde bölünmüş iki boyutlu bir düzlem düşünün. Yatay eksen, iyiden kötüye kadar gitmekte ve kullanıcının niyetini göstermektedir. Dikey eksen de bireyselden gruba kadar uzanmakta ve söz konusu kullanıcıların sayısını göstermektedir. Bu yöntemle geliştirilen dört kategori, dört farklı varlığı göstermektedir."* [267]

Birinci kategoride iyi niyetli bireysel kullanıcılar yer almaktadır. Bu bölümün kullanıcıları, yanlış bir biçimde bilgisayar korsanı (hacker) olarak adlandırılmaktadır. Bilgisayar korsanı terimi esasen belirgin ölçüde bilgisayar bilgisini vurgulamakta ve kötü niyeti kapsamamaktadır. Çağdaş dilde dahi (geeks) şeklinde de adlandırılmaktadır. Bilgisayar dâhisi sözcüğü teknoloji düşkünü, "*garip veya acayip kişi*", özellikle aşırı derecede entelektüel kişi şeklinde tanımlanmaktadır.[268]

İkinci kategoride ise iyi niyetli kullanıcı grupları yer almaktadır. Bunlar, ağ ve vatandaş sözcüklerinden oluşan "*ağdaşlar*" (netizen) olarak anıldıkları gibi "*akıl takımı*" (smart mobs) olarak da adlandırılmaktadır. Bu kullanıcılar, grubun amaçlarına ulaşılabilmesi için bir ağ üzerinden paylaşılan teknoloji ve bilgiyi kullanmaktadırlar. Sorun, kötü niyetli kullanıcılardan kaynaklanmaktadır. Kötü niyetli kullanıcı grupları, siber savaşçılar (cyber warriors) şeklinde tanımlanmaktadır. Bunlar, hükümet veya hükümet dışı varlıklar tarafından desteklenebilir. Her iki şekilde de, bu insanlar örgütsel hedeflere ulaşmak amacıyla ağ teknolojisini kötüye kullanmaktadır. Son kategoride de kötü niyetli kullanıcılar yer almaktadır. Bu kullanıcılar önceleri, bilgisayar korsanından çok şifre kırıcı (cracker) şeklinde adlandırılmaktaydılar Öte yandan, şahsi amaçları için değil de siyasi amaçları için yıkıcı faaliyetlerde bulunanlara ise siber terörist denilmektedir. Genel olarak siber terörist teriminin siber savaşçıları kapsaması gerekmektedir.[269]

Kötü niyetli kullanıcıların yürüttüğü faaliyetler ise, içeriklerine göre iki kategoriye ayrılmaktadır. ABD kaynaklı Rand Kurumu'ndan John Arquilla ve David Ronfeldt, ağ savaşı

---

267 TSUCHIYA Motohiro, "Siber Terörizm Tehdidi ve Önlemler", Küresel Terörizm ve Uluslararası İş Birliği, **II. Uluslararası Sempozyum Bildirileri**, Ankara, 10–11 Mart 2008, ss. 195–200.

268 Ibid.

269 Ibid.

ve siber savaş arasındaki farkı şu şekilde ortaya koymaktadır: "*Ağ savaşları toplumsal düzeyde fikirsel çatışmalardan meydana gelir ve hem devletler arası hem de toplumlar arası olabilir. Hedef kitlenin bildiklerini, halkın veya elitlerin yahut her ikisinin de görüşlerini hedef alarak, alt üst etmeyi ya da değiştirmeyi amaçlamaktadır. Basit bir şekilde ifade etmek gerekirse, ağ savaşlarının hedefi insanların kafalarını karıştırmaktır. Bunun aksine, siber savaş, askeri harekâtların bilgi tabanlı ilkelere göre yürütülmesidir. Açıkçası, bu savaş, bilgi ve muhabere sistemlerinin fiziksel olarak bozulmasıyla varlık göstermektedir.*"[270]

Siber terörizm, siber suç ve bilgi savaşı ile karıştırılabilir. Fakat bilgi savaşı ve siber terörizm arasında büyük bir fark vardır. Siber terörizm kasıtlı, çoğu zaman siyasi amaçlar ile beslenebilen, ulusal gruplar ve gizli ajanların veya bireysel olarak, bilgi sistemlerine, bilgisayar programlarına, verilere, silahsız hedeflere karşı şiddetle sonuçlanan eylemdir. Fakat eski tabirle bilgi savaşları; devletler ve onların temsilcileri tarafından bilgi veya bilgisayar sistemlerine, bilgisayar programlarına, verilere karşı yapılan düşman kaybı ile sonuçlanan planlı bir saldırıdır.[271]

Siber terörizm terör örgütlerinin internet aracılığıyla saldırı yapması veya terör örgütlerinin bir yayın organı gibi faaliyet gösteren internet sitelerinin var olması anlamlarına gelmemektedir. Bu durum daha çok bilişim suçlarının kapsamına girmektedir. Siber terörizm terörist grupların konvansiyonel eylem biçimi olarak gördükleri bombalama, güvenlik güçlerine saldırı, intihar saldırısı gibi eylem biçimlerinin dışında yeni bir eylem biçimidir. Saldırılarda hedef diğer eylem türlerinde olduğu gibi devlet, güvenlik kurumları ve toplumdur. Fakat şu ana kadar siber terör eylemlerinin hedefi daha çok devlet kurumları olmuştur. Siber terör saldırılarında devlet kurumlarının internet sitelerine yönelik saldırılar gerçekleştirilmektedir. Bu saldırıların ülkemiz için en önemli örneği olarak 2012 Şubat ayında Redhack isimli grubun Ankara Emniyet Müdürlüğü internet sitesine yönelik gerçekleştirdiği siber saldırıyı gösterebiliriz.[272]

Siber terörizm konusunu daha iyi anlayabilmek için siber dünyanın sınırlarını incelemek yararlı olabilir. Siber dünya "*iletişim teknolojileri ağının ve bütün kapsamlı*

---

270 Ibid.

271 JANCZEWSKI L. J., A. M. COLARIK, **Cyber Warfare And Cyber Terrorism, Information Science Reference**, 2008, Aktaran Murat DOĞRUL, Adil ASLAN, Eyyüp ÇELİK, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism" , Turkish Air War College, Istanbul, Turkey, p.3.

272 BALCI Çağatay, "Türkiye'nin Yeni Güvenlik Sorunu: Siber Terörizm", http://afasam.org/tr/savunma-guvenlik/turkiyenin-yeni-guvenlik-sorunu-siber-terorizm/, (e.t. 23.10.2012).

bilgilerin bir bütünü" olarak tanımlanabilir. Bir başka deyişle, internetin en geniş ve ilgili parçası olduğu bilgisayar iletişim ağlarının bütünüdür. Siber boşluk teknolojiyi ve değerli bilgiyi elektronik olarak depolamak ve göndermek için kullanılır. Dünyadaki birçok "*kritik bilgi altyapıları*" kontrol ve diğer fonksiyonlar için bilgisayar sistemlerine bağımlıdır. Sözü edilen altyapılar ulaşım sistemlerinde, endüstri, bankacılık ve finans kuruluşlarında, enerji dağıtımında, sağlık hizmetleri vb. alanlarda yoğun bir şekilde kullanılmaktadır.

Sosyal sistemimiz bilgisayarlara ne kadar bağlı hale gelirse toplumumuz siber terör saldırılarına o kadar açık hale gelecektir. Sorun şu ki, bilgisayar ve ağlar, çoğumuz için hala bir kara kutudur. İç işleyişin anlaşılması gittikçe daha da zorlaşmaktadır. Bunun bir neticesi olarak bir saldırının gerçekleşeceğini bilememe tehlikesi ortaya çıkar. Ağın uzaktan kontrolü ile bir barajın yıkılması için yapılan saldırılar herkes tarafından bilinmektedir. Diğer taraftan, eğer, bilgilerde tahrifat yapmak ve kayıtları değiştirmek amacıyla bir bilgisayar veritabanına girilirse, saldırının zamanı ve faili bilinemeyebilir. Bu, siber terörizmin huzursuzluk yaratan zor bir konsept haline gelmesinin nedenidir.[273]

Dikkate alınması gereken bir diğer husus da teröristlerin en yeni teknolojiden gerektiği şekilde yararlanmadıklarıdır. 11 Eylül saldırılarını yapan teröristler, şifresiz düz bir metin şeklinde bir elektronik posta gönderdiler. Oysaki bir saldırı öncesinde amaçları ifşa edilmediği müddetçe, ihtiyaçlarını karşılamak için basit bir teknoloji yeterli gelebilmektedir. Sıradan gözüken metin ve grafikler içinde gizli mesajlar iletebilir veya Youtube gibi video paylaşım siteleri ile mesajlarını yayabilirler. Bu geniş çaplı bilgi selinde zararlı olanı olmayandan ayırmak büyük önem arz etmektedir. İnternet çoğunlukla; telefon sistemlerini, kablosuz ve uydu iletişimlerini de içeren ulusal ve uluslararası telekomünikasyon altyapısı üzerine kurulmuştur. Söz konusu altyapılar da az önce bahsettiğimiz alanlar gibi bilgisayar teknolojisine bağımlı durumdadırlar. Bu yüzden tanımımıza göre onlar da siber dünyanın bir parçasıdır. Şu an dünya çapında 1,5 milyardan fazla internet kullanıcısı vardır. İnternet 200'den fazla ülkede kullanılmaktadır. Ayrıca bu ülkelerin çoğunda siber güvenlik donanımı ya mevcut değil ya da yetersizdir.[274]

İnternetten daha hızlı yayılan tek iletişim vasıtası ise cep telefonudur. Bugün yaklaşık 3 milyar telefon kullanımdadır ve her gün 1,6 milyon kullanıcı bu sayıya eklenmektedir. Son

---

273 Ibid.
274 Ibid.

teknolojik gelişmelerin mobil telefonları doğal olarak internet için bir platform haline getirmesi, milyonlarca yeni kullanıcının bu kaynağa erişebilmesini sağlamaktadır.[275]

Terörist örgütlerin internet kullanımını incelediğimizde karşımıza gittikçe artan bir oran çıkmaktadır. Terörist gruplar interneti özellikle sınırlı denetim olanakları nedeniyle ideoloji yayma ve hızlı/örtülü iletişim kurma vasıtası olarak kullanmaktadır. Bu nedenle terörist internet sitelerinin sayısı son on yılda 12'den 5400'e (1998–2007) yükselerek ciddi bir tehdit oluşturmaya başlamıştır. Teröristler tarafından web sitelerinin kullanımına yönelik olarak verilebilecek en çarpıcı örneklerden biri PKK/KONGRA-GEL terör örgütünün web siteleridir. Bu örgüt ile ilişkili halen 37 web sitesi vardır.[276] Bu sitelerin içeriğinde terör örgütünün tarihi, etkili olan teröristlerin otobiyografisi, öldürülen teröristlerin bilgileri ve terör örgütünün siyasi mesajları bulunmaktadır. Sitelerin hedefinde kimlik temelli bölücülük oluşturmak vardır.[277]

Bugün hangi terör örgütlerinin amaçları için internetten yararlandığı sorulsa muhtemel cevap hepsi olur. Günümüzde hemen hemen bütün terörist örgütler interneti amaçları için kullanmaktadır. Siber terörizmi genel anlamda; insanlara, kaynaklara ve sistemlere zarar vermek amacıyla interneti kullanmak veya kısaca internet vasıtasıyla saldırı düzenlemek olarak tanımlayabiliriz. Ancak, tanım ile boğuşmak yerine internetin terörist amaçlar için kullanımının yolları hakkında genel bir değerlendirme yapmak daha yararlıdır. [278]

Terör örgütleri interneti dört temel amaçla kullanırlar. Bunlardan birincisi; aynen bizim günlük yaşantımızda yararlandığımız gibi kullanım, ikincisi; propaganda, istihbarat toplama ve eleman temini amaçlı yararlanma, üçüncüsü; ekonomik avantaj sağlamak için siber suç amaçlı kullanım, dördüncüsü ise yıkım, hedef kitlede korku yaratma ve siber terörizm amaçlı kullanım.[279]

Tarihte, siber terörizm olayına rastlamak neredeyse imkânsızdır. Bunun nedenleriyle ilgili iki farklı yaklaşım vardır. Birincisi; hükümetlerin yapılan siber terörizm saldırılarını toplumda oluşabilecek korku ve paniği önlemek için kamuoyu ile paylaşmadıkları düşüncesidir. Diğer bir yaklaşıma göre ise, şu ana kadar terörist örgütlerce politik

---

275 Ibid.

276 2011 yılı için tespit edilen rakamdır.

277 DOĞRUL Murat, Adil ASLAN, Eyyüp ÇELİK, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism" , **Turkish Air War College**, Istanbul, Turkey, p.5.

278 Ibid.

279 Ibid.

motivasyon, şiddet ya da panik ve hedef kitlede yaratılan korku gibi terörizmin kabul gören tanımı kapsamına giren herhangi bir siber terörizm olayı gerçekleşmemiştir.

Günümüzde endüstriyel tesisler, fabrikalar ve üretim sistemleri; kamu ve özel hizmetler; hastaneler, destek kuruluşları ve altyapılar; silah sistemleri, barajlar ve reaktörler vb. tesisler bilgisayar teknolojilerine bağımlı olduğundan siber terörizmin hedefi olabilir ve bu sistemlere yapılacak saldırılar toplu kayıplar ve ciddi zararlarla sonuçlanabilir. Siber saldırılar doğrudan yıkıcı sonuçlar yaratmak amacıyla yapılabilir ya da sıradan terörist saldırılarının yıkıcı sonuçlarını artırmayı ve acil durumlarda kurtarma eylemlerini engellemeyi amaçlayabilir.

İnternet, hem doğası gereği hem de avantajları nedeniyle birçok yönden terörist örgütlerin eylemleri için uygun bir ortam sağlamaktadır. İnternet aracılığıyla gerçekleştirilen saldırılar dünyanın herhangi bir yerinden başlatılabilir. Klasik bombalı eylemdeki gibi "*olay yerinde"* olmak gerekli değildir. Saldırıların başlatılması için gerekli olan internet bağlantılarına kolaylıkla erişilebilir ya da yeni nesil cep telefonları bu amaçlarla kullanılabilir.

Siber terörizm; siber uzay ve terörizmin birbirleri ile olan yakınsamasıdır. Genellikle bu tanımdan bilgisayarlara, iletişim ağlarına, bilginin saklandığı e-depolara karşı, siyasi ya da sosyal hedeflerine ulaşmak için yapılan yasadışı saldırılar anlaşılmaktadır. Ayrıca bir saldırıyı siber terörizm olarak nitelendirmek için kişi ya da mala karşı bir zararın veyahut en azından korkunun oluşması yeterli olacaktır. Bir kişinin ölümü, bedensel zarara sebep olan saldırılar, patlamalar, uçak kazaları, su kirliliği ya da ciddi bir ekonomik kayıp diğer siber terörizm örnekleridir. Kritik alt yapılara karşı yapılan saldırılar siber-terörizm olarak nitelendirilebilir.[280]

Herhangi bir konuda düzenleme veya kanun olmadığı zaman doğal olarak ihlal ve suç da oluşmaz. Yasal olarak siber saldırılar ile ilgili hala yeterli yasal düzenlemenin birçok ülkede yapılmamış olması siber saldırganların yakalanmasını zorlaştırmaktadır. Siber saldırıların çoğu zaman başka devletten gerçekleşmesi uluslararası bir yapının ve yasaların olmasını zorunlu kılmaktadır.

---

[280] DENNING D., "Cyber terrorism. Testimony before the Special Oversight Panel on Terrorism," **Committee on Armed Services U.S. House of Representatives**, Georgetown University, May 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (e.t. 10.08.2011).

İnternet kullanımı oldukça ucuzdur. Eylem için çoğu ülkede kolaylıkla temin edilebilecek küçük bir ağ bağlantısı yeterlidir. Ancak verilebilecek zararlar çok daha yüksek olabilir. Sistemlerin birçoğunda güvenlik önlemleri yetersiz kaldığından siber saldırıları düzenlemek oldukça kolaydır. Bu yüzden teröristlerin ilgisini çekebilecek oldukça fazla seçenek bulunabilir.[281]

Siber dünyanın hızı teröristler için oldukça caziptir ve eylemleri kolaylaştırıcı bir etki yaratmaktadır. Saldırının hızı sadece teröristin bağlantı hızına bağlı değildir. Konrol altına alınan bilgisayarların bağlantı hızı bu amaçla rahatlıkla sömürülebilmektedir. Böylece teröristin özel bir çaba göstermesine gerek kalmadan virüsler hızlı şekilde yayılmaktadır. Küresel ölçekte çok sayıda kullanıcısının olması, medya ortamı ve interaktif iletişim imkânları internetin terörist örgütlerce tercih edilmesine sebep olmaktadır.[282]

Her ne kadar bazı yetkililer gerçek anlamda bir siber terörizm saldırısının olmadığını söyleseler de, bazıları da teröristlerin çoktan siber dünya da üstünlüğü ele geçirdiğini iddia etmektedirler. Bu büyük fark "*terörizm*" ve "*siber terörizm*" tanımlamasındaki anlaşmazlıklardan kaynaklanmaktadır. Daha önce de belirttiğimiz gibi terörizm ve siber terörizmin evrensel olarak kabul edilmiş bir tanımı yoktur.[283]

Siber uzay ise sürekli saldırı altındadır. Siber casuslar, hırsızlar, sabotajcılar, heyecan arayanlar, bilgisayar sistemlerine girerek kişisel verileri, ticari sırları çalabilir, web sitelerine erişimi durdurabilir, bilgisayarlara virüs, solucan yerleştirebilir, hileli işlemler yapabilirler. Tüm bu işlemler ile bireyleri ve kurumları rahatsız edebilirler. Son günlerde bu saldırılar internet web sitesinden kolayca bulunabilecek, kullanımı basit, binlerce ücretsiz ve daha güçlü casus yazılımlar ile daha kolay olmuştur.[284]

Toplumlar bu yeni tip terörizme karşı çok hassastır. Çünkü günümüzün gelişmiş toplumu artık elektronik cihazlara daha bağımlı hale gelmiştir. Savunma, emniyet, bankacılık, ticaret, ulaştırma ve bilimsel çalışmaların yanında devlet ve özel sektörün büyük bir kısmı birbiriyle elektronik yolla irtibat halindedir. Bu da bilgisayar korsanları vasıtasıyla bu kuruluşları büyük tehlikelere maruz bırakmaktadır. Yakın bir dönemde; yapılabilecek bu tür

281 Ibid.
282 Ibid.
283 DOĞRUL, ASLAN, ÇELİK, op.cit., p.3.
284 Ibid.

sabotajların ülkelerin hayati fonksiyonlarını felç edecek nitelikte olacağı değerlendirilmektedir.[285]

Bazı istihbarat kaynaklı raporlara göre bu yoldan 20 yetenekli kişi ve 1 milyar dolarla ABD gibi bir süper gücün bile çökertilmesi mümkündür. Bu mümkünse, teröristlerin de bunu başarabilecek nitelikte olabileceği göz ardı edilmemelidir. Elektronik casuslar artık, kredi kartları, endüstriyel istihbarat ile ilgili belli hedeflere yönelmektedir. Terörist gruplar, muhataplarını zayıflatmak isterken, bunları uzun dönemde imha edemeyeceklerinin bilincindedir. Ayrıca unutulmamalıdır ki teröristlerinde bu tarz yöntemleri deneyecekleri muhakkaktır.[286]

Örnek vermek gerekirse ILOVEYOU virüsü milyonlarca kullanıcıyı etkilemiştir ve milyarlarca dolar zarar verdiği tahmin edilmektedir. Şubat 2000 yılında Yahoo, CNN, eBay ve diğer e-ticaret sitelerine yapılan saldırılar sonucu bu sitelere uzun zaman erişim sağlanamamıştır. Bunun karşılığında ilgili siteler büyük maddi kayıplar yanında sanal ticaret anlamında güven kaybına uğramıştır.[287]

Bu söylenenler ışığında siber terörizmle mücadele için ne yapılabilir? İlk olarak, akıl savaşını (head war) kazanmalıyız. Teröristler sadece fiziksel hedeflerle değil aynı zamanda zihinlerimize de saldırmaktadırlar. İnsan zihni soyuttur ancak bir kez zarar gördü mü iyileşmesi zordur. Uzun vadede, kalplere ve zihinlere karşı yapılan saldırılar fiziksel hedeflere yapılandan daha yıkıcı olabilir. Psikolojik ve sosyolojik öngörü, siber terörizmle mücadele için önemlidir. Toplumumuzu korumak için teröristlerin niyetleri ve örgütlenme şekillerini anlamalıyız.[288]

İkinci olarak, noktaları birleştirmeliyiz. Teröristler, ağlardan yararlandıkları için, tepkimiz aynı zamanda ağ ilkelerine göre olmalıdır. Ağda yayılmış bir vaziyette bulunan ipuçlarını bir araya getirmeli, birbiri ile irtibatlandırmalı ve önemlerini kavramalıyız. Teröristler, birçok yerde faaliyetlerinden iz bırakırlar.[289]

İnternet gibi elektronik ağlardan geçen veri akışı, gittikçe artan bir oranda devam edecektir. Bilgi iletişim teknolojilerindeki yeni gelişmeler artık ulusal güvenliği

---

285 ÖZEL Yücel, "Terörün Değişen Yapısı ve Asimetrik Harp İle İlişkisi", **Harp Akademileri Bülteni**, Kasım, 2003, s.51.

286 Ibid.

287 DENNING, loc.cit.

288 TSUCHIYA, loc.cit.

289 Ibid.

etkilemektedir. "*Bilgi toplumu*" sözcüğünü üreten Masuda, yeni bilgi iletişim teknolojisi ile rüyalarımızı gerçekleştirecek ve fikirlerimizi hayata geçirecek yeni fırsatlar elde edebileceğimizi öngörmüştür. Aynı şey teröristler için de söylenebilir. Toplumumuz, gitgide bilgisayar ağlarına bağımlı hale gelmektedir ve bu yolun geri dönüşünün olmadığını söyleyebiliriz. Bu yeni fırsatların, her zaman toplumumuz yararına gelişmelere kapı aralaması için savunma politikaları geliştirmeliyiz.

"*İnternet, küresel bir varoluştur*." Siber saldırılar kolaylıkla ulusal sınırların ötesine geçebilmektedir. Gizli bir şekilde bu saldırılar başlamıştır. Siber terörizmle mücadele için hükümetler, özel şirketler ve sivil toplumlar arasında küresel iş birliğinin gerektiği açıktır. Uluslararası Telekomünikasyon Birliği (International Telecommunication Union-ITU) bünyesinde düzenlenmiş olan Bilgi Toplumuna Yönelik Dünya Zirvesi (World Summit on the Information Society-WSIS), böyle çok-sektörlü iş birliği yaklaşımına örnek olarak verilebilir. Söz konusu zirve, küresel dijital bölünmeyle mücadele ve internet yönetişimi için daha iyi yöntemler bulmayı amaçlamıştır.[290] Bilgisayar dâhileri hükümetlere karşı çok dostça olmayabilirler ancak birbirleriyle küresel konular hakkında kolaylıkla iletişim kurabilmeleri arzu edilen bir durumdur. Çünkü onlar küresel olan internetin sağlığını her zaman önemsemektedirler. Daha önce belirtildiği gibi yeni iletişim teknolojileri kötü niyetli insanlara yardım edebilmektedir. Ancak bizler hayatımızı harikulade bir hale getiren ve küresel iletişimimizi kolaylaştıran bu teknolojilerden vazgeçmemeliyiz.

Botnetler son yıllarda siber ataklar başta olmak üzere geniş çaplı internet atakları için en yaygın kullanılan zararlı yazılımlardır. Bot kelimesi "*Robot*" kelimesinden türetilmiştir. Robot daha önceden planlanmış işleri yapan makinedir. Bu botların bir merkezden yönetilen büyük gruplarına botnet adı verilmektedir. Botnetler genellikle tek bir merkezden yönetilerek botların bir koordinasyon içerisinde belli amaçlar için yönlendirilmesinde kullanılırlar. Botnetler tarafından kontrol edilen bilgisayarlar botnet üyesi ya da köle bilgisayar (zombie) olarak adlandırılmaktadır. [291]

Teröristlerin siber uzayı tercih etmelerinde birçok sebep vardır. Siber saldırılar ile teröristler daha geniş bir alanda faaliyet gösterebilir. Fiziksel bir şiddet uygulamadan bir devlete daha fazla zarar verebilirler. Nüfusun büyük bir çoğunluğu sadece izleyici

---

290 Ibid.

291 KARA Mehmet, Necati E. ŞİŞECİ, "Botnetlerle Mücadelede Dünyadaki ve Türkiye'deki Durum", TÜBİTAK-UEKAE, http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/botnetlerle-mucadelede-dunyadaki-ve-turkiyedeki-durum.html, (e.t. 06.02.2012).

konumundadır ve terörist faaliyetlerden etkilenmez. Terörist faaliyetlerde medya ve halkın dikkati can ve mal kaybı olduğu için siber eylemlerin nedenleri o kadar da dikkat çekmez. Siyasi ve sosyal hedeflerini nüfusun büyük bir kısmına ulaştırma imkânını siber uzay teröristlere verdiği için, bu alan onlar için büyük bir fırsat olmuştur. [292]

Siber saldırıların teröristler için cazip olmasının birçok sebebi vardır. Bunlar;

1. "*Teröristler için siber saldırıların maliyeti çok düşüktür. Az bir maliyetle çok fazla insanı etkileyebilmektedirler. Başka bir değişle fayda-maliyet oranı son derece yüksektir.*

2. *Terörist faaliyetlerin yapılacağı yerlere uzak olma veya mekân kavramını ortadan kaldırabilme imkânını teröriste vermektedir. Siber güvenliğin zayıf olduğu bir devletten hedef devlete veya kuruma istediği saldırıları kolayca yapabilmektedir.*[293]

3. *Siber uzayda hedef olarak nitelendirilebilecek organların korunması son derece zayıf olduğundan, siber teröristler için geniş bir seçim yelpazesi sunmaktadır.*[294]

4. *Saldırı için fazla bir hazırlık süresine ihtiyaç duyulmaz.*[295]

5. *Siber uzayın girişinde, daha teknik bir tabirle internet ağına bağlanırken herhangi bir güvenlik kontrolü yapılmamaktadır. Bu yüzden herkese erişim hizmeti açıktır.*[296]

6. *Siber terörist için kendi bilgisayarı ve bağlantı hızı o kadar da önemli değildir. Ele geçirilen bilgisayarların ve ağlarının hızları daha etkili olabilmektedir.*[297]

7. *Siber terörizm ve somut olarak yapılan terörist eylemlerin birlikte oluşturduğu birleşim beklenenden büyük etki yaratmaktadır."*[298]

Teröristler bilgi teknolojisini ve interneti aşağıdaki sebeplerle kullanabilmektedirler.

---

[292] WARREN M. J., "Terrorism and the Internet," **Cyber Warfare And Cyber Terrorism, Information Science Reference**, 2008, pp.42-49.

[293] OBA T., "Cyberterrorism seen as future threat," **Computer Crime Research Centre Tech. Report**, April 2004, http://www.crime-research.org/news/2003/04/Mess0103.html , (e.t. 11.08.2011).

[294] BRUNST P.W., "Use of the Internet by terrorists, A threat analysis," **Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism**, Ankara, Turkey (Ed.) IOS Press, 2008, pp.34-60, http://libraryguides.waldenu.edu/crjs4303, (e.t. 11.08.2011).

[295] Ibid.

[296] SÜTALAN Z., "Current and future trends in terrorism," **COE-DAT Newsletter,** vol.3 issue.16, pp.37-49, July-September 2010.

[297] BRUNST P.W., loc.cit.

[298] CURRAN K., K. CONCANNON and S. MCKEEVER, "Cyber terrorism attacks cyber warfare and cyber terrorism," **Information Science Reference**, 2008, pp.1–6.

- *"Plan hazırlamak*
- *Para kaynaklarını arttırmak ve aklamak*
- *Propaganda yapmak*
- *Üyeler ile güvenli iletişim yapmak*[299]
- *Benzer gruplar ile bilgi ve tecrübe paylaşımı yapmak*[300]
- *Komuta ve kontrol* [301]
- *Araştırma ve geliştirme (ARGE) faaliyetleri yapmak*
- *Yeni üyeler kazanmak*
- *Uluslar arası destek sağlamak*
- *İstihbarat toplamak*
- *Bilgi savaşı yapmak*
- *Düzenleme yapmak*
- *Büyük kitlelere bilgi akışını sağlamak*"[302]

Botnet tehdidi 1999 yılında "*win32/prettypark*" zararlı yazılımı ile ilk defa yapılan dağınık servis dışı bırakma (DDoS) atağından beri bilinmektedir. 2007 yılının sonunda tüm güvenlik endüstrisi, botnetleri güvenlik listelerinin en önemli tehdidi olarak kabul etmiştir. İlk botnetler IRC (Internet Relay Chat) protokolünü kullanmışlardır. Daha sonra IRC protokolünün kolayca fark edilmesi ve önlenebilmesinden dolayı http, https, P2P gibi yeni haberleşme protokolü arayışlarına girmişlerdir.[303]

Botnetler çevrimiçi (online) bilgisayar sistemlerinin karşı karşıya olduğu en büyük tehdittir. Dağıtık bilgisayar sistemleri olan botnetler, finansal dolandırıcılık, siber ataklar, dağıtık servis dışı bırakma atakları (DDoS), istenmeyen e-posta gönderme, ajan yazılımlar,

---

299 Ibid.

300 ROGERS M. "The psychology of cyber-terrorism," **Terrorists, Victims and Society**, In A. Silke (ed.), Chichester:Wiley, 2003, pp.77-92.

301 SÜTALAN, loc.cit.

302 CURRAN, CONCANNON, MCKEEVER, loc.cit.

303 KARA, ŞİŞECİ, loc.cit.

yemleme (Phising) e-postaları, yazılımların yasal olmayan dağıtımı, bilgi ve bilgisayar kaynaklarının çalınması, kimlik hırsızlığı gibi birçok bilgisayar saldırısı için de kullanılabilirler.[304] "*Birkaç katmanlı C&C (Komuta Kontrol - Command&Control) merkezleri sayesinde değişik dillerdeki, ülkelerdeki, zaman dilimlerindeki, farklı yasalar altındaki bilgisayarları kontrol etmeyi sağlayan mekanizmalardır. Bu mekanizmalar botnetlerin izlerini sürmeyi zorlaştırdığı için onları bilişim suçları için çekici bir araç haline getirmektedir.*"[305]

Terör örgütleri ve işgale karşı direnenlerin örgütlendiği bir mecra olarak internet, günümüzde lojistik bir amaca hizmet edebilmektedir. Öyle ki, El-Kaide gibi terör örgütleri, haberleşmelerini internet üzerinden, kendi geliştirdikleri şifre algoritmalarıyla rahatlıkla yapabilmektedirler.[306]

Önceki nesil virüs ve kurtçuklarda olduğu gibi botnetler de kendi kendilerine açıklık içeren bilgisayarlara bulaşarak yayılan zararlı yazılımlardır. Buna karşın botnetleri diğerlerinden ayıran özellik C&C merkezi ile haberleşerek, kendilerini güncelleyebilmeleri ve yönetilebilmeleridir. Çok katmanlı komuta kontrol yapısı botnet yöneticilerini gizleyen yapılar sunmaktadır. Botnetler C&C merkezlerine göre IRC tabanlı, http tabanlı, P2P (Point To Point) tabanlı ve DNS tabanlı olmak üzere dört kategoride değerlendirilmektedir.[307]

Sonuç olarak, siber terörizmle mücadeleye bilgisayar dâhileri de dâhil edilmelidir. Bilgi ve becerileri olmaksızın siber terörizmle mücadele etmek mümkün olmayacaktır. Ancak, teröristlerin sahip oldukları imkân ve kabiliyetlerden daha fazlasını barındıran kaynaklar elde edilemez ise bu durum sadece hükümet sistemlerinin değil aynı zamanda sosyal sistemin zafiyetini artıracaktır.[308]

2. ULUSLARARASI İŞBİRLİĞİ

Son zamanlarda önem kazanan bir gelişme siber alanın gittikçe siyasallaşmasıdır. Bütün saldırıların siyasi amaçla yapıldığını ifade etmek zor olmakla beraber, gerçek olan husus kamusal ve özel aktörlerin siber alanın siyasal faaliyetleri için önemini gittikçe kavramaya başlamış olmalarıdır. Devlet dışı aktörlerin gösteri, yürüyüş, protesto, sivil

---

304 Ibid.
305 Ibid.
306 CEYLAN Cenk, "Savaş Cephesi Olarak, Sanal Ortamda Savunma ve Saldırı", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/savas-cephesi-olarak-sanal-ortamda-savunma-ve-saldiri.html?Itemid=6, (15.02.2012).
307 KARA, ŞİŞECİ, loc.cit.
308 Ibid.

direnme gibi geleneksel faaliyetlerini siber saldırılarla tamamladıkları, güçlendirdikleri görülmektedir. Egemen devletler için siber alan yeni eylem imkânları yarattığı gibi büyük bir zafiyet de oluşturmaktadır.[309]

Devletler açısından siber saldırılar, siyasi, ekonomik, sosyal amaçları doğrultusunda tespit edilen koordineli stratejilerin önemli bir parçasını teşkil etmeye başlamıştır. Böylece siber saldırılar, baskı, diplomatik eylemler, sosyal etkileşimlerden fiziki protestolara kadar şekillenen ve hedef ülkeyi etkilemeyi amaçlayan karma stratejilerin ayrılmaz parçası olmuştur. Bu çerçevede devletlerarası güç mücadelesi siber alanda gittikçe yoğunlaşan biçimde yaşanmaya başlanmıştır.

Siber Savaşı olası kılan üç boyut var;

1. "*İnternet'in tasarımında mevcut hatalar;*

2. *Donanım ve yazılımdaki hatalar;*

3. *Gitgide daha kritik sistemlerin çevrimiçi erişim olasılığı*".[310]

Bir ülke vatandaşı ulusal "*gerçek*" bir alanda yeni fiziksel bir mekânda ikamet eder. Ayrıca genel ağ çağında vatandaş bir "*siber uzayda*" ikamet eder ve Lessig'in de dediği gibi, "*İnsanların, aralarında üstünlük ilkesi olmadan, aynı anda iki yerde birden yaşadıklarını söyleyebileceğimiz bir zaman olmamıştır*." [311] Dolayısıyla, çifte egemenlik şeklinin geçerli olduğu gerçek alanda farklı durumlara uyan üst yetkinin resmî olarak belirlenmesi söz konusudur. Siber uzay ilişkilerinde, vatandaşın yaşadığı gerçek ve siber mekânlar arasında resmî ve üzerinde anlaşılmış bir üstünlük yoktur. Hükümetler (bir kısım) vatandaşlarının siber mekânlara erişimini engellemeye çalışır. Fakat bu, geleneksel "*çifte"* egemenliklerde olduğu gibi farklı durumlara uyan üstün anayasal otoriteyi belirleyen resmî otorite ve egemenlik çerçevesine sahip olmakla aynı değildir. Bu yüzden vatandaşların var oluşunun siber uzay unsurları hakkında bir devletsizlik durumu söz konusudur. Bu var oluş, yasa dışı kumardan ahlâkî olarak çok çirkin olan pornografiye, gerçek zaman ve mekânda vatandaşın içinde yaşadığı devleti hedef alan terör faaliyetlerine kadar uzanan davranışların pek çok patolojik biçiminde açıkça ifade bulan bir düzensizlik durumudur. Bu kesimdeki işlerin büyük kısmı

309 BİLGESAM, op.cit., s.2.

310 CLARK Richard A., Robert K. KNAKE, **Siber Savaş**, TC İstanbul Kültür Üniversitesi, İKÜ Yayın Evi, 2010, çev. Murat ERDURAN, s.45

311 TAYLOR John, "Bilgi Çağı ve Teknolojik Gelişmelerin Devlet Yönetimine Etkileri", **Üçüncü Uluslararası Sempozyum Bildirileri**, Genelkurmay Basım Evi, İstanbul, 12–13 Mayıs 2005, SAREM, s.123.

genel ağdan yapılmakta ve böylece işlem yaptıkları devletlerde geçerli olan kanunlardan kaçılmaktadır. Bu alanda genel ağ büyük oranda kullanılmaktadır çünkü "*genel ağ ortamında sahte kimlikler kolaylıkla oluşturulabildiği için gizlilik imkânı vermektedir*."[312]

3. ULUSLARARASI SİBER GÜVENLİK TATBİKATLARI

Siber savunma alanında farkındalık yaratmak, ülkelerin bu alandaki tecrübelerinden faydalanmak ve uluslararası bir örgütlenme için ortak bir platform oluşturmak için siber güvenlik tatbikatları yapılmaktadır. Tezimin bu bölümünde tatbikatların amaçları ve kısaca içeriği hakkında bilgiler verilecektir.

3.1. DARK SCREEN (2002 -2003)

2002 yılında ABD'nin Texas eyaletinin San Antonio şehrinde gerçekleştirilmiştir. Şehirdeki kamu kurumları katılmıştır. Özellikle su, elektrik gibi kritik altyapılarla ilgili kurumların katılması önemlidir. "*Tatbikat üç aşamada gerçekleştirilmiştir. Merkezi olarak gerçekleştirilen ilk aşamada, tüm katılımcılar tek bir alanda toplanmışlar ve bir gün boyunca siber güvenlik hakkında bilgi almışlardır. İkinci aşamada ise birçok katılımcı kuruluşa sızma testleri gerçekleştirilmiş ve sistemlerdeki açıklıklar raporlanmaya çalışılmıştır. Son aşamada ise katılımcıların yaşanan olaya tepki verme yeteneklerinin ölçülmesi amaçlanmıştır. Bu aşamada, sahip olunan iletişim altyapıları (telefon hatları vb.) zarar gördüğünde kurumlar arası iletişimin nasıl sağlanacağı, kurumlar arası koordinasyonun nasıl gerçekleşeceği tespit edilmeye çalışılmıştır.*"[313]

3.2. CYBER STORM I–II–III (2006 –2008 –2010)

Eylül 2010'da gerçekleştirilen CyberStorm III tatbikatında büyük ölçekli ve kritik altyapıları hedef alan siber saldırılar simülasyon ortamında denenmiştir. Tatbikata ABD'de bulunan 11 eyalet, 12 ülke (Avusturalya, Kanada, Fransa, Almanya, Macaristan, Japonya, İtalya, Hollanda, Yeni Zelanda, İsveç, İsviçre ve İngiltere), 60 özel sektör kuruluşu katılmıştır. 3 gün boyunca 1500'ün üzerinde enjeksiyon uygulanmıştır.[314]

---

312 Ibid., s.124.

313 TATAR Ünal, "Dünyada ve Türkiye'de Siber Güvenlik Tatbikatları", TUBİTAK, UEKAE, Ankara, 2011.

314 Ibid.

3.3. APCERT DRILL 2006-2011 (OCAK 2010)

Asya Pasifik Bilgisayar Olayları Müdahale Ekibi (APCERT) tarafından organize edilen APCERT DRILL'in yedincisi 2011 yılında düzenlenmiştir. Tatbikatta 14 ülkeden 16 katılımcı yer almıştır ve tatbikat bir gün sürmüştür. Katılımcı ülkeler, Avustralya, Brunei, Çin, Tayvan, Hong Kong, Hindistan, Endonezya, Japonya, Kore, Malezya, Singapur, Sri Lanka, Tayland ve Vietnam'dır. Yapılan tatbikatın teması finans sektörüne yönelik saldırılar olarak belirlenmiştir. Tatbikat esnasında hem ülkelerin yaşanan olaylara tepki vermesi hem de kendi aralarında koordine olmaları sağlanmaya çalışılmıştır. [315]

3.4. NATO CYBER DEFENSE EXERCISE (2008–2009–2010)

"*NATO Cyber Defence Exercise*", ilki 2008 yılında gerçekleştirilen, siber savunma amaç ve kapasitelerini hedef alan NATO tatbikatıdır. Tatbikatın amaçları:

- ✓ Stratejik karar verme süreçlerini,
- ✓ NATO ve ulusal siber savunma sorumluluklarını,
- ✓ NATO ve üyesi ülkeler arasındaki siber savunmaya katılım yeteneklerini,

tespit etmek olarak belirtilmiştir. Tatbikat, Brüksel ve Mons'taki NATO NCIRC merkezlerinde ve katılımcı devletlerin BOME merkezlerinde gerçekleştirilmiştir.

Katılımcı NATO üyeleri: Fransa, Almanya, Yunanistan, İtalya, Litvanya, Norveç, İspanya, Türkiye, ABD'dir. Gözlemci NATO üyeleri ise Bulgaristan, Hırvatistan, Çek Cumhuriyeti, Danimarka, Estonya, Letonya, Hollanda, Polonya, Romanya, Slovakya, Slovenya ve İngiltere'dir. 2010 yılında düzenlenen tatbikatta ülkemizi Genelkurmay Başkanlığı ve TÜBİTAK UEKAE temsil etmiştir. 2011 yılında düzenlenecek olan tatbikatta ise ülkemizi Genelkurmay Başkanlığı ve TÜBİTAK UEKAE temsil edecektir.[316]

4. DÜNYADA VERİ KAÇAĞI

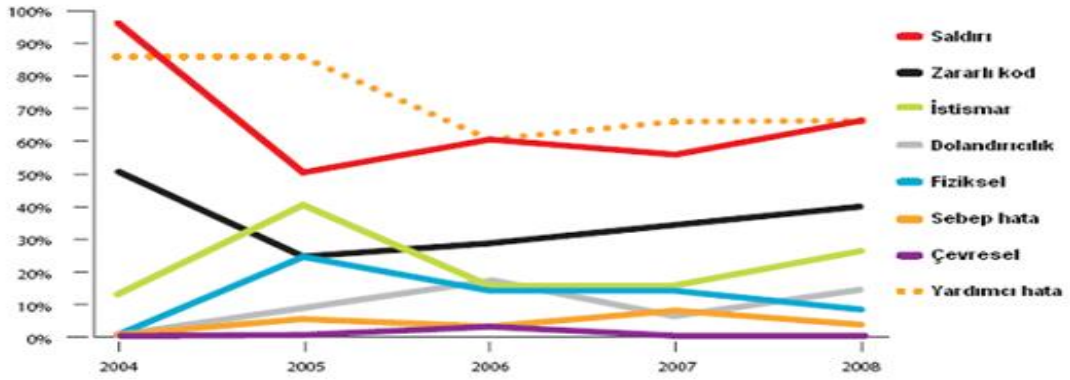
Bilişim sistemleri güvenliği alanında gerçekleştirilen bazı istatistiksel çalışmaların sentezlenmesi dünya genelinde tehdidin ulaşmış olduğu noktayı ortaya koymak adına doğru olacaktır. Verizon tarafından gerçekleştirilen çalışmada 2008 yılında bilgi sistemleri üzerinden kontrolsüz veri çıkışı ile ilgili bilgiler sunulmuş, Önümüzdeki yıllar için öngörüler

315 Ibid.
316 Ibid.

detaylandırılmıştır. Dünya genelinde binlerce bilgi sisteminden elde edilen verilerin analiz edilmesi sonucunda hazırlanan raporda[317] geçen çarpıcı bazı bilgileri şu şekilde özetlemek mümkündür:

2008 yılında 285.000.000 adet veri kaydı istenmeyen kişilerin eline geçmiştir. Kaybedilen verilerin %91'i organize çalışan örgütler tarafından gerçekleştirilmiş planlı suçlar sonucunda ortaya konmuştur. Kaybedilen verilerin %99,6'sı sunucu ve bu sunucularda çalışan uygulamalar üzerinden elde edilmiştir. Bu bilgi özellikle sunucuların korunma ihtiyacını net olarak ortaya koymaktadır.

Saldırıların %74'ü kurum dışı erişim noktalarından gerçekleştirilmiştir. Kaybedilen verinin %91'inin organize çalışmalar sonucunda elde edilmesi bilgisi göz önünde bulundurulduğunda bazı organize örgütlerin kurum veya firmaların içerisine sızdıkları ve faaliyetlerini kuruların iç ağlarından gerçekleştirdikleri görülecektir. Bu oran yaklaşık %20 civarındadır. Öte yandan iç ağlardan gerçekleşen saldırılar sonucunda kaçırılan verinin tüm veri kaçağına oranı %65 olduğu için iç ağ kaynaklı saldırıların çok daha büyük etki bıraktığı söylenebilir. Saldırı kaynaklarının yüzdesel olarak gösterimi Şekil 7'de yer almaktadır.



Şekil 7. Veri kaçağı tehditlerinin yıllara göre durumu

Kaynak:http://www.internetworldstats.com/stats.htm (e.t. 17.05.2011)

5. SİBER GÜVENLİĞİN ÖNGÖRÜLEMEYEN SONUÇLARI

Siber saldırılar, maliyet açısından düşünüldüğünde trilyon doları bulabilecek niteliktedir. Örneğin, 2008 yılında bir veri hırsızlığı olayında mikroişlemci devi Intel

317 Verizon Business, 2009 Data Breach Investigations Report , http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf, (e.t. 13.02.2012).

şirketinin eski bir çalışanı Intel'in rakibi AMD'ye katılmadan önce, 1 milyar dolar değerinde gizli mülkiyet belgelerini bilgisayarına indirmiştir.[318]

Bilgi sistemleri güvenliği ile teknolojik gelişme arasında ters bir orantı söz konusudur. Saldırılar çeşit ve sayıca arttıkça, teknoloji dünyasındaki günlük ilerlemeler de hızlanmaktadır. Bir nevi paradoks yaşandığını söyleyebiliriz. Başlıca siber tehditlerin sebebi yazılım kodlarıdır. Bütün bilgi sistemlerimizin çökmesine neden olabilecek bir durumdur.[319]

Büyük bir bilgisayar firması olan Symantec, 2008 yılında yapmış olduğu çalışmalarda 1 milyon 656 binden fazla sayıda zararlı kod hakkında istatistiksel bilgi topladı. Bu zararlı, yani kötü niyetli kodlarla ilgili olarak, 2007–2008 yılları arasındaki artış dikkat çekmektedir. 600 binden fazla kodun bu kapsama dahil edildiği görülmektedir. Symantec tarafından 2008 yılında toplanan verilere göre, bu zararlı kodlarda muazzam artış kaydedildiği ve bunun doğrusal bir seyir izlemediği görülmektedir.[320]

Zararlı yazılımlara ek olarak her gün 75 bin ele geçirilmiş, yani sahibinin denetiminden çıkmış olan bilgisayar bildirilmektedir. Bir önceki yıla göre %31 artış demektir. 2008 yılında 5 binden fazla güvenlik açığı kayda geçmiştir. Bu da bir önceki yılın % 20 fazlasıdır. Symantec ayrıca yaklaşık 60.000 "*phishing"* adı verilen türden dolandırıcı web sitesi tespit etmiştir. Bunlar bizim kredi kartı numaramızı, pasaport numaramızı, kimlik bilgilerimizi çalmaya yönelik internet uygulamalarıdır.[321] 2012 Şubat ayında özel phishing sitelerinin sayısı 56 bin 859 ile tüm zamanların en yüksek seviyesine ulaşmıştır.[322]

Şimdi internet bağlantısı olan bilgisayarların rakamlarına bakacak olursak, 2013 yılında bu rakamın 3 milyara yaklaşacağı öngörülmektedir. Bunun ötesinde kullanıcı nüfusu da artmaktadır ve Batıdan Doğu'ya doğru bir artış söz konusudur. Çok büyük olasılıkla bunun sonucunda geleceğin internet dünyası birçok dili ön plana çıkaracaktır. Çince, Portekizce, Rusça İngilizcenin yanında daha çok öne çıkmakta ve bu dillerdeki internet trafiği de gittikçe artmaktadır. Yıllık orana baktığımızda bu artış % 50'ye ulaşmış durumdadır.[323]

---

318 ÜÇÜNCÜ Murat, "Siber Savunmada Mücadele Alanları ve Sistem Yönetiminin Önemi", Küresel Terörizm ve Uluslararası İş Birliği, **III. Uluslararası Sempozyum Bildirileri**, Ankara, 15–16 Mart 2010, ss. 55–61.

319 Ibid.

320 Ibid.

321 Ibid.

322 http://www.antiphishing.org/, (e.t. 23.10.2012).

323 ÜÇÜNCÜ, loc.cit.

İran'da sanayi tesislerine bağlı bilgisayar sistemlerini "*Stuxnet*" adlı bir virüsün etkilemesi, İran'ın nükleer programının bir "*siber saldırıya"* uğramış olabileceği kuşkusuna yol açmıştır. İran ise Buşehr'deki nükleer tesisin etkilenmediğini, virüsün sadece bazı çalışanların kişisel bilgisayarlarına bulaştığını açıklamıştır. Ardından olayın daha ciddi olduğu ve virüsün yaklaşık 30 bin bilgisayara bulaştığı ortaya çıkmıştır. Ancak bu olayın kurbanı İran olduğu için, saldırının amacını ortaya koymak pek de zor olmamıştır. İran'ın nükleer programını başarısızlığa uğratmak için bilişim teknolojisinden yararlanılmıştır. İran Sanayi ve Madencilik Bakanlığı, yaklaşık 30 bin bilgisayarın virüsten etkilendiğini açıklamış ve İran'a bir siber savaş açıldığını ifade etmiştir. Uzmanlar, ilk kez geçen haziran ayında ortaya çıkan Stuxnet virüsünün, yazılımının özel olarak hazırlandığı konusunda hemfikir kalmışlardır. Bonn Üniversitesi'nden bilişim uzmanı Felix Leder, "*Stuxnet virüsünü özel kılan, işletim sistemlerinde daha önce hiç karşılaşılmamış, örneğin sıfır-tarih denilen, tüm Windows sistemleri için neredeyse evrensel anahtar olduğu söylenen zayıf noktalar yaratıyor*." diyerek, Stuxnet bilgisayar virüsünün oldukça etkileyici bir donanıma sahip olduğunu ifade etmiştir.[324]

Bilişim uzmanı Felix Leder ayrıca Sutxnet'in özellikle Siemens şirketinin ama kumanda sistemlerini hedef aldığını hatırlatmış ve bu sistemlerin başta enerji santralleri olmak üzere, karmaşık teknik altyapısı olan tüm büyük sanayi tesislerinde mevcut olduğunu söylemiştir. Sutxnet aracılığı ile tesislerin ana kumanda sistemlerinin kontrolünü ele geçirenlerin, motorların devir sayılarını düşürüp yükseltebileceğini, sonuç olarak sistemin işlemez hale getirilebileceğini belirtmiştir.[325] Stuxnet virüsü ABD tarafından o güne kadar bir başka ülkeye karşı yapılan ilk siber saldırı hamlesi olarak yorumlanmıştır. Bu virüsün normal virüslerden 50 kat daha karmaşık ve etkili olması bir kişi tarafından değil bir ülke tarafından yapılmış olma ihtimalini yükseltmiştir.[326]

Stuxnet virüsünün verdiği zararın gerçek boyutları henüz bilinmemektedir. Virüsün gerçekten İran'ın nükleer programına zarar vermiş olması, en azından uranyum zenginleştirme programını sabote etmiş olması da ihtimal dâhilindedir. Wikileaks adlı internet platformu İran'ın Natanz'daki uranyum zenginleştirme tesisinde bir kaza meydana geldiğini açıklamıştır. Aslında böylesi kritik sistemlerin güvenlik gerekçesiyle internetle doğrudan bağlantıları bulunmamaktadır. Ancak Estonya'nın Talinn kentindeki NATO Siber Savunma

---

324 Ibid.

325 Ibid.

326 http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html, (e.t. 23.10.2012).

Merkezi'nden Kenneth Geers, "*Flaş bellekler veya insan faktörü sayesinde her yere girmek mümkün. Ya zararlı yazılımı yükleyecek birine ödeme yapabilirsiniz ya da ona bir USB flaş bellek verebilir ya da dâhili web sistemine girmiş bir kişinin belleğiyle değiştirebilirsiniz*." diyerek, internet ağına bağlı olmasa da, kapalı sistemlere girişin mümkün olduğuna dikkat çekmiştir.[327] Siber saldırılar için belli kalıplarda düşünmenin yanlış olduğu İran'a karşı yapılan saldırılar ile anlaşılmıştır.

Stuxnet çok karmaşık bir yapıya sahiptir. Bu yüzden bu solucanın birçok farklı alandan uzmanların bir araya gelerek üzerinde uzun süre çalıştığı ve kayda değer bir bütçeye sahip bir projenin ürünü olduğu anlaşılmıştır. Yine birçok araştırmacı tarafından bu tür bir projenin basit bir suç örgütünden ziyade devlet desteğindeki bir kuruluş tarafından gerçekleştirilmiş olması daha gerçekçidir.[328]

Stuxnet virüsünün kimin tarafından hazırlandığı ya da yollandığı bilinmemektedir. Kaspersky Güvenlik Şirketi'nden Tilman Werner, " *Hâlihazırda bu işin arkasında kimlerin olduğunu tespit edecek yeterli bilgiye sahip değiliz*." derken, böylesi ileri tekniğe sahip bir yazılımın arkasında bir devletin olma olasılığının yüksek olduğunu belirtmiştir. [329] Ayrıca NATO Siber Savunma Merkezi'nden Kenneth Geers "*Stuxnet, devlet adına çalışan hackerlerin ulaştığı kabiliyete dair bir örnek teşkil ediyor*. *Bu virüsü sadece güvenlik uzmanları değil, suç şebekeleri de en ince ayrıntısına kadar inceleyecek, hatta kopyalamaya çalışacaktır. Bir kaç gün ya da haftaya kalmadan, benzer virüslerin siber suçlularının eline geçmesinin hiç de uzak bir ihtimal olmadığını düşünüyorum*." diyerek Stuxnet virüsünün, suç şebekeleri için de son derece cazip olabileceği konusunda uyarmıştır. [330]

Berlin Hür Üniversitesi'nden Sandro Gaycken, gelecekte askerî görevli hackerlerin önemli bir rol oynayacağını ve siber birliklerin artmaya başladığını söylemiştir. İranlı yetkililer bir süre önce istihbarat servisleri tarafından ortaya atılan İran'daki bilgisayar ağlarına "*Stuxnet*" adlı bir virüsün bulaştığı yönünde iddialara karşısında, söz konusu virüsten İran'daki 30 bin bilgisayarın etkilendiğini doğrulamıştır. Ancak Buşehr'deki nükleer tesisin

---

327 HEIN, loc.cit.

328 PAMUK Osman, "Stuxnet'i Özel Yapan Ne?", http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/stuxneti-ozel-yapan-ne.html, (e.t. 23.10.2012).

329 HEIN, loc.cit.

330 Ibid.

söz konusu virüsten etkilenmediği ve yakında faaliyetlerine başlayacağı belirtmiştir. Ayrıca Gaycken, "*siber saldırılarda seçeneklerin sınırsız olduğunu*" vurgulamıştır.[331]

John Taylor ise ulusun ve egemenliğinin güvenliğinin genel ağ dünyasında daha da hassas hâle geldiğini ve ulusal egemenlik için aşağıdaki noktaların gerçekleşmesini sağlayacak yeni bir tanımlamanın gerekli olduğunu savunmaktadır. [332]

—"*Olaylardan sonra ayakta kalabilecek, güçlü bir kurumun, bir "Dünya Güvenlik Örgütü"nün oluşturulması,*

—Teröristlere ve uluslararası suçlulara "gerçek" (fiziksel) barınak sağlayan devletlerin bireysel egemenliğine müdahale etmeye istekli, daha güçlü bir BM,

—Belirli uluslararası suçlara verilen cezaları ve yüklenen anlamları birbirine uyumlu hale getirecek ortak ve küresel bir kanunlar çerçevesi,

—İstihbarat ve bilgi paylaşımı yönetimi sistemlerinin oluşturulmasını ve tüm ülkelerin bundan faydalanmasını sağlayacak uluslararası düzeyde kaynakların seferber edilmesi,

—Dünya çapında, insan hayatına her yerde eşit değerin verilmesini sağlayacak yeni bir hümanizmin teşvik edilmesi."

6. NATO SİBER SAVUNMA MÜKEMMELİYET MERKEZİ

Tezimin teorik bölümünde de değinildiği üzere Ken Booth'a göre güvenlik, gelecekle ilgili beklentilerin garanti altına alınabilmesi veya isteklerin gerçekleştirilmesi, önündeki engellerin kaldırılmasıdır. Siber savunma son yıllarda büyük güçlerin savunma stratejilerinde ve son defa da Lizbon NATO Zirve toplantısında gündeme giren bir kavramdır. Geleneksel savaş araçları gibi siber teknoloji devlet mekanizmalarını, mali kurumları, ulusal enerji ve ulaşım altyapıları ile toplum moraline saldırı düzenlemenin aracı olabilir. Bununla beraber bazı eylemler savaş olarak nitelendirilmeyebilir. O takdirde bu ayırım nasıl yapılacak? Burada söz konusu olan ilgili aktörler kadar geleneksel savaş niteliği kazanan eylemlerdir. Örneğin terörist grupların istihbarat operasyonları veya organize büyük suç örgütlerinin girişimleri savaş sayılmayabilir. Siber savaş aslında bir "*asimetrik savaş*" olarak da tanımlanabilir. Bir taraf geleneksel imkânlar açısından zayıf olmakla beraber zeki ve atik, diğeri ise hantal ve katı

---

331 ARMBRÜSTER Tobias, **Ülkeler Siber Birlikler Kuruyor**, çev. Başak SEZEN, http://www.dw.de/dw/article/0,,6061521,00.html, (e.t. 06.02.2012).

332 TAYLOR, op.cit., s.125.

bir tutum sergileyebilir. Siber savaş ve tehdidin en önemli niteliği son derece süratle gelişmesidir. Tehdit öylesine hızlı gelişebilir ki geleneksel stratejideki eylem/tepki geç kalabilir.[333]

Siber savaş devletlerarası bir ihtilaf olmakla beraber, değişik yollardan devlet dışı aktörler de devreye girebilir. Siber savaş da belirgin ve orantılı gücü devreye sokmak son derece zordur. Hedef askeri, sanayi, sivil veya değişik sektörlere hizmet veren veya onlardan sadece birisi örneğin sunucuların (server) bulunduğu bir oda dahi olabilir.[334]

Siber savaşın en belirgin niteliklerini şöylece sıralamak mümkün:[335]

1. "*Siber savaş sıcak çatışmaya dönüşmeden, aktörün siyasi ve stratejik amaçlarına ulaşmasına imkân verir.*

2. *Siber savaş normalde tehdit olarak görülmeyecek aktörlere orantısız güç imkanı verir.*

3. *Sahte adreslerle (IP) yabancı sunucularla (server) hiç olmazsa kısa vadede gizlilik ve ceza görmeden faaliyet gösterirler.*

4. *Siber savaşta asker ile sivil, fiziki ile sanal sınırlar bulanıktır. Güç, devletler, devlet dışı aktörler veya "by proxy" kullanılabilir.*

5. *Siber savaş, kara, hava, deniz, uzay yanında 5. Alan olarak değerlendirilmelidir.*

6. *Siber savaşın zarar verme yeteneği ve gerginlik yaratmada geleneksel savaşlarla beraber yürütüleceği varsayılmakla beraber, ihtilaf şekli olarak diğerlerinden ayrıca değerlendirilmek gerekir*."

Siber dünya bilinmeyenin bilinenden daha fazla olduğu bir durum ile karşı karşıyadır. Oluşturulacak politikalar, meydan okumalara etkin yanıt verecek şekilde esnek olmalıdır. Bu yapılırken önemli bazı soruların cevaplarının aranması da gerekmektedir. Bireysel saldırıdan siber savaş konumuna geçişteki fark ne olacak? Gelecekteki konvansiyonel ve konvansiyonel

333 BİLGESAM, op.cit., s.6.
334 Ibid., s.7.
335 Ibid.

dışı savaşlardaki etkisi ne olacak? Stratejik ve siyasal anlamda siber savaş nasıl değerlendirilmeli? Teknik olarak siber savaş "*kansız savaşı*" gerçek kılabilir mi? [336]

Siber saldırılar ve kritik altyapıların güvenliği NATO'nun 2008 Bükreş Zirvesi'nde bazı sorunlara çözüm arayışları konusu gündeme gelmiş, siber savunmada işbirliği için birimlerin kurulması kararı alınmıştır. Bu karar neticesinde "*Savunma Yönetim Otoritesi*" ile "*Siber Savunma Mükemmeliyet Merkezi*" kurulmuştur. Ayrıca NATO'nun yeni stratejik konsepti ve "*2012 Chicago Zirvesi*" sonuç bildirisinde de sürekli gelişen ve karmaşıklaşan siber tehditlerle etkin biçimde ve işbirliği içinde mücadele edilmesi gerektiği vurgulanmıştır.[337]

NATO'nun siber savunmadaki odak noktası Müttefik ülkelerin siber güvenliğinin güçlendirilmesine yardımcı olacak şekilde genişletilmiştir. NATO, iletişim ve enformasyon sistemlerini saldırılar veya yasadışı erişime karşı koruma sistemlerini sürekli olarak geliştirmekte ve güçlendirmektedir.[338]

Uluslararası düzeyde işbirliğine gidilmesinin ön şartı siber savaş konusunda ortak bir anlayışa varılmasıdır. Mevcut askeri ve siyasi anlayışın siber savaşın ortaya koyduğu tehdit ve meydan okumalara cevap bulabilmesi zordur. O nedenle, siber alan için oluşturulacak politikalarda yeni düşünce sistemlerine ihtiyaç vardır. Ulusal stratejilerin, geleneksel kalıplardan uzaklaşarak siyasetin güvenilir, bilinir, pragmatik yönlendirmesiyle hızlı değişikliklere cevap verebilir modeller üzerine bina edilmesi gerekmektedir. Bir diğer önemli nokta da, siber alanın kesin biçimde askerileşmesinin engellenmesidir.[339]

6.1. NATO BİLGİ HAREKÂTI KONSEPTİ ÇALIŞMALARI

Uluslararası Askeri Karargâh (IMS: International Military Staff) Harekât Başkanlığı (Operations Division) tarafından yürütülen bir çalışma sonucunda, teknolojik gelişmelere paralel olarak NATO çapındaki doktrinleri ve harekât planlarını destekleyecek yeni bir

---

336 Ibid.

337 AKÇADAĞ Emine, "Sürekli Artan Önemi Işığında Siber Güvenlik", http://www.bilgesam.org/tr/index.php?option=com_content&view=article&id=2178:suerekli-artan-oenemi-inda-siber-guevenlik&catid=122:analizler-guvenlik&Itemid=147, (e.t. 23.10.2012).

338 AAVIKSOO Jaak, Estonya Savunma Bakanı, "Siber Güvenliğin Güçlendirilmesi", http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_new-security-challenges-tu.pdf, (e.t. 23.10.2012).

339 BİLGESAM, loc.cit.

"Komuta ve Kontrol Harbi" konsepti oluşturulmuş ve anılan doküman MC 348 adı altında onaylanmıştır.

Bilgi Harekâtı Konsepti, NATO'nun yanı sıra, bazı ileri NATO ülkelerinin de, milli olarak, üzerinde çalıştığı güncel bir konu olup, bu konuda, ABD planlarını geliştirip konuyu icra safhasına sokmuştur. İngiltere ve Kanada, "Bilgi Harekâtı" konsepti geliştirmek maksadıyla teşkilatlarını kurmuş ve personelini tahsis etmiştir. Almanya ise aktif olarak çalışmalarını sürdürmektedir. Bilgi Harekâtı konusunda NATO'daki çalışmalar, kabul edilmiş bir başlangıç noktası olduğundan, Komuta ve Kontrol Harbi üzerine bina edilmektedir. Komuta Kontrol Harbi Politikaları, geniş kapsamda Bilgi Harekâtı için bir çekirdek teşkil etmektedir. Bilgi Harekâtı barış, kriz ve savaşta yapılan geniş kapsamdaki askeri ve sivil uygulamaları içermektedir. [340]

6.2. NATO'NUN BİLGİ HAREKÂTINA BAKIŞI

NATO'nun Bilgi Harekâtı ile ilgilenmesinde birçok nedenler mevcuttur. Bunları genel olarak şu şekilde belirtebiliriz;

(1) "*Körfez harbinden alınan dersler; komutanlara bütün bilginin bir yerde ve tam parmaklarının ucunda olmasını dikte ettirmektedir.*

(2) Bilgi anında ve çok sık kullanılmaktadır. Seyir tehdit ve hedef bilgileri, algılayıcılardan, tanka, uçağa ve gemiye doğrudan gönderilebilmektedir. J2 ve J3 faaliyetleri arasındaki farklılık azalmaktadır.

(3) Teknolojik gelişmeler sivil endüstri alanında da hızla devam etmektedir. Cihazlar sadece askeri kullanım için gelişmemektedir. Ticari bilgisayar ürünleri askeri kullanımın her yerinde yer almaktadır.

(4) Diğer bir gelişme ise "küçülme" olgusudur. Eskiden genelde askeri birimlerce yapılan birtakım teçhizatlanma faaliyetleri artık sivil organizasyonlarca gerçekleştirilmektedir.

(5) Diğer bir gelişme de açıklık ve bilginin serbestliği açısından her türlü bilginin internette yer almasıdır."

---

340 TSK, loc.cit.

Bilgi harekâtı ile yakın olarak ilgilenmede yukarıdaki hususların yeterli nedenler olmadığını, uygulamaların sadece askeri sistemlere dayandırılacağını düşünsek bile askeri sistemlerin yine de sivil bilgi iletişim alt yapısı tarafından desteklenme olgusu bilgi harekatı ile yakından ilgilenilmesi gerçeğini ortaya çıkarmaktadır.[341]

6.3. NATO'NUN BİLGİ HARBİ VE BİLGİ HAREKÂTI TANIMLARI

NATO tarafından Bilgi Harbinin henüz kabul edilmiş bir tanımı bulunmamakla birlikte, MC 422 (NATO Bilgi Harekâtı Politikası-TASLAK) 'de önerilen Bilgi Harbi tanımı şu şekildedir;

"Belirgin bir politik ve/veya askeri hedefleri ele geçirmek veya geliştirmek maksadıyla belirlenmiş bir muhasım veya muhasımlara karşı kriz ve çatışma zamanlarında icra edilen bilgi harekâtıdır. " diğer bir tanım şekli de:

"*Politik ve askeri hedefleri desteklemek için, kendi bilgi ve/veya bilgi sistemlerini etkili bir şekilde kullanıp korurken, hasmın bilgiye dayalı işlemlerini, komuta kontrol (C2) sistemlerini, muhabere ve bilgi sistemlerini etkileyerek karar vericilerin müessir olmalarını sağlamak maksadıyla icra edilen faaliyetlerdir.*"

İcra edilen harekâtın tabiatına göre, bilgi harekâtı ikiye ayrılır: "*Tesadüfi Bilgi Harekâtı*" ve "*Taarruzi Bilgi Harekâtı*." [342]

"*Siber saldırıları nasıl engelleyebiliriz? Mükemmel bir sistemi nasıl tanımlayabiliriz? Sistem konfigürasyonunu nasıl yapabiliriz? Sistem yönetiminin unsurları nelerdir? Bunlar; sistem kurulumu, kaynak yönetimi, konfigürasyonların yönetimi, güvenlik olayı yönetimi, kayıt sistemlerinin yönetimi, rutin teftişler, performans yönetimi, yazılım sürümü yönetimi ve iyi bir destek servisidir.*"[343]

"Neyi yönetmemiz ve neyi korumamız gerektiğini biliyor muyuz? Son derece büyük ve karmaşık sistemleri yönetmemiz gerekiyor. Acaba sistemdeki her bir parçayı, her bir ayağını tanıyor muyuz ve bunu bildiğimizden, tanıdığımızdan emin miyiz? İkinci olarak şunu biliyor muyuz; acaba en uygun donanımı, yazılımı seçmiş miyiz? Kendi sistemimize uygun sistemler mi kullanıyoruz? Sonuçta piyasada yüzlerce farklı araç, çözüm veya seçenek söz konusudur.

341 Ibid.
342 Ibid.
343 ÜÇÜNCÜ, loc.cit.

Acaba bizim modelimiz bizim amacımıza en uygun model midir? Siber saldırıları önlemek için gerekli önlemleri almış durumda mıyız? Uygun araçlar mı kullanıyoruz?" [344]

Siber dünyada terminalleri tabiî ki kontrol altında tutmamız gerekiyor ama hem buradaki santralleri hem de yazılımları göz önünde bulundurmalıyız. Acaba hangi varlıklar bizim kontrolümüz altında ve donanımımızda hangi yazılımlar kullanılıyor, bunları tam olarak bilmemiz gerekiyor. Bunu bilmek için rutin denetimler, incelemeler yapmamız ve ihlallerin engellenmesi için güvenlik ihlali yönetim sistemini hayata geçirmemiz gerekiyor. Yalnızca güvenlik önlemi almak yeterli değildir. İyi bir sistem tesis ettikten sonra, düzenli aralıklarla güvenlik denetiminin yapılması gerekiyor ki eğer belli noktalarda güvenlik açıkları varsa, bunlar yamalarla bertaraf edilebilsin. Bilişim sistemleri yaşayan organizmalar gibidir ve her zaman özel ilgi, alaka gösterilmesi çok büyük önem arz etmektedir. Bu güvenlik açıklarıyla ilgili bir başka konu daha var, o da saldırganın bilgi düzeyi ile saldırı düzeyi arasındaki ters orandır. Burada bir ters oran söz konusu; sistemlere izinsiz sızmaya çalışanların bilgi düzeyi azalmakta, çünkü artık internette bu konuda birçok yazılım hazır bulunmakta ve saldırıları kolaylaştırmaktadır. Saldırganlar aynı zamanda bu hazır araçlardan faydalanarak sürekli daha karmaşık saldırılarda bulunabilirler. Bu nedenle bilgisayar güvenlik uzmanlarının, saldırganların kullandığı araçlar konusunda da eğitilmesi büyük önem arz etmektedir. Günümüzde siber saldırılara karşı savunma çok daha kolay ve daha etkili hale gelmiştir. Hatta iletişim ve bilgi sistemleri, kişiler ve istihbarat kurumları arasında yakın bir koordinasyon oluşturulabilmektedir. Aslında, siber suçla mücadelede bu mutlak surette zorunludur.[345]

"*Bilişimin büyük bir silah haline dönüştüğü günümüzde, devletler sanal silah üretimine de büyük önem veriyor. Bilişim uzmanları, sanal âlemden kaynaklanan bu yeni tehlikenin yabana atılmaması konusunda birleşiyor. Kimliği belirsiz bir azmettirici, sessiz bir silah ve meçhul bir tetikçi... Kimi strateji uzmanları, siber saldırıları, bugünün en sinsi savaş yöntemi olarak nitelendiriyor. Geride hemen hemen hiç iz bırakmayan, fail ve azmettiricisinin siber dünyanın derinliklerinde kaybolmasını sağlayan bu soyut düşmanla mücadelenin ne kadar zor olduğunu, "Stuxnet" adlı son bilgisayar virüsü saldırısı bir daha gösterdi.*"[346]

---

344 Ibid.

345 Ibid.

346 HEIN Matthias von, "Siber savaş tehdidi artıyor", çev. Gezal ACER, http://www.dw.de/dw/article/0,,6058903,00.htmlhttp://www.dw.de/dw/article/0,,6058903,00.html, (e.t.06.02.2012).

Güvenlik hizmeti sağlayıcılarının sayısı da gittikçe artmaktadır ve bu güvenlik hizmeti sağlayıcılar katkıda bulunanlardan verileri topladıktan sonra küresel bir risk haritası oluşturarak farkındalığı arttırmakta ve bilgilendirme sağlamaktadır. Çünkü tek bir kurumun bu güvenlikle ilgili verileri tek başına toplayıp paylaşması mümkün değildir. Hâlbuki bu ağlar sayesinde bir ilişki sağlanmaktadır. Burada belli üçüncü taraf organizasyonlar arasında bağlantılar sağlanmakta, acil durum müdahale ekipleri bu şekilde oluşturulmaktadır. İş birliği sayesinde ve ortaklaşa savunma yöntemleri geliştirmek suretiyle siber saldırılara karşı daha sağlam durulabilmektedir. Artık günümüzde Siber Savunma ya da Siber Komutanlık çok daha büyük önem arz etmektedir. Türk Silahlı Kuvvetleri siber dünyada savunma ve saldırı unsurlarını en kısa sürede oluşturmalı, konu ile ilgili mevcut uluslararası organizasyonlar ile ortaklaşa tatbikatlar yapmalıdır. Genç ve dinamik Türkiye nüfusu bunun için yeterlidir. Kim bilir belki Türk Silahlı Kuvvetleri'ndeki bu oluşum mevcut askerlik hizmetinde de radikal değişikliklere sebep olabilecektir. Elinde silahı ile nöbet tutan bir Mehmetçik'in yerine bilgisayarı ile siber savunma güçlerinde yer alan bir "*E-Mehmetçik*".

Sonuç olarak tehditler ne kadar karmaşık hale gelirse, o kadar fazla sağlam zemin çalışması yapmamız, farkındalığımızı arttırmamız gerekmektedir. Hem güvenlik çalışmalarını sürdürmeli, hem de yeni hassasiyet noktalarını tespit etmeliyiz.

7. TÜRKİYE VE SİBER GÜVENLİK

Çalışmamızın bu bölümünde; Türkiye'nin siber güvenlik çalışmalarındaki mevcut durumu, geleceğe yönelik planları ve bu yönde özellikle Türk Silahlı Kuvvetleri'nin yapılanması üzerinde durulacaktır. Siber güvenlik alanında ileri seviyede olan devletlerin mevcut yapılanmasından örnek alarak oluşum arayışında olan Türkiye, uluslararası yapılanma içerisinde de kendisini özellikle bölgesel siber güç olarak konumlandırmayı istemektedir. Bu bağlamda komşu devletler ile yapılacak ortak tatbikatlar ve bilgi paylaşımı alanında oluşturulacak üst yapılanmalar, bölgesel siber barışa hizmet etmede uluslararası siber güvenliğe de çok önemli katkılar sağlayacaktır. Bölgesel güç olma yolunda kararlı adımlarla ilerleyen Türkiye, gelecekte oluşabilecek güç merkezleri için bu fırsatları çok iyi değerlendirmelidir.

7.1. TÜRKİYE'NİN SİBER GÜVENLİK ALANINDAKİ DURUMU

"*Siber güvenlik için en büyük tehdit, siber güvenliği küçümsemektir.*"[347] Bu sözü her zaman kendimiz için bir rehber kabul ederek bu sahada çalışmalarımız hız kazanmalı ve eksiklerimiz uzman kişilerin önderliğinde tamamlanmalıdır. Çünkü siber güvenliğin önemi her geçen gün artmakta ve yeni yüzyılda bölgesinde etkisini arttırmaya çalışan bir Türkiye için çok önemli fırsatları da beraberinde getirmektedir.

Türkiye'nin bilgisayar ile tanışması 1960'ta Karayolları Genel Müdürlüğü'nde hizmete giren Türkiye'nin ilk bilgisayarı ile olmuştur. Çoğu, fizikçi, matematikçi ve inşaatçılardan oluşan Türkiye'nin alaylı ilk bilgi işlemcileri de bu kurumlardan yetişmiştir.[348] Türkiye'nin ilk bilgisayar destekli karayolunun hesaplarını yapmak üzere 1960 yılında getirilen IBM 650, daha önce 3–4 ay süren yol hesaplarını 1 saatte yapabilmiştir. İlk etapta pek çok insanın tereddütle yaklaştığı bilgisayar 1960 yılı Eylül ayının son günü Türkiye'ye gelmiş ve o zaman ki adıyla Karayolları Umum Müdürlüğü'nde kurulmuştur. IBM 650 Model-I adını taşıyan bu sistem sadece Türkiye'nin değil Balkanlar ve Ortadoğu'nun da ilk bilgisayarı olmuştur. Türkiye'nin ikinci bilgisayarı (IBM 1620), 1963 yılında İstanbul Teknik Üniversitesi'ne; üçüncüsü ODTÜ'ye, dördüncü bilgisayarı (UNIVAC 1005) ise yine 1964'te Devlet İstatistik Enstitüsü'ne (DİE) kurulmuştur.[349] Bilgi Çağı'nı yakalama adına ilklere imza atan Türkiye, bu alandaki başarısını siber güvenlik yapılanmalarına adapte etmede zorlanmıştır. Siber güvenlik alanında zafiyetler ortaya çıktıkça, günübirlik kararlar ile tedbirler alınmış ve o anlık tehdit bertaraf edilmiştir. Milli Güvenlik Kurulu'nun son zamanlarda artan siber saldırı tehdit algısı ile birlikte daha somut ve Türkiye'nin siber savunma alanındaki etkinliğini arttırmaya yönelik bir üst yapılanmaya ihtiyaç duyduğu ortaya çıkmıştır. 27 Ekim 2010 tarihli MGK bildirisi siber güvenlik alanında yapılanmayı tarif etmiştir. Bu açıklama da "*Siber tehdidin global düzeyde ulaştığı boyut ve bu tehdidin ulusal güvenliğe etkilerinin kapsamlı surette ele alındığı, siber tehdidin engellenebilmesi açısından milli düzeyde yürütülen çalışmaların da değerlendirildiği belirtilmiştir.*"[350]

TBMM tarafından ilgili yasal düzenleme ile "*Siber Güvenlik Kurulu*" oluşturulmuştur. Bu kurul; kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü

---

347 Türk Silahlı Kuvvetleri'nin kendisine rehber olarak belirlediği bu cümle, her zaman kurumu dinamik ve canlı tutacaktır.

348 ÖZKAN Akdoğan, "Elektronik Beyinden Akıllı Kaleme", National Geographic Türkiye, Mart 2012.

349 Ibid.

350 http://www.mgk.gov.tr/Turkce/basinbildiri2010/27ekim2010.html , (e.t. 14.02.2012).

hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğinin korunmasına yönelik tedbirlerin alınmasını sağlayacaktır. "*Ayrıca bilgi iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasları düzenlemekle görevlendirilmiştir. İlgili yasal düzenlemeler ile ulusal siber güvenliğin sağlanması amacıyla mümkün olan tüm alanlarda milli çözümler geliştirilmesi, yazılım ve donanım alt yapılarında azami ölçüde milli kaynakların kullanılmasını amaçlanmıştır.*"[351]

Siber Güvenli Kurulu'nun genel sorumluluğu Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na verilmiştir. Ayrıca kurul içerisine üye olarak; "*Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticileri*" bulunacaktır.[352]

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın siber güvenlik alanında görevleri şunlardır;

- "*Ulusal siber güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak,*

- *Kamu kurum kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasları hazırlamak,*

- *Ulusal siber güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik alt yapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak,*

- *Ulusal bilgi teknolojileri ve iletişim alt yapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik alt yapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri*

351 www.resmigazete.gov.treskiler20121020121020-18-1.pdf, (e.t. 29.10.2012).
352 Ibid.

kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmalar yapmak,

- *Ulusal siber güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımını sağlamak,*

- *Ulusal siber güvenlik açısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini planlamak, koordine etmek ve yürütmek,*

- *Bu karar çerçevesinde diğer devletler ve uluslararası kuruluşlarla işbirliği yapmak,*

- *Ulusal siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı arttırma çalışmaları yürütmek,*

- *Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esaslarını belirleyerek güvenlik belgesi vermek,*"[353]

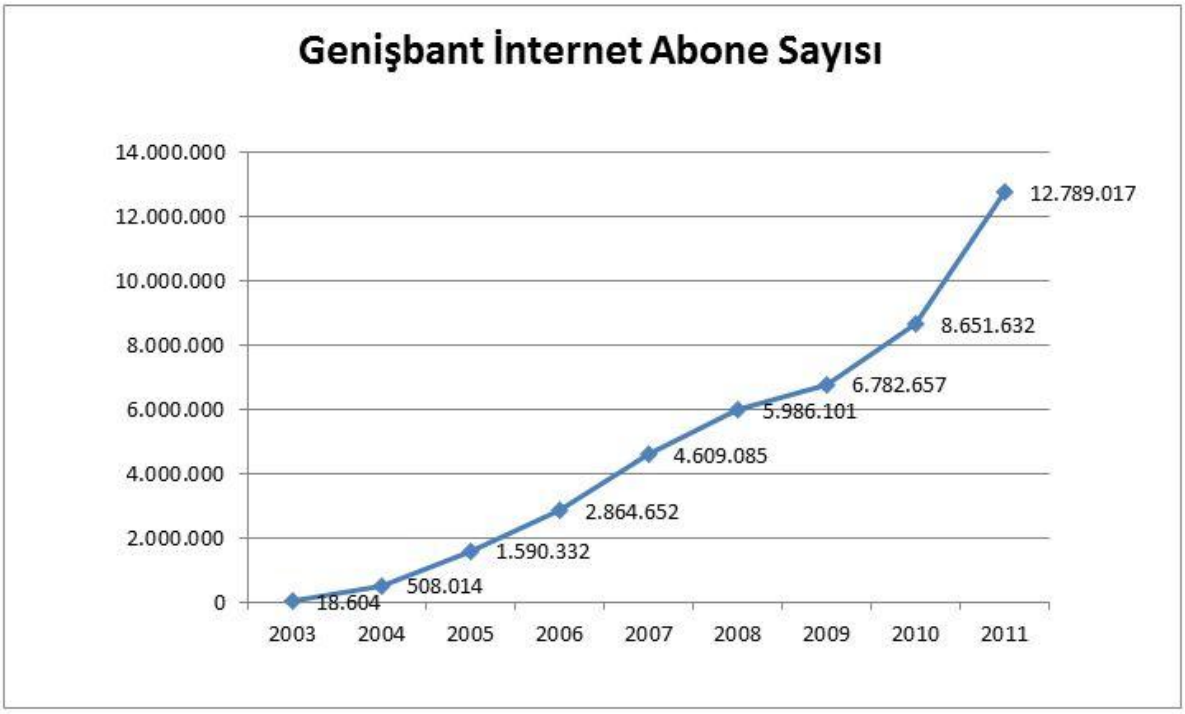
Diğer taraftan, 25–26 Ocak 2012 tarihlerinde Ankara'da gerçekleştirilen Siber Güvenlik Hukuku Çalıştayı'nda ise siber varlıkların sınırlarının ve bu varlıklar arasındaki iletişimin ulusal sınırları aştığı belirtilmiştir. Siber ortamda saldırgan ve mağdurların çoğu durumda farklı devletlerde yer alabildiği, dolayısıyla siber güvenlik alanında, uluslararası birlikte çalışılabilirlik mekanizmalarının ve sözleşmelerin önem kazandığı, önümüzdeki günlerde uluslararası işbirliklerinin daha da arttırılmasına ihtiyaç olduğu vurgulanmıştır.[354]

Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanı Tayfun ACARER'in yaptığı açıklamada; "*Türkiye'de geniş bant internet kullanan abone sayısının Şekil-8'den de anlaşılacağı üzere 11,3 milyona ulaştığı ve ülkemizin Hollanda ve İngiltere'den sonra Avrupa'da en çok internet kullanan üçüncü devlet konumunda olduğunu belirtmiştir. Ayda yaklaşık 32 saat internetin kullanıldığı, bu artış hızı ile birlikte siber güvenlik konusunun da öneminin artırdığını, ülkemizde teknik altyapının, siber savunma sistemlerinin ve bu alana*

353 Ibid.

354 **Siber Güvenlik Hukuku Çalıştayı 2012**, http://www.iscturkey.org/calistay/2/, (e.t. 16.02.2012).

ilişkin idari düzenlemelerin hızlı bir biçimde hayata geçirilmesi gerektiğini vurgulamıştır."[355]



Şekil 8- Türkiye'de Geniş Bant İnternet Abone Sayısı: BTK'nın 2011 yılı 3. çeyrek verilerine göre 12.789.017'a çıkmıştır.

Kaynak: http://www.gig.org.tr/tr-menu-2-arastirmalar.html, (e.t. 20.02.2012).

Siber saldırılar gerçekten çok kolaylıkla hayata geçirilebilmektedir. Saldırı planlayanlar küresel bir kapasite havuzundan yararlanabilmekte ve bu saldırıları gerekli yazılımları kullanarak tasarlayabilmektedirler. Donanım ve yazılım dünyasında sistemin çalışabilmesi için asgari olarak bazı kapıların açık kalması kaçınılmazdır ve kötü niyetli kişilerin de bundan faydalanmaları çok doğaldır. Siber tehditler bağlamında kuruluşların çok büyük bir kısmı, birbirinin benzeri güvenlik duvarları, anti virüs ve casus program tarayıcıları ile önlemler almaktadır. Ancak milyonlarca dolar harcansa da güvenlik ürünleri yine de yeterli güvenliği sağlamamaktadır. Önemli olan, gerekli önlemlerin hayata geçirildiğinden ve bunun etkin bir şekilde süreklilik arz ettiğinden emin olabilmektir. Büyük kuruluşlar açısından tabiî ki bu alanda kapsamlı çalışmaların, sistematik güvenlik sistemlerinin hayata

[355] II. Ulusal Siber Güvenlik Çalıştayı, 29 Eylül 2011, Ankara, http://www.iscturkey.org, (e.t. 16.02.2012).

geçirilmesi hayati önem taşımaktadır. Tabiî uluslararası çapta kabul gören bazı iyi uygulamalar da vardır. ISO 27000 standartları da bunun bir parçasını oluşturmaktadır. [356]

Bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişim ve siber ortamda sunulan hizmetlerin yaygınlaşması, "*Siber uzay nasıl kontrol edilecek?*" sorusunu gündeme getirmiştir. Günümüzde siber savaş, diğer muharebe sahalarını kapsar hale gelmiş ve bunun ötesinde de başlı başına bir muharebe sahası olarak şu anda kullanılmaktadır.

Türkiye bulunduğu coğrafya itibariyle ve bilgi sistemleri alt yapısına yapmış olduğu yatırımlar sonucu siber saldırılara maruz kalma riski en yüksek olan devletlerden biridir. Böyle bir saldırıyı önlemek için teknolojiyi yakından takip ederek dünya ülkeleri ile aynı anda ve hatta tehdit olarak değerlendirdiğimiz komşularımızdan daha önce bu teknolojilere sahip olarak, caydırıcı bir güce sahip olmalıdır.

Siber saldırılara karşı kullanıcılarda güvenlik konusunda belirli bir bilinç bulunmamaktadır. Potansiyel olarak bazı insanların bilgileri istem dışı olarak yanlış kaynaklara aktarması söz konusu olabilmektedir. Bu durumda bir kurum içinde bilgisayar sistemlerine bu şekilde giriş yapılabilmekte ve kurum çapında bilgiler elde edilebilmektedir. Bu yüzden güvenlik meselesine daha çok dikkat edilmesi gerekmektedir. Ne yazık ki kullanıcılar parolalarını, şifrelerini monitörlerin üstüne iliştirdikleri yapışkan notlarda ya da kolay bulunabilecek şekilde klavyelerinin altına yapıştırdıkları etiketlere gizleyebilmektedir. Özellikle, Devlet Planlama Teşkilatının topladığı istatistikler de bize gösteriyor ki internet kullanıcılarının %50'si bilgisayarlarında herhangi bir güvenlik önlemi almamaktadır. Kullanıcıların % 7,9'u bu konuda herhangi bir şey bilmemektedir. Yani internet güvenlik araçlarıyla ilgili hiçbir bilgiye sahip değillerdir. Kullanıcıların %42'si de hiçbir güvenlik aracı kullanmamakta ve hiçbir önlem almamaktadır. Bütün bu nedenlerden dolayı güvenlikle ilgili farkındalık programlarının hayata geçirilmesi, eğitim programlarının düzenlenmesi hayati önem taşımaktadır. En azından temel nitelikte güvenlik önlemlerinin bütün kullanıcılar tarafından bilinmesi güvenli bilgi sistemlerinin oluşturulabilmesi için şarttır.[357]

Türkiye de bu anlamda yapılan Siber Güvenlik Çalıştayı'nda siber güvenliğin temel unsurlarından olan güvenlik yazılım ve donanımlarının yerli üretiminin kısıtlı olduğu, bu

---

[356] Bu konuda daha geniş bilgi için bknz.; ÜÇÜNCÜ Murat, "Siber Savunmada Mücadele Alanları ve Sistem Yönetiminin Önemi", Küresel Terörizm ve Uluslararası İş Birliği, **III. Uluslararası Sempozyum Bildirileri**, Ankara, 15–16 Mart 2010, ss. 55–61.

[357] Ibid.

durumun devlet güvenliği için stratejik öneme sahip olması nedeniyle yerli ürünlerin üretimine daha fazla teşvik verilmesinin gerekli olduğu belirtilmiştir. Çalıştayın sonuç bildirgesinde ayrıca, "*ağ ve bilgi sistemlerin ve varlıklarının devlet ekonomisi, kamu refahı ve güvenliği için çok önemli olduğu, dolayısıyla da siber varlıkların güvenliğinin devlet ve toplum güvenliğiyle eşdeğer olduğu, bu hususun her zaman hatırda tutularak kapsamlı ve uzun soluklu adımlar atılması ve çözümler geliştirilmesi gerektiği belirtilmiştir.*"[358]

Ayrıca, "*hızla artan ve çeşitlenen tehditlere karşı etkin mücadelenin küresel ölçekte örgütlenmiş organizasyonlar eliyle yürütülebileceği, bu yönüyle siber saldırılara karşı uluslararası bilgi paylaşımı ve işbirliklerinin de önem arz ettiği, Türkiye'nin ilgili organizasyonlarla işbirliğini daha da güçlendirmesi gerektiği, hatta bu konuda bölgesel bir siber güvenlik organizasyonunun kurulmasına öncülük etmesinin çok yerinde olacağı ve bölgede lider devlet olma vizyonunu da güçlendireceği*"[359] ifade edilmiştir. Bu durum benzer devletlerde olduğu gibi siber güvenlik alanında ayrı bir kurumun bu mücadeleyi vermesini gerekli kılmaktadır.

Alınan sonuçlar arasında; "*tüm kurum ve kuruluşların birçok hizmetlerini internet ortamında sunmaya başlamasıyla birlikte bu ortamda yaşanacak olumsuzlukların kişisel, sosyal ve ekonomik hayatımızı önemli ölçüde etkilediği belirtilmiştir. Etkili tedbirler alınmadığı takdirde gelecekte yaşanabilecek olumsuzlukların daha da artacağı, oluşabilecek siber güvenlik vakalarının hem maddi hem de manevi zararlar verebileceği, bu tür zararlarının büyük ölçüde engellenebilmesi için ilgili tüm taraflara görevler düştüğüne değinilmiştir.*" [360]

Türkiye siber güvenlik alanında fikir alış verişini, kendi iç dinamikleri ve uluslararası yapılar ile ortaklaşa yaptıkları çalışmalar sonucu belli bir seviyeye getirmiştir. Gerekli kurumların bir an önce oluşturulması ve daha öncesinde bir üst yapılanmanın bu oluşumları tek elden yürütmesinin faydalı olacağı değerlendirilmektedir. İşte bu noktada, Bu üst yapılanmayı kim yönetecek? Türkiye'nin siber güvenliğinden hangi kurum sorumlu olacak? soruları akıllara gelmektedir. Bana göre bu sorunun şüphesiz cevabı Türk Silahlı Kuvvetleri'dir. Mevcut yapılanması, bilgi birikimi ve bu yönde planlamış olduğu geleceğin "*Siber Kuvvet Komutanlığı*" gibi projeleri konunun öneminin tam olarak anlaşıldığının bir göstergesidir. Kurulması düşünülen

358 II. Ulusal Siber Güvenlik Çalıştayı, 29 Eylül 2011, Ankara, http://www.iscturkey.org, (e.t. 16.02.2012).
359 Ibid.
360 **Siber Güvenlik Hukuku Çalıştayı 2012**, loc.cit.

"*Siber Kuvvet Komutanlığı*" TSK'nın bilgi savaşı kabiliyetlerini artırmak istediği şeklinde yorumlanabilir. Gerek stratejik seviyede gerekse taktik seviyede gelişmiş bilgisayar ağlarına sahip TSK'nın elbette bu alt yapısını barış ve savaş zamanında daha organize bir şekilde korumak istemesi doğaldır. Benzer hassasiyetin diğer kamu kuruluşlarında da gösterilmeye başlanması Türkiye adına sevindirici gelişmelerdir.

Bu bağlamda Bilim Teknik Dergisi'nin Kasım 2010 sayısında ki haber aynen dikkat çekicidir; *"Siber tehditlere karşı hareket başlatılacağını açıklayan MGK, yeni bir ordu kurmaya hazırlanıyor. Son bir ayın yoğun gündeminde gözümüzden kaçan ya da fazla dikkate almadığımız gelişmelerden biri de "Siber Ordu"ydu. MGK'nın bildirilerinde "siber tehditle mücadele için ulusal çapta savaş başlatılarak yeni bir ordunun kurulacağı" açıklanıyordu. Siber tehditle mücadele için topyekun hareket başlatılacağını açıklayan MGK, yeni bir ordu kurmaya hazırlanıyor. ABD'de Pentagon'un çalışma sisteminin benzeri olarak kurulacak "Siber Ordu"nun özel bütçesi olacak, özel birlikler oluşturup özel timlerle özel operasyonlar yapacakları belirtiliyor. Kamuoyunda "Kırmızı Kitap" olarak bilinen Milli Güvenlik Siyaset Belgesi'ne tehdit algısı olarak giren siber terörizme karşı 20 kurumun ortaklaşa hazırladıkları "Ulusal Sanal Ortam Güvenlik Politikası" hayata geçirilecek. Cumhurbaşkanlığı, Genel Kurmay başkanlığı ve Başbakanlık da bu çalışmaya katılacak. Çalışmalar TÜBİTAK'ın başkanlığında yürütülecek ve geliştirilecek strateji yerli hackerların yanı sıra küresel ölçekli siber tehdit anlamındaki "yabancı" hackerlardan da korunmayı başa yazıyor. Yerli ya da "yabancı" olsun hackerların metodolojisi konusunda bilgilendirme ve aydınlatma yapılarak "beyaz hacker"lar yetiştirilmesi planlanıyor. Siber ordu" çalışmaları aslında uzun zamandır yasal olmayan şekilde internet ortamında yapılıyordu; şimdi bunun yasallaştırılması gündemde. ABD'de Pentagon'un 15 bin siber ordu çalışanı olduğu tahmin ediliyor. MGK da benzer bir çalışmayı uzun zamandır hayata geçirmeye çalışıyor."* Günümüzde dünya orduları bilgi teknolojilerinin nimetlerinden en üst düzeyde faydalanacak şekilde bir yapılanmaya gitmektedir. Bu gelişmiş bilgi alt yapısı TSK'ya birçok avantaj sağladığı gibi, aynı zamanda, bilgi savaşı hedeflerinden biri haline de gelmiştir.

7.2. SİBER GÜVENLİK ULUSAL EYLEM PLANI

Türkiye, oluşturulmaya çalışılan "*Ulusal Bilgi Güvenliği*" programı ile yüksek önemi haiz kamu kuruluşlarının bilgisayar sistemlerini ve ağlarını koruma altına almak için TÜBİTAK tarafından kurulmuş birimler vasıtasıyla çalışmalarını sürdürmektedir. Bu amaç için kurulan Bilgisayar Olaylarına Müdahale Ekibi (BOME) Gebze'de bir danışma/sorun

çözme merkezi olarak çalışmaktadır. Daha yetkin bir merkez olması beklenen Elektronik Ortam Savunma Merkezi ise Ankara'da kurulmaktadır. [361]

10 Aralık 2009 tarihinde Savunma Sanayii İmalatçılar Derneği tarafından Ankara'da düzenlenen "*Sayısal Ortamda Savaş*" sempozyumunda (SOS2009) bilgi savaşı konusunda Türkiye'de ve dünyadaki gelişmeler masaya yatırılmıştır. Bu konuda ortak akıl oluşturması açısından bu sempozyum, gerek sivil gerekse asker katılımcılara Türkiye'nin bilgi savaşı konusundaki çalışmaları açısından yol gösterici olmuştur. [362]

Tehdit kaynakları ne kadar kuvvetli ve becerikli olursa olsun bunlara karşı alınacak önlemler mevcuttur. Teknoloji geliştikçe buna paralel olarak alınan güvenlik önlemleri de geliştirilmektedir. Bir devlet bazında bu konuda atılacak en önemli adım, bilgi güvenliği için politika, prensip, yöntem ve standartların belirlenmesi, tamamen milli olarak gerçekleştirilmesi ve tüm bu faaliyetleri yürütecek bir teşkilatın kurulmasıdır.[363]

Savunma Sanayi, milli teknolojiye dayalı ve bilgi savaşı kapsamında gizlilik nedeniyle mutlaka milli olması gereken savunma sistemlerinin üretilmesine olanak sağlayarak, caydırıcılığa ve devlet güvenliğine katkı sağlayan bir sanayi dalıdır. Türkiye her platformda siber güvenlik alanında kendi fikirlerini ortaya koymakta ve bunları desteklemektedir. 16–18 Kasım 2005 tarihlerinde Tunus'un başkenti Tunus'ta yapılan Dünya Bilgi Toplumu Zirvesi'nde Türkiye, bilgi toplumuna geçişi destekleyici, aynı zamanda bilgi güvenliği ve siber suçlar gibi yeni tehditler karşısında uluslararası işbirliklerinin geliştirilmesi gerektiği belirtmiştir. Ayrıca internet yönetiminin; internetin mevcut güvenliği ve devamlılığından ödün vermeden, çok taraflı, meşru, şeffaf ve katılımcı bir yapıya sahip olması gerektiği, bunun için tüm paydaşların katılım sağlayacağı yeni mekanizmaların geliştirilmesinin uygun olacağını belirtmiştir. [364]

Geleceğin savaşları bilgi savaşları olacaktır ve bilgiyi zamanında elde eden taraf üstünlük sağlayacaktır. Dolayısıyla, savunma sanayinin öncelikli teknoloji alanı bilgi savaşı ile ilgili teknolojiler olmalıdır. Savunma sanayi alanında güçlü olabilmek için yazılım

---

361 ÇAY Ömer, "Bilgi Harbi ve Türkiye", 03.11.2009, http://www.ekopolitik.org/public/news.aspx?id=4348&pid=4082, (e.t. 06.09.2011).

362 Ibid.

363 **Silahlı Kuvvetler Dergisi**, Ekim, 2001, ss., 56–57.

364 **Dünya Bilgi Toplumu Zirvesi**, Tunus, Kasım 2005. http://www.bilgitoplumu.gov.tr/Documents/5/Documents/080100_DBTZNihaiDokumanlari.pdf, (e.t.16.02.2012).

alanındaki bilgiye sahip olunması gerektiği bilinmelidir. Yazılım alanında uzmanlaşmış siber savunma birlikleri bilgi savaşı alanında bizleri son derece kuvvetli kılacaktır.

Örneğin Hürriyet gazetesinin 15 Ocak tarihli bir haberinde[365], "*Anonymous*" adlı grubun, BTK'yı hedef aldığı ve internet sansürüne destek olduğu gerekçesiyle veritabanına saldırarak elde ettiği bilgileri internet üzerinden paylaştığı belirtilmiştir. 25–28 Ocak tarihlerinde 41 kurum ve kuruluşun temsilcilerinin katılımıyla bir tatbikat gerçekleştirilmiştir. "*Ulusal Siber Güvenlik Tatbikatı*" olarak adlandırılan tatbikat sonucu kurumlar siber güvenlik alanında başarısız olmuşlardır. Tatbikat raporuna göre saldırılar, MSB, MGK, BDDK, Ankara Başsavcılığı, MB ve SPK dahil 41 kurumun bilgisayar sisteminin çökmesiyle sonuçlamıştır.

Bu anlamda düşündüğümüzde; ülkemizin e-devlet uygulamalarına açılan kamu hizmetlerinin büyük bir bölümü, bilgi güvenliği yaklaşımından çok uzaktır. Yaşadığımız bilgi güvenliği olaylarına kısaca değinmek gerekirse;

"*KEY ödemeleri için açılan ve sadece TC kimlik numarası ile 8 milyon çalışana ait bilgilerin sorgulandığı web sitesi http://www.keyodemeleri.com ve Resmi Gazete web sitesi aracılığıyla, kişiye özel bilgilerin ortaya serildiği ve diğer ardışık kamu web sitelerinde (SGK vb) yapılan paralel sorgulamalarla tehlikeli bir örnek olduğu söylenmiştir. (Tempo Dergisi, 7 Ağustos 2008, Çırıl çıplağız Röportajı).*"

"*Milli Eğitim Bakanlığı (İLSİS) web sitesinden 687 bin öğretmenin kimlik bilgileri çalınıp, internette dosya paylaşım sitesi Rapidshare yüklendi.(12 Şubat 2009)"*

"*29 Mart 2009 yerel seçimlerinde Yüksek Seçim Kurulunun bilgi sistemlerine yetkisiz bilgisayarlardan oy girilmesi sonucu sistem çöktü.(İstanbul, İzmir, Hatay, Kütahya vb)."*

"*DNA Verileri ve Türkiye Milli DNA Veri Bankası Kanunu ile kurulacak olan Ulusal Gen Bankasına ait bilgilerinde internetten paylaşılacağı ifade ediliyor.*[366]

"*Elektronik Kimlik Doğrulama Sistemi (EKDS) projesi kapsamında geliştirilen yeni T.C. Kimlik Kartı, yakın gelecekte kanuni olarak nüfus cüzdanın yerine geçerek vatandaşlık kartı olarak kullanılacaktır.*[367]"

365 http://www.hurriyet.com.tr/teknoloji/19921755.asp, (e.t. 15.02.2012).
366 http://www.gen.hun.edu.tr/genom, (e.t. 10.09.2012).
367 http://www.ekds.gov.tr/ekds/tanitim.jsp, (e.t. 14.02.2012).

Yukarıda aktardığımız örneklerden de anlaşıldığı üzere Türkiye'nin siber güvenlik alanında uygulamaya koyacağı uygulamalardan belki de en kritik olanı elektronik kimlik kartıdır. TC. Kimlik Kartı; vatandaşa ait nüfus bilgilerinin kartın üzerindeki yonga üzerine güvenli bir şekilde kaydedilmesi ve bu işlemden sonra yetkisiz kimseler tarafından yeniden üretilmesini ya da bilgilerinin değiştirilmesini olanaksız hale getirecek şekilde tasarlanması esasına dayanan, görsel ve mantıksal güvenlik unsurlarına sahip olan bir akıllı karttır. Bununla birlikte TC. Kimlik Kartı, kamu hizmeti sağlayacak kurumların birbirlerine sundukları hizmetlerden faydalanabilmesi için, e-devlet yapısı kapsamında alt yapıyı destekleyecektir.[368]

Siber güvenlik alanında diğer dikkat etmemiz gereken sektör elektrik altyapısı sistemidir. Tüm elektrik altyapısı sisteminin kontrolü Ankara Gölbaşı'nda bulunan Ulusal Kontrol Merkezi'nden yapılmaktadır. Bu merkez Genel Müdürlük binasında bulunan Acil Durum Kontrol Merkezi ile yedeklenmektedir. Hali hazırda Adapazarı, Gölbaşı, İzmir, Keban, İkitelli, Keban Samsun olmak üzere 6 adet bölgesel kontrol merkezi bulunmaktadır. Bölge kontrol merkezleri de elektrik üretim testilerinden aldıkları bilgileri ulusal kontrol merkezine iletmektedir. [369]

2010 yılı itibari ile 235 trafo merkezi ve santral, Ulusal Kontrol Sistemine bağlanmıştır. SCADA Sistemi kapsamında uzaktan kumanda fonksiyonu pilot uygulama olarak 12 istasyonda gerçekleştirilmiş bulunmaktadır. EÜAŞ'a bağlı 51 Hidrolik santral, 20 Termik santral bulunmaktadır. Bunların dışında elektrik üreten birçok kurum ve kuruluştan da elektrik alınmaktadır. [370] Kritik altyapı güvenliği adına Türkiye'nin de kendisini hedef devlet olarak görmesi gerekmektedir.

7.3. TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİSİ

Hazırlanmış olan strateji belgesi ile Türkiye'nin ulusal kapsamda siber güvenliğine yönelik ilkelerini, stratejik hedeflerini, bu hedeflere ulaşmak için ele alınması gereken temel uygulamaları ve ilk planda atması gereken somut adımları belirtilmektedir.[371]

---

368 Ibid.

369 KARA Mehmet, "Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği", http://www.bilgiguvenligi.gov.tr/siber-savunma/elektrik-uretim-ve-dagitim-sistemleri-scada-guvenligi.html, (e.t.06.01.2012).

370 Ibid.

371 Bilgi Güvenliği Derneği (BGD), "Ulusal Siber Güvenlik Stratejisi", Haziran, 2012, http://www.bilgiguvenligi.gov.tr, (e.t. 06.11.2012).

Ülkemizin stratejik yerlerinde görevli çalışanların, bilgilerinin yabancı kurum ve kuruluşların eline geçebileceğini söylemek kehanet olmaz. Ulusal Bilgi Güvenliği yaklaşımını organize edecek merkezi bir kurumun (ABD de bulunan Ulusal Güvenlik Ajansı NSA benzeri) bir an evvel kurulması, tüm kamu kurumları ve özel sektör için bağlayıcı nitelikte bir otorite olması, istihbaratın internetten yapıldığı günümüz de bizleri e-saldırılara karşı güçlü kılacaktır.[372]

Hazırlanan Siber Güvenlik Strateji Belgesi'ne[373] göre siber güvenlik stratejisinin hedefi, bireylerin, şirketlerin ve kamu kuruluşlarının iş ve hizmetlerinde kullandıkları sistem ve altyapıların güvenliğini artırıp, sağlamlaştırmaktır. Böylece bilgisayar ve iletişim ağı altyapıları yasal ve teknolojik açılardan korunurken, toplumsal ve ekonomik düzen de koruma altına alınacaktır. Bu belgede siber güvenlik alanında atılacak önemli adımlardan da bahsedilmektedir. Bir üst kurul olarak "*Ulusal Siber Güvenlik Kurulu*" oluşumu öngörülmekte ve siber güvenlik farkındalığının artırılması amaçlanmaktadır. Diğer taraftan siber güvenlik kültürünün yaygınlaştırılması, kişisel ve kurumsal bilginin korunmasına yönelik daha sıkı tedbirler alınması önemli güvenlik tedbirleri olarak karşımıza çıkmaktadır. Uluslararası işbirliğinin güçlendirilmesi, ulusal siber güvenlik Ar-Ge politikasının oluşturulması ve milli teknolojilerin geliştirilmesinin özendirilmesi konuları da eğitim kurumları ile iş birliği içerisinde geliştirilecek alan içerisinde yer almaktadır. Bu konu ile ilgili Avrupa Konseyi'nin siber suçlar sözleşmesi, uluslararası işbirliğine gidilmesini tavsiye etmektedir.[374] Üniversitelerde bilimsel çalışmaların arttırılmasına yönelik çalışmalar, insan kaynakları yetiştirilmesine ve mevcutların geliştirilmesine yönelik çalışmalar, kurumsal siber güvenlik yeteneklerin arttırılmasına yönelik çalışmalar, kurumlara siber güvenlik sızma testleri yapan bağımsız merkezlerin kurulması, yasal mevzuatın düzenlenmesi gibi birçok maddeyi ekleyerek siber güvenlik alanında eksikliklerimizi tespit edebilmemiz mümkündür.

Bu anlamda Ulaştırma Denizcilik ve Haberleşme Bakanlığı önderliğinde Ulusal Siber Güvenlik Stratejisi baz alınarak gerekli çalışmaların yapılacağı belirtilmektedir.

---

372 CEYLAN Cenk, Ulusal Güvenliğin Zayıf Halkası E-devlet, Turkish Forensic / GÖKTÜRK BT Ltd, 11.06.2009, http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/ulusal-guvenligin-zayif-halkasi-e-devlet.html, (e.t. 10.09.2011).

373 http://www.sabah.com.tr/Ekonomi/2012/07/17/ulusal-siber-guvenlik-stratejisi-hazirlandi (e.t.23.07.2012).

374 Avrupa Konseyi Siber Suçlar Sözleşmesi, (Convention on Cybercrime), www.imef.org.tr, (e.t. 01.11.2012).

Hazırlanmış olan Siber Güvenlik Stratejisi Belgesi'ne [375] göre;

- "*Ulusal siber güvenliğin sağlanması noktasında; hukuki düzenlemelerin hazırlanması,*

- *Siber güvenlik kapsamında devlet kapasite ve yeteneklerinin arttırılmasına yönelik çalışmalar yapılması,*

- *Politika, düzenleme ve denetleme işlerini yerine getirecek kurumsal yapıların belirlenmesi,*

- *Her seviyede bilgilendirme ve bilinçlendirme çalışmalarının gerçekleştirilmesi,*

- *Kritik altyapıların tanımlanması, bu altyapıların güvenliğinin risk tabanlı bir yaklaşımla sağlanması,*

- *Gerek ulusal gerekse uluslararası boyutta işbirliği ve eşgüdümün sağlanması gerekmektedir*."

Ayrıca Siber Güvenlik Strateji Belgesi'ne[376] göre aşağıdaki hedefler belirlenmiştir;

- "*Kritik altyapıları belirlemek,*

- *Siber güvenlik konusunda bilgilendirmeler yapmak,*

- *Siber güvenlik konusunda mümkün olduğu kadar milli teknolojileri kullanmak,*

- *İlgili yasal mevzuatı geliştirmek,*

- *Siber güvenlik uzmanları yetiştirmek,*

- *Ulusal Siber Güvenlik Danışma Kurulu oluşturmak,*

- *Siber saldırılara karşı ulusal eşgüdümü sağlamak için görevli merkezler kurmak,*

- *Uluslararası kurumlar ile yakın işbirliği içinde olmak,"*

---

375 http://www.sabah.com.tr/Ekonomi/2012/07/17/ulusal-siber-guvenlik-stratejisi-hazirlandi (e.t.23.07.2012).

376 BGD, loc.cit.

Kurumların internetten elde ettiği istihbarat akışının, stratejik olarak bilgiye çevrilmesi, merkezi e-devlet saldırılarına karşı, ülkemizin savunmasını güçlendirecektir. İnsanların gen haritalarının çözüldüğü günümüzde, ulusal bilgilerimizin arasında bulunan kan bilgilerimiz ve yeni kurulmakta olan gen bankası bilgilerinin, e-devlet uygulamalarıyla çalınması, ülkemizi olası biyolojik bir saldırı karşısında, savunmasız bırakabilir.[377]

Devletin şeffaflaşması adına, stratejik olarak bilgi güvenliği analizi yapılmadan vatandaşlara ait verilerin e-devlet uygulamalarıyla paylaşılması, ulusal güvenliğimizi tehlikeye sokabilmektedir. Başlangıçta e-devletin kolaylaştırıcı etkisi, e-savunma stratejisi oluşturulmamış projelerde ciddi kayıplara yol açabilmektedir. Günümüzde askeri savaş doktirinlerinde, siber saldırı tekniklerinin test aşamasından çıkıp, olgunlaşmaya başladığı görülebilmektedir. Dünya, uydulardan gözlenmekte, coğrafi bilgi sistemleriyle kuşatılmakta, tüm ağlar internetle bağlanmaktadır. Orduların operasyonel üstünlükleri, bilgi teknolojilerinin stratejik olarak kullanılmasıyla artmaktadır. İnternetten sunulan haritalarda, insanların her şeyin yerini işaretlediği ve farkında olmadan, bir devletin savaş öncesi keşfine yarayacak derece coğrafi bilgi sistemi destekli lojistik sağladığını ifade etmek, paranoya değildir. E-devlet uygulamalarından kaynaklanan güvenlik açıkları ve e-saldırılar sonucu, elde edilecek stratejik bilgiler, veri madenciliği analizleriyle oldukça tehlikeli sonuçlar verebilmektedir. Siber savaşı planlayan ve yürütenlerin, günümüzde devletin zayıf yönleri olarak, e-devlet uygulamalarını hedef seçmektedir. Bu nedenle devlet olarak siber savunmamızı oluşturmamız gerekmektedir. [378]

İran gibi bir devletin, kendisine satışı yasak olan ABD teknolojisi Windows işletim sistemini ve kapalı kaynak kodları olan Siemens Simatic PLC yazılımlarını ve donanım sistemlerini kullanarak, çekirdek enerjisi santrali inşaa etmesine karşı olan devletler tarafından, siber savaş yöntemleriyle sekteye uğratılması, hemen yanı başında 2 tane nükleer santral inşaa edecek olan Türkiye'yi yakından ilgilendirmektedir. Çekirdek enerjisi üretme amacıyla, Sinop ve Mersin de inşaa edilmesi planlanan nükleer santrallerin güvenliği için, şimdiden SCADA sistemleriyle ilgili çalışma başlatılması; Türkiye'nin ulusal çıkarları için çok önemlidir. Siber savaş cephesi olarak SCADA sistemlerin hedef seçilmesi, insanlık ve dünya için çok ağır sonuçlara sebep olabilir. Bir devleti veya bir bölgeyi, sular altında bırakabilir. Kışın ortasında gazsız, elektriksiz ve susuz kalabiliriz. Yangın, çevre zararı ve

377 Ibid.
378 Ibid.

maddi kayıp gibi telafisi çok zor yapay afetler oluşturabilir, hatta radyasyona bile maruz bırakabilir.[379]

Ülkemizde bilişim ve internet ortamında işlenen suçlar ile ilgili mevcut mevzuat değerlendirildiğinde, 5237 sayılı "*Türk Ceza Kanunu*", 5651 sayılı "*İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*", 5070 sayılı "*Elektronik İmza Kanunu*" gibi kanunlar ve ilgili yönetmeliklerle siber güvenlik hukuku altyapısının desteklendiği fakat sadece bu düzenlemelerle günümüz ihtiyaçlarının tümüyle karşılanmasının mümkün olmadığı değerlendirilmektedir.

7.4. SİBER GÜVENLİK TATBİKATLARI

Siber güvenlik alanında bilgi ve tecrübe aktarımı, mevcut verilerin ve saldırı analizlerinin yapılması adına ulusal-uluslararası tatbikatlar yapılmaktadır. Türkiye kendi içerisinde bu tatbikatları özellikle TUBİTAK önderliğinde yapmaya başlamıştır. Tabi ki şu anda tatbikatlar emekleme safhasındadır. Uluslararası alanda yapılacak tatbikatlar ile kendi bilgi ve tecrübelerini aynı zamanda kalifiye elemanlarını oluşturacaktır. Siber güvenlik tatbikatlarının amaçlarına değinmek gerekirse[380];

- "*Bilgi sistemlerini hedef alabilecek saldırılara karşı hazırlıklı olmak,*
- *Saldırılara karşı kurum içi politikaları ve karar destek mekanizmalarını değerlendirmek,*
- *Kurumlar arası bilgi paylaşımını, haberleşmeyi ve koordinasyonu test etmek,*
- *Olası bir saldırıdan sonra geri kurtarma planlarını test etmek ve*
- *Tehditlere ve açıklıklara karşı farkındalık oluşturmak,*
- *Personeli eğitmek olarak sıralanabilir."*

Şimdiye kadar yapılan tatbikatları amaçları ve katılımcılar olarak kısaca değerlendirirsek;

379 Ibid.
380 TATAR Ünal, **Dünyada ve Türkiye'de Siber Güvenlik Tatbikatları**, Ankara, Haziran 2011.

7.4.1. Bome 2008 Tatbikatı

7.4.2. Amaçları

- ✓ "*Kurumsal BOME süreçlerinin kontrol edilmesi,*
- ✓ *TR-BOME işbirliği süreçlerinin kontrol edilmesi,*
- ✓ *Olay Müdahale sürecindeki eksikliklerin ortaya çıkartılması*"

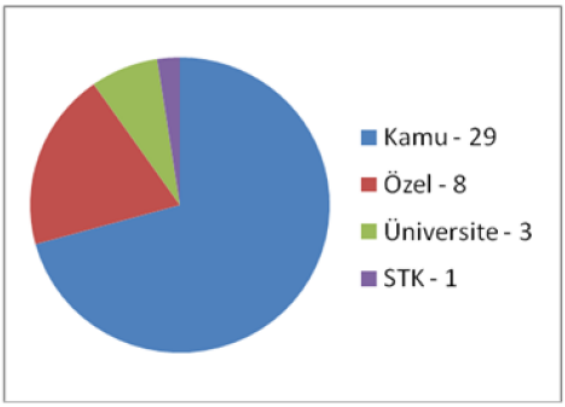
BOME 2008 Katılımcıları;

Cumhurbaşkanlığı, Başbakanlık, Adalet Bakanlığı, Hazine Müsteşarlığı, Sayıştay Başkanlığı, Merkez Bankası, Sermaye Piyasası Kurulu, Tapu Kadastro Genel Müdürlüğü

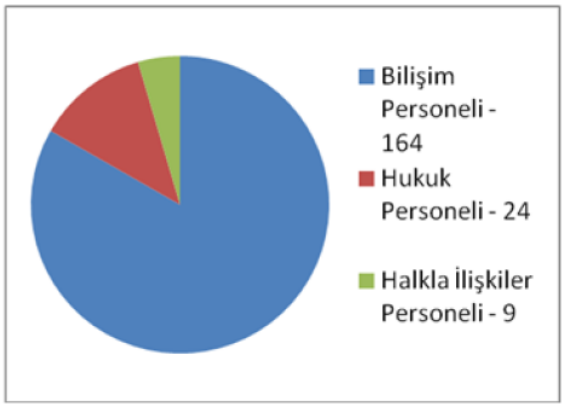
7.4.3. Ulusal Siber Güvenlik Tatbikatı (USGT) 2011

TÜBİTAK BİLGEM ve BTK koordinasyonunda 39 kurum/kuruluşun katılımıyla 25-28 Ocak 2011 tarihlerinde gerçekleştirilmiştir. USGT 2011 ile, gün geçtikçe daha somut bir tehlike haline gelen siber tehditlere karşı hazırlıklı olunması, kurumların bilgi sistemi güvenliği olaylarına müdahale ve kurumlar arası koordinasyon yeteneklerinin tespit edilmesi, kurumlar arası iletişimin arttırılması, bilgi ve tecrübe paylaşımının ve ulusal siber güvenlik bilincinin arttırılması amaçlanmıştır.[381] TÜBİTAK BİLGEM ve BTK düzenleyici kurumlar olmak üzere 39 kurum ve kuruluşun katılımıyla gerçekleştirilmiştir.

[381] Ibid.



Sektör Bazında Katılımcı Kurum ve Kuruluşların Profili



Kurum Temsilcilerinin Uzmanlık Bazında Profili

Şekil-9 Ulusal Siber Güvenlik Tatbikatına Katılanlar

Kaynak: TATAR Ünal, Dünyada ve Türkiye'de Siber Güvenlik Tatbikatları, Ankara, Haziran 2011.

7.4.4. Ulusal Siber Güvenlik Tatbikatı Uygulama Konuları

"*1.Kurumun resmi web sayfasının içeriğinin yetkisiz kişilerce değiştirilmesi,*

2.Kuruma ait bir IP adresinden başka bir kurum/kuruluşa DDoS saldırısı yapıldığının tespit edilmesi,

3.Kuruma ait bir IP adresinden başka bir kurum/kuruluşa spam mesajlar gönderildiğinin tespit edilmesi,

4.Kuruma başka bir kaynaktan DDoS saldırısı yapılması,

5.Kurumdan ayrılan kötü niyetli bir personelin ayrılmadan önce veritabanına zarar vermesi,

6.Kuruma ait sistemlere İnternet üzerinden yayılan bir solucanın bulaşması,

7.Telefon yoluyla kurumda çalışan personelden bilgi çalma girişimi,

8.Elektronik posta yoluyla kurumda çalışan personelden bilgi çalma girişimi

9.Kurum çalışanlarından biri tarafından 5651 sayılı kanun kapsamında erişimi engellenen bir siteye giriş yapıldığının tespit edilmesi,

10.Kuruma aitmiş gibi görünen sahte bir web sitesinden "spam" mesajlar gönderildiğinin tespit edilmesi,

11.İzinsiz yapılan bir kazı neticesinde kurumun internet bağlantısını sağlayan fiber hattının kopartılması,

12.Sistem odasında bulunan soğutma sisteminin mesai saati dışında bir saatte arızalanması,

13.Kurumun bulunduğu bölgede elektrik kesintisi yaşanmasına rağmen jeneratör sisteminin devreye girmemesi

14.Kurum içinde ismi kolaylıkla tahmin edilerek bağlanılabilinen bir kablosuz ağ erişim noktasının tespit edilmesi,"[382]

Siber güvenlik konusunda durum tespiti, olası saldırılara karşı hazırlıklı olmak, iletişim kanallarını kontrol etmek ve farkındalık oluşturmak gibi amaçlarla düzenlenen siber güvenlik tatbikatlarına verilen önem artmaktadır. Gerek kurum içi gerekse kurumlar arası koordinasyon ve olay müdahale yeteneğine katkı sağlayacak olan siber güvenlik tatbikatlarının ülkemizde de 2008 ve 2011 yıllarında yapılmıştır. Siber güvenlik tatbikatlarının hem ulusal çapta devam etmesi hem de kurumsal ve sektörel çapta tatbikatların düzenlenmeye başlanmasının ülkemize fayda sağlayacağı değerlendirilmektedir.[383]

7.5. SİBER KUVVET KOMUTANLIĞI

Gelecek harekâtlar bilgiye dayandığı için bugünün harekâtlarında kullanılan ara hatları ve muharebe düzenleri gibi sınırlamalar kullanılmayacaktır. Konvansiyonel Savaş içerisinde mevcut olan bütün kuralları, savaş prensiplerinin yeniden yorumlanması, yeni tanımların sisteme dahil edilmesi gerekmektedir. Tarihinde her türlü görevi başarılı bir şekilde yürüten TSK, Bilgi Savaşı konusunda da kendisine verilen görevleri en iyi şekilde yerine getirecektir.

Teknolojik üstünlüğe sahip devletlerin orduları, sayısal üstünlük yerine nitelik açısından bir üstünlüğü tercih etmektedirler. Teknolojide meydana gelen gelişmeler geleceğin

382 Ibid.
383 Ibid.

savaşlarında siber saldırı ve savunma imkânlarının her türlü durumda kullanılacağını göstermektedir. Günümüzde olabilecek bir savaşta insan ve malzeme kaybının en az seviyede olması özellikle istenen bir durumdur. Bu bakımdan istenen kriterlerin yakalanabilmesi ve verilecek görevlerin başarılabilmesi için teknolojinin yakından takip edilmesi ve gereken siber saldırı ve savunma imkânlarının sisteme dâhil edilmesi gerekmektedir.

Silahlı Kuvvetler bilgi, temel olarak, komuta kontrol maksatları için kullanılmaktadır. Komuta kontrol sistemlerine sağlanan bilgi akışının güvenilirliği ve yeterliliği Silahlı Kuvvetlerin muharebe sahasındaki başarısı ile doğru orantılı olacaktır. Bu bağlamda bilgi akışının güvenilirliği ve yeterliliği bilgi savaşlarının hedefi olacaktır.

ABD, İngiltere, hatta Fransa gibi NATO devletleri artık kendi siber güvenlik birimlerini kurduklarını açıklamışlardır. Türkiye, siber savunmada en iyi durumdaki üye devletlerin kaynaklarını kullanarak bir koordinasyon merkezi görevi alabilmelidir ve bulunduğu bölgede siber bölgesel güç olabilecek potansiyele sahiptir. Türkiye NATO seviyesinde siber savaş kapsamında yürütülen faaliyetler çerçevesinde üzerine düşen sorumlulukları yerine getirmesi gerekmektedir. Bu kapsamda, NATO savunma planlama ihtiyaçlarını göz önünde bulundurmak ve bunlara uygun şekilde milli planlamalar yapmalıdır.[384] Ayrıca Harekât ve tatbikatlarda NATO Bilgi Harekâtını destekleyecek eğitimli personel ve kaynak sağlamak, diğer müttefiklerle birlikte Türkiye'nin de üzerine düşen sorumluluklardır.[385]

Diğer taraftan günümüzde küresel ortak bir siber savunma sistemine gereksinim vardır. Siber saldırı yapıldığında uluslararası iletişim şebekeleri kullanılabilmektedir. Siber uzaydaki mücadele artık devletler boyutuna ve politik alanlara yönelme eğilimi göstermektedir. Estonya bunun iyi bir örneğidir. Bazı devletlerin siber saldırı, sızma ve casusluk yetenekleri kazandıkları ve bunları artan oranda kullandıkları bilinmektedir. Ellerinde en ileri seviyede teknolojik cihaz ve altyapı bulunmaktadır. Bunlara karşı savunma yapmak gerçekten oldukça zordur. Çünkü politik açıdan da koruma altındadırlar. Siber saldırıların tespiti ve sonuçlandırılması genellikle politik gerekçelerle belli bir noktadan sonra bitmektedir.[386]

---

384 Türk Silahlı Kuvvetleri (TSK), **Türk Silahlı Kuvvetleri Bilgi Harbine Nasıl Hazırlanmalıdır?**, Harp Akademileri Basım Evi, Yenilevent , İstanbul, Nisan, 1999, s.84.

385 MCM-069-98 (NATO Bilgi Harekatı Konsepti).

386 BUKSUR Resul, "NATO'nun ODTÜ'lü Siber Savaş Komutanı", Röportaj, 20 Ekim 2010, http://www.ntvmsnbc.com/id/25142902/#storyContinued, (e.t. 30.07.2012).

ABD, İngiltere ve Fransa gibi siber savunma gücü oluşturduğunu resmen açıklayan devletlere baktığımızda savunmanın ötesinde saldırı amaçlı birimleri de hayata geçirdikleri ve zaman zaman bu yeteneklerini kullandıkları açıktır. Birçok devlet de siber saldırı yeteneklerini gizlice geliştirmiştir. Bu yüzden politik siber çatışmalar önümüzdeki yıllarda yoğunlaşma potansiyeli taşıyor. Küçük bir devlet dünyanın öteki ucundaki büyük bir devletin internet, finans, medya, hatta enerji sistemini gibi kritik alt yapılarını işlemez hale getirebilir. Bu durum siber savaşın asimetrik bir savaş olduğunun göstergesidir.[387]

Türkiye'de TÜBİTAK bünyesinde kurulmuş bir siber savunma birimi bulunmaktadır. Türkiye'nin teknik bir kapasitesi vardır. Ama siber savunma konusunda henüz yasal düzenlemeleriyle birlikte milli siber güvenlik stratejisi bulunmamaktadır. Türk Silahlı Kuvvetleri'nde ise Kara Kuvvetleri Komutanlığı bünyesinde oluşturulan "*Siber Savunma Şube Müdürlü*ğü" kurulmuştur. Bu şube şu an için gelecekte kurulması planlanan "*Siber Kuvvet Komutanlığı*"na alt yapı olması için oluşturulmuştur.

Türkiye geleceğe yönelik olarak yapacağı tehdit değerlendirmelerinde kendi etki sahasını genişleterek herhangi bir düşmandan gelebilecek siber saldırı tehdidine karşı siber savunma yapabilecek yeterliliğe sahip olmalıdır.[388] Bundan daha önemlisi gelebilecek siber saldırıları önceden değerlendirmeli, buna uygun siber savunma yöntemleri geliştirmelidir. Siber saldırı için uygun koşul ve şartlar oluşması durumunda proaktif bir yaklaşımla hedefe yönelik saldırılar yapmak için tüm imkânlarını kullanmalıdır.

Türkiye için tehdit olarak devletin bilgi altyapısı düşünülmektedir. Bu altyapının temel yapı taşlarını, *"kamu ve özel sektörün tüm faaliyetleri; yönetim, bankacılık, üretim, ulaşım, lojistik, ödemeler, diğer parasal konular, insan gücü, personel faaliyetleri, eğitim elemanları, askeri tesisler, TSK kabiliyetleri*" vb. unsurları kapsamaktadır.[389]

Bilgi Savaşı'na hazırlanan TSK subay lider kadrosunda belli başlı özellikler olmalıdır. Bu özelliklere değinmek gerekirse; "*başarılı elektronik lider, geleneksel liderle karşılaştırıldığında bilgi, beceri ve davranışlarda sistematik farklılıklar ortaya çıkmıştır. Elektronik liderler elektronik iletişim yollarının kullanılmasında model olmalıdır. Elektronik ağla ve bu ağ vasıtasıyla çalışırken rahat olmalıdır. Elektronik liderlerin neler olup bittiğini hızla anlayabilmeleri gerekmektedir. Yapılması gereken şeyler konusunda açık bir önseziye*

387 Ibid.
388 TSK, loc.cit.
389 Ibid., s.131.

sahip olmalıdırlar. Küresel ağlarda zaman bölgelerini, ulusal tatil günlerini, kültürel farklılıkları ve yerel ihtiyaçlardan doğan baskı ve zorunlulukları göz önünde bulundurmalıdırlar. Elektronik liderler hem elektronik teknolojinin nasıl kullanılacağını hem de gruplarını bu teknolojiyi kullanmaya nasıl teşvik edeceklerini bilmelidirler. Elektronik liderler bilgi üretimindeki sorumluluklar ve güvenilirlik konularında bilgi ağlarında ortaya çıkan anlaşmazlıklardan nasıl kaçınacaklarını veya bunları nasıl çözeceklerini bilmelidirler."[390]

"*Geleceğin çok boyutlu harekât kavramı; bugünden geleceği görebilen ve hazırlıklarını da çok boyutlu sürdürebilen liderlere ihtiyaç göstermektedir. Bu unsurlarının kalitesini yükseltebilen devletler, mutlaka gelecekte daha kaliteli bir yaşam olanağını; bunu başaramayanlar aleyhine elde edeceklerdir*."[391]

TSK'nin önümüzdeki yıllarda kazanacağı yeni yeteneklerin etkin kullanılabilmesi için işlemlerde, eğitimde ve teçhizatta standartlığın sağlanması yanında, bilgi sistemlerinin beka kabiliyeti yüksek, güvenilir, esnek ve gerçek zamanlı bilgi alışverişine imkân veren bir yapıda olması ve sivil asker bütün kaynakların bu maksatla koordineli bir şekilde kullanılması öngörülmektedir.[392]

TSK, ulusal bilgi harbini uygulayacak en önemli kurumdur. Bu uygulama ulusal bilgi harbini tamamlayıcı ve en başta ulusal siber saldırı imkânlarını kullanma tarzında olmalıdır. Ulusal bilgi harbinde verilecek görevin en etkin bir şekilde yerine getirilebilmesi için sahip olunması gereken imkân kabiliyetler belirlenmelidir. Bu imkân kabiliyetlerin hedefe yönlendirilmesi için kuvvetler arası koordinasyon esasları tespit edilmelidir. Kuruluş, malzeme ve eğitim ihtiyaçlarının karşılanması ve etkinliğin arttırılması maksadıyla diğer milli güç unsurları ile işbirliği içerisinde çalışılmalıdır.

Bu ve benzeri nedenlerden dolayı, Siber Kuvvet Komutanlığı asker ihtiyacını karşılamaya en uygun modelin benim tabirimle "*E-Mehmetçik*" kuvvetler olarak önceden eğitime alınması ve hizmet ihtiyacı olduğunda göreve çağrılmasıdır. Siber çatışmanın doğasında yer alan belirsizlik, zorunlu askerliği veya asker ihtiyacı için askere çağırma hakkında sorunları ortaya çıkarır. Ne yazık ki, deneyimler saldırı sonlandıktan çok sonra bile

---

390 BASS Bernard, "Bilgi Çağı ve Teknolojik Gelişmeler Işığında Yönetici ve Lidere Karşılaştırmalı Bir Bakış", **Üçüncü Uluslararası Sempozyum Bildirileri**, Genelkurmay Basım Evi, İstanbul, 12–13 Mayıs 2005, SAREM, s.168.

391 KUBAT Erhan, "Gelecekteki Çok Boyutlu Harekât", **Harp Akademileri Bülteni**, Mart, 2004.

392 Ibid.

saldırının kaynağının ve gerçek destekleyicisinin kim olduğunun bulunamadığını göstermiştir. Siber saldırı tamamen farklı bir durum olduğu için normal askere alım sürecinden farklı işlemesi gerekir. BT personelini seçerken aldığı eğitim, iş tecrübesi, değişik platformlara ve yazılımlara olan aşinalığı hakkındaki bilgiler önem taşır. Bu nedenle askerliğe alım süreci daha uzun, planlı ve takım halinde aynı anda çalışma gerektireceği için belli bir kurumu ya da şirketi askere çağırma şeklinde yürütülebilir. Siber saldırılar değişik alanlarda olabileceği için farklı konularda uzman BT çalışanları almak ve bu kişileri geleneksel olmayan taktiklere ve çalışma koşullarına hazır hale getirmek gerekir. [393]

Türk Silahlı Kuvvetleri'nin mevcut durumu incelendiğinde çağımızın teknolojisine uygun, gelecekteki bilgi muharebe ortamına yönelik bir teşkilat, teçhizat ve imkânlara henüz sahip olmadığı görülmektedir. Buna yönelik çalışmalar devam etmekle beraber bu çalışmaların hızının sürekli gelişen teknolojiyle paralellikte güçlükler olduğu görülmektedir. Bu çalışmaların artırılarak, bilimsel teknolojiye uygun şekilde yürütülmesi son derece önemlidir.

Sonuç

Çalışmamızın bütünlüğü içinde analiz ettiğimiz üzere internetin hızla yayılması ile beraber siber uzayda meydana gelen güvenlik ihlalleri de çoğalmıştır. Bu gelişme ile paralel olarak teknolojik aygıtlar bireylerin hayatlarının her alanında olduğu gibi devletlerin de kritik altyapılarına entegre olmuştur. Diğer bir ifade ile vurgularsak siber uzaydaki güvenlik ihlalleri bireysel olarak bizleri etkilediği gibi devletlerin de güvenliğini etkilemeye başlamıştır.

Bu bağlamda devletler tarafından üretilen ve envanterlerde yer alan konvansiyonel silahların yanı sıra artık siber silahlarda savaş alanında ki yerini almıştır. ABD ordusu kara, deniz ve hava kuvvetleri içerisinde siber güç kuvvetlerini oluşturmuştur. Diğer devletler de benzer şekillerde ordularını yapılandırmışlardır. Siber güç unsurları on binlerle ifade edilen azımsanmayacak rakamlar ile ifade edilmektedir ve bu birimlerin görevi gerekli yer ve zamanda siber saldırı ve savunma yapmaktır. Fakat çoğu zaman bir siber saldırıda saldırganın kim veya kimler olduğu bilinememekte ve yeri tam olarak tespit edilememektedir. Bu özelliklerinden dolayı siber saldırı olayları sonrası çok ayrıntılı ve uzun süreli çalışmalar yapılması gerekmektedir. Ayrıca çoğu zaman siber saldırılar sonrasında uluslararası bir olayla

393 Ibid.

ve faillerle karşı karşıya kalınmaktadır. İran nükleer tesislerine Stuxnet zararlı yazılımı ile yapılan saldırı bu duruma en iyi örnek olarak karşımıza çıkmaktadır.

Siber saldırı ve savunma yetenekleri de devletler adına beklenmeyen sonuçlar doğurmuştur. Siber saldırı anlamında daha güçlü gözüken devletler (örneğin ABD ve Çin) aslında siber saldırıya maruz kalma yönünden en hassas devletler olabilmektedir. Bu durum, devletler için silahlı güç unsurlarını kıyaslarken sayısal olarak yapılacak hesaba siber güç unsurlarını da katmasını gerekli kılmaktadır. Siber uzayın doğası ise devletleri çoğu zaman asimetrik bir saldırı ve savunma ile karşı karşıya bırakmaktadır ve bundan dolayı bireysel olarak bir devlete zarar vermek siber uzayda mümkündür.

Siber uzayda meydan gelen güvenlik ile ilgili olaylara teorik olarak baktığımızda ise hala tam olarak netleştirilemeyen ve tanımlanmayan çok sayıda sorunun olduğu tespit edilmektedir. Siber saldırının tam olarak ne zaman başladığı? Siber saldırının hangi şartta kişisel veya kurumsal hakları ihlal edeceği? Bir devletin egemenliğinin siber uzayda nerede başlayacağı? Siber uzaydaki bir sorunun ne zaman uluslararası bir sorun haline geleceği? Bireyin siber uzayda nasıl korunacağı ve kim tarafından temsil edileceği? gibi buna benzer soruları uzatmak mümkündür. Özellikle uluslararası arenada bütün bu soruların cevabını ortak bir irade ile cevaplamaksa son derece güçtür ve siber uzay bu yönüyle ileride şimdiden tahminde bulunamayacağımız sorunları da gündeme getirecektir.

Siber terörizm ise çağımızın yeni terör saldırı şekli olmuştur. Siber uzayın imkânları devletlerin olduğu kadar terörist oluşumlarında dikkatini çekmiştir. Mevcut terör tanımlarında ve terörizmin her türlü şekline karşı mücadele de ortak hareket edemeyen dünya, siber terör noktasında da ortak bir akıl ortaya koyamamıştır. Bu sebeple oluşturulacak güvenlik kurulları veya organizasyonlar vasıtası ile en kısa sürede terörist oluşumların siber uzayın sınırsız imkânlarından rahat bir şekilde faydalanmasının önüne geçilmelidir.

Günümüzün savaş konseptleri ise siber uzayın sınırsız harekât alanı içerisinde geçerliliğini yitirmiştir. Yeni tanımlara ve askeri birlikler için yeni yapılanmalara ihtiyaç vardır. Şüphesiz siber uzay içerisinde askeri bir kabiliyetten söz ettiğimizde en önemli unsur olarak karşımıza, siber uzayın imkânlarını kullanan ve mevcut savaş sahasına siber silahlarını adapte eden tek başına bir asker çıkmaktadır. Bu sebeple askerin konu ile ilgili bireysel eğitimleri son derece önemlidir. Diğer bir deyişle devletler arası anlaşmazlıkların çözülmesi için orduların ve silahların caydırıcı bir güç olarak kullanılması taktiğine, sanal orduların ve

saldırılarında dâhil edilmesi gerekmektedir. Zira devletlerin, kamu, özel sektör ve askeri haberleşmelerinin, internetten geçtiği ve bu trafiğin süzülerek bilgilerin tekrar elde edilebildiği unutulmamalıdır.

Madalyonun diğer tarafından bakıldığında ise siber uzay kullanıcılarının da sanal ortamda gezinirken uyması gereken kurallar olmalıdır. Fakat bu tarz genel kuralların olmaması ayrı bir sorunu oluşturmaktadır. Bu sebeple kullanıcıların siber uzayın kuralları, siber uzayın faydalarının yanında ne gibi sorumluluklar da getirdiği, olası yanlış kullanımdan doğabilecek sorumluluklar konularında bilgilendirilmeleri gerekmektedir. Unutulmamalıdır ki e-ticaret, e-devlet, e-finans gibi birçok alanda yaşanan gelişmeler siber güvenlik ve bu anlamda oluşabilecek suçlara karşı devletlerin iş birliği içinde çalışmasını zorunlu kılmaktadır. İşte tam bu noktada, e-devlet uygulamaları çok stratejik hale gelmektedir. Özellikle devletlerin kritik altyapılarının güvenliği, ulus güvenlik noktasında önemlidir. Zira bilindiği üzere herhangi bir konuda hukuksal bir düzenleme olmadığı zaman doğal olarak ihlal ve suç da oluşmamaktadır. Yasal olarak siber saldırılar ile ilgili hala yeterli yasal düzenlemenin birçok devlette yapılmamış olması siber saldırganların yakalanmasını zorlaştırmaktadır. Siber saldırıların çoğu zaman başka devletten gerçekleşmesi ise uluslararası bir yapının ve yasaların olmasını zorunlu kılmaktadır.

Bizce bu kapsamda belirtilmesi gereken son husus, siber terörizmle mücadeleye bilgisayar dâhileri de dâhil edilmesidir. Çünkü bilgi ve becerileri olmaksızın siber terörizmle mücadele etmek mümkün olmayacaktır ve ancak teröristlerin sahip oldukları imkân ve kabiliyetlerden daha fazlasını barındıran kaynaklar elde edilemez ise bu durum sadece hükümet sistemlerinin değil aynı zamanda sosyal sistemin zafiyetini artıracaktır.

Siber güvenlik konusunu Türkiye açısından analiz edildiğinde ise bulunduğu coğrafya itibarıyla ve bilgi sistemleri alt yapısına yapmış olduğu yatırımlar sonucu siber saldırılara maruz kalma riski en yüksek olan devletlerden birisi olduğu görülmektedir. "*Siber savunma*" ya da "*siber komutanlık*" hususlarının çok büyük önem arz ettiği Türkiye siber güvenlik alanında fikir alış verişini, kendi iç dinamikleri ve uluslararası yapılar ile ortaklaşa yaptıkları çalışmalar sonucu belli bir seviyeye getirmiştir. Fakat gerekli kurumların bir an önce oluşturulması ve bu kurumları koordine edecek bir üst yapılanmanın kurulması hususunda önemli eksiklikler bulunmaktadır.

TSK’nin mevcut durumu incelendiğinde ise çağımızın teknolojisine uygun, gelecekteki bilgi muharebe ortamına yönelik bir teşkilat, teçhizat ve imkânlara henüz sahip olmadığı görülmektedir. Buna yönelik çalışmalar devam etmekle beraber bu çalışmaların hızının sürekli gelişen teknolojiyle paralellikte güçlükler olduğu görülmektedir. Bu çalışmaların artırılarak, bilimsel teknolojiye uygun şekilde yürütülmesi son derece önemlidir. Diğer bir deyişle vurgularsak TSK siber dünyada savunma ve saldırı unsurlarını en kısa sürede oluşturmalı, konu ile ilgili mevcut uluslararası organizasyonlar ile ortaklaşa tatbikatlar yapmalıdır. Genç ve dinamik Türkiye nüfusu bunun için yeterlidir. TSK’ndeki bu oluşum mevcut askerlik hizmetinde de radikal değişikliklere sebep olabilecektir. Örneğin Harp Akademileri'nde, sanal savaş ve savunma anlayışı konusunda bölümler açılabilir ve askeri bir taktik olarak benimsenebilir.

Bu kapsamda belirtilmesi gereken son husus, geleceğin savaşlarının bilgi savaşları olacağı ve bilgiyi zamanında elde eden tarafın üstünlük sağlayacağıdır. Dolayısıyla, savunma sanayinin öncelikli teknoloji alanı bilgi savaşı ile ilgili teknolojiler olmalıdır. Savunma sanayi alanında güçlü olabilmek için yazılım alanındaki bilgiye sahip olunması gerektiği bilinmelidir. Yazılım alanında uzmanlaşmış siber savunma birlikleri ise bilgi savaşı alanında devletleri son derece kuvvetli kılacaktır.

KAYNAKLAR

Kitaplar

ANDRESS Jasan, Steve WINTERFELD**, Cyber Warfare:Teckniques, Tactics and Tools for Security Practitioners**, Syngress, 1 ed.

ARI Tayyar, **Uluslararası İlişkiler Teorileri: Çatışma, Hegemonya, İşbirliği**, 2010, 6.Baskı, MKM Yayıncılık.

AYDIN Mehmet S., "Küreselleşmeye Genel Bir Bakış", **Siyasi, Ekonomik Ve Kültürel Boyutlarıyla Küreselleşme**, Mehmet S. AYDIN, Mustafa ERDOĞAN, Ali Yaşar SARIBAY, Süleyman Hayri BOLAY- Mehmet ALTAN, Ufuk Kitapları, İstanbul 2002.

BUZAN Barry, Ole WEAVER, Jaap de WILDE, **Security: A New Framework for Analysis. Boulder**, Lynne Rienner Publishers, 1998, http://books.google.com.tr, (e.t. 31.12.2011).

BUZAN Barry, **The United States and the Great Powers: World Politics in the Twenty-First Century**, Cambridge, 2004, Polity Press. Cambridge University Press, http://books.google.com.tr, (e.t. 31.12.2011).

CLARK Richard A., Robert K. KNAKE, Siber Savaş, Çeviren Murat ERDURAN, İstanbul Kültür Üniversitesi, İKÜ Yayın Evi, 2010.

COLLINS Alan, **Contemporary Security Studies,** 2007, Oxford, Oxford University Press, http://books.google.com.tr, (e.t. 31.12.2011).

CSTB (Computer Science and Telecommunications Board), 1991, "**Computers at Risk: Safe Computing in the Information Age**", Washington, DC, National Academy Press, http://www.nap.edu/openbook.php?record_id=1581&page=7, (e.t. 31.12.2011).

DENNING Dorothy E, "Cyber terrorism. Testimony before the Special Oversight Panel on Terrorism," **Committee on Armed Services U.S. House of Representatives**, Georgetown University, May 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, (e.t. 10.08.2010).

DENNING Dorothy E., **Information Warfare and Security**, 1999, Addison - Wesley.

DERIAN James Der , **Antidiplomacy: Spies, Terror, Speed, and War**, 1992, Oxford, Basil Blackwell.

DRUCKER Peter F., **Kapitalist Ötesi Toplum**, Çeviren: Belkıs Dişbudak ÇORAKÇI, İstanbul, İnkilap Kitapevi, 1994.

GOMPERT David C., **Right Makes Might: Freedom and Power in the Information Age**, Washington, DC, National Defense University, 1998.

HUYSMANS Jef, **The Politics of Insecurity: Fear, Migration and Asylum in the EU**, 2006, London, Routledge, http://books.google.com.tr, (e.t. 31.12.2011).

KRAUSE M., H.TIPTON, 2007, **Information Security Management Handbook**, CRC Press, 6th Ed.

KUEHL Dan, **Enformasyon Harekâtları: Yumuşak Gücün Sert Gerçeği.**

MORGANTHAU Hans J., **Politics among Nations: The Struggle for Power and Peace**, New York, Alfred A. Knopf, 1967.

NISSENBAUM Helen, **Hackers and the Contested Ontology of Cyberspace**, 2004, New Media & Society.

ÖRGÜN Faruk, **Küresel Terör**, Okumuş Adam Yayınları, İstanbul, 2001.

ROBBINS Anthony, **Sınırsız Güç**, Çeviren: Mehmet DEĞİRMENCİ, İstanbul, İnkilap Kitabevi, 1992.

SCHLEHER Curtis, **Bilgi Çağında Elektronik Harp**, Çeviren: Berna KARA, Ankara, 2004, Doruk Yayımcılık.

Türk Dil Kurumu, **Türkçe Sözlük**, TDK, Ankara, 2005, 10.Baskı.

Türk Silahlı Kuvvetleri (TSK), **Türk Silahlı Kuvvetleri Bilgi Harbine Nasıl Hazırlanmalıdır?**, Harp Akademileri Basım Evi, Yenilevent , İstanbul, Nisan, 1999.

WAEVER Ole, Barry BUZAN, Morten KELSTRUP, Pierre LEMAITRE, **Identity, Migration and the New Security Agenda in Europe**, 1993, http://books.google.com.tr, (e.t. 31.12.2011), London, Pinter.

WAEVER Ole, **Security Communities**, Cambridge, 1998, Cambridge University Press.

YILMAZ Sait, Olcay SALCAN, **Siber Uzayda Güvenlik ve Türkiye,** Milenyum Yayınları, İstanbul, 2008.

Makaleler

AAVIKSOO Jaak, Estonya Savunma Bakanı, "Siber Güvenliğin Güçlendirilmesi", http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_new-security-challenges-tu.pdf, (e.t. 23.10.2012).

AKÇADAĞ Emine, "Sürekli Artan Önemi Işığında Siber Güvenlik", http://www.bilgesam.org/tr/index.php?option=com_content&view=article&id=2178:suerekli-artan-oenemi-inda-siber-guevenlik&catid=122:analizler-guvenlik&Itemid=147, (e.t. 23.10.2012).

AL Umut, "İnternet'te Veri Güvenliği", http://yunus.hacettepe.edu.tr/~umutal/publications/datasecurity.pdf, (e.t. 22.10.2012).

ANDERSON Robert, Daniel DOMBEY, Stephen FIDLER, Isabel GORST, Maija PALMER, "US Warns Cyber-Attacks Will Increase", 2007, **Financial Times**, May 18.

ARMBRÜSTER Tobias, "Ülkeler Siber Birlikler Kuruyor", çev. Başak SEZEN, http://www.dw.de/dw/article/0,,6061521,00.html, (e.t. 06.02.2012).

ATALAY Ahmet Hamdi, "Akıllı Şebekeler ve Siber Güvenlik: Akılllı Şebekelerde Bilgi Güvenliği", http://elektrikmedya.com/akilli-sebekeler-ve-siber-guvenlik-akilli-sebekelerde-bilgi-guvenligi/, (e.t. 22.10.2012).

AYDIN Mehmet S., "Küreselleşmeye Genel Bir Bakış", **Siyasi, Ekonomik Ve Kültürel Boyutlarıyla Küreselleşme**, Mehmet S. AYDIN, Mustafa ERDOĞAN, Ali Yaşar

SARIBAY, Süleyman Hayri BOLAY, Mehmet ALTAN, 2002, Ufuk Kitapları, İstanbul.

AYDIN Mustafa, "Uluslararası İlişkilerin Gerçekçi Teorisi: Kökeni, Kapsamı, Kritiği", **Uluslararası İlişkiler Dergisi**, Cilt: 1, Sayı:1, 2004.

BALDWIN David A., "Güvenlik Kavramı", **Avrasya Dosyası Güvenlik Bilimleri Özel Sayısı**, 2003, Cilt 9, Sayı 2.

BASS Bernard, "Bilgi Çağı ve Teknolojik Gelişmeler Işığında Yönetici ve Lidere Karşılaştırmalı Bir Bakış", **Üçüncü Uluslararası Sempozyum Bildirileri**, Genelkurmay Basım Evi, İstanbul, 12–13 Mayıs 2005, SAREM.

BAYLIS John, "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler Dergisi**, Güvenlik Özel Sayı, Cilt 5, No 18, 2008.

BBC Türkçe, "Pentagon: Amerika Siber Saldırılara Hazırlıksız", 17.03.2011, http://www.bbc.co.uk/turkce/haberler/2011/03/110317_pentagon_cyber.shtml, (e.t. 30.12.2011).

BENDRATH Ralph, "The American Cyber-Angst and the Real World – Any Link? In Bombs and Bandwidth", **The Emerging Relationship Between Information Technology and Security**, Robert Latham, 2003, New York, The New Press.

BİLGİN Pınar, "Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları", **Stratejik Araştırmalar**, Ocak, 2010.

BOOTH Ken, "Security and Emancipation", **Review of International Studies**, Cilt 17, No 4, 1991.

BRUNST P.W., "Use of the Internet by terrorists, A threat analysis," **Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism**, Ankara, Turkey (Ed.) IOS Press, 2008, pp.34-60, http://libraryguides.waldenu.edu/crjs4303, (e.t. 11.08.2011).

BUZAN Barry, "People, States and Fear, An Agenda For International Security Studies in the Post Cold War Era", **Boulder**, 1991.

CARAFANO James Jay, Eric SAYERS, " Building Cyber Security Leadership For The 21st Century", **The Heritage Foundation**, No.2218, 16.12.2008, http://www.carlisle.army.mil/DIME/documents/bg_2218[1].pdf, (e.t. 02.11.2011).

CEYLAN Cenk, "İnterneti Durdurmak için Siber Savaş Aracı olarak DDoS Saldırıları", **Turkish Forensic**, http://www.bilgiguvenligi.gov.tr/siber-savunma/interneti-durdurmak-icin-siber-savas-araci-olarak-ddos-saldirilari.html, (e.t. 03.01.2012).

CEYLAN Cenk, "Savaş Cephesi Olarak, Sanal Ortamda Savunma ve Saldırı", http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/savas-cephesi-olarak-sanal-ortamda-savunma-ve-saldiri.html?Itemid=6, (e.t. 15.02.2012).

CEYLAN Cenk, "Ulusal Güvenliğin Zayıf Halkası E-Devlet", Turkish Forensic / GÖKTÜRK BT Ltd, 11.06.2009, http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/ulusal-guvenligin-zayif-halkasi-e-devlet.html, (e.t. 10.09.2011).

CNNTÜRK, "Pentagon'da bir İlk: Siber Savaş Birimi", 24.05.2010, http://www.cnnturk.com/2010/dunya/05/24/pentagonda.bir.ilk.siber.savas.birimi/577439.0/index.html (e.t. 03.11.2011).

CURRAN K., K. CONCANNON, S. MCKEEVER, "Cyber terrorism attacks cyber warfare and cyber terrorism," **Information Science Reference**, 2008.

ÇAY Ömer, "Bilgi Harbi ve Türkiye", **Ekopolitik**, 03.11.2009, http://www.ekopolitik.org/public/news.aspx?id=4348&pid=4082, (e.t 06.09.2011).

ÇERİ Yusuf, "Mobil Güvenlik", TÜBİTAK-UEKAE, http://www.bilgiguvenligi.gov.tr/mobil-cihaz-guvenligi/mobil-guvenlik.html, (e.t. 06.02.2012).

ÇOLAK H. Cahit, "Harbin Değişen Yüzü: Askeri Alanda Devrim ve Transformasyon", **Harp Akademileri Bülteni**, Mart, 2004.

DEIBERT Ronald J., Circuits of Power, "Security in the Internet Environment. In Information Technologies and Global Politics", 2002, James N. Rosenau-J. P. Singh, **The Changing Scope of Power and Governance**, Albany, State University of New York.

DEMİRAY Muhittin, İsmail Hakkı İŞCAN, "Uluslararası Sistemde Güvenlik Kavramının Değişimi Ekonomik ve Jeopolitik Arka Planı", **Dumlupınar Üniversitesi Sosyal Bilimler Dergisi**, Sayı 21, Ağustos 2008.

DENNING D., "Cyber terrorism. Testimony before the Special Oversight Panel on Terrorism," Committee on Armed Services U.S. House of Representatives, Georgetown University, May 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html, (e.t.10.08.2010).

Dış Politika ve Savunma Araştırmaları Grubu, **BİLGESAM**, "Siber Tehdit, Güvenlik, Savaş ve Stratejiler", www.bilgesam.org/, (e.t. 09.11.2011).

DOĞRUL Murat, Adil ASLAN, Eyyüp ÇELİK, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism" , **Turkish Air War College**, Istanbul, Turkey.

FINN Peter, "Cyber Assaults on Estonia Typify a New Battle Tactic", 2007, **The Washington Post**, May. 19.

GÖKALP Ziya, "PKI (Açık Anahtar Altyapısı) Nedir?" Vasco Data Security, http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/pki-acik-anahtar-altyapisi-nedir.html, (e.t. 15.01.2012).

GÜNEŞ Metin, "Çin ile Batı arasında sanal savaş", **CNN Türk**, 09.03.2010, http://www.cnnturk.com/2010/dunya/03/09/cin.ile.bati.arasinda.sanal.savas/566888.0/index.html, (e.t. 24.10.2011).

GÜNEŞ Metin, Londra, "Ermeni Siteleri Türk Korsanlar Mı Felç Etti?", 31.01.2011, http://www.cnnturk.com/2011/dunya/01/31/ermeni.siteleri.turk.korsanlar.mi.felc.etti/605178.0/index.html, (e.t. 24.10.2011).

HANSEN Lene, Helen NISSENBAUM, "Digital Disaster, Cyber Security, and the Copenhagen School", **International Studies Quarterly**, 2009, vol 53, http://www.nyu.edu/projects/nissenbaum/papers/Digital%20Disaster,%20Cyber%20Security%20and%20the%20Copenhagen%20School.pdf, (e.t. 31.12.2011).

HEIN Matthias von, "Siber savaş tehdidi artıyor", çev. Gezal Acer, http://www.dw.de/dw/article/0,,6058903,00.htmlhttp://www.dw.de/dw/article/0,,6058903,00.html, (e.t. 06.02.2012).

HUNDLEY Richard O., Robert H. ANDERSON, "Emerging Challenge: Security and Safety in Cyberspace", **In Athena's camp: preparing for conflict in the information age**, National Defense Research Institute, http://books.google.com.tr, (e.t. 31.12.2011).

IŞIKÇI Çağatay , "COBIT Denetimleri Açısından Bilgi Güvenliği", Şekerbank Bilgi İşlem, http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/cobit-denetimleri-acisindan-bilgi-guvenligi.html, (e.t. 07.11.2011).

JANCZEWSKI L. J., A. M. COLARIK, **Cyber Warfare And Cyber Terrorism, Information Science Reference**, 2008. Aktaran Murat Doğrul, Adil Aslan, Eyyüp Çelik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism" , Turkish Air War College, Istanbul, Turkey.

KARA Mehmet, "Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği", http://www.bilgiguvenligi.gov.tr/siber-savunma/elektrik-uretim-ve-dagitim-sistemleri-scada-guvenligi.html, (e.t. 06.01.2012).

KARA Mehmet, Hayretdin BAHŞİ, "Bilişim Güvenliği Araştırmalarının Yönü", **TÜBİTAK-UEKAE**, http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html, (e.t. 06.02.2012).

KARA Mehmet, Necati E. ŞİŞECİ, "Botnetlerle Mücadelede Dünyadaki ve Türkiye'deki Durum", **TÜBİTAK-UEKAE**, http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/botnetlerle-mucadelede-dunyadaki-ve-turkiyedeki-durum.html, (e.t. 07.11.2011).

KUBAT Erhan, "Gelecekteki Çok Boyutlu Harekât", **Harp Akademileri Bülteni**, Mart, 2004.

KULOĞLU Armağan, "Broken Balances After The Cold War: Searches for Regional Stability", **The Thirteenth International Confrence on Security and Cooperation**, Antalya, 2003.

LANDLER Mark, John MARKOFF, "Data Assault Hits Estonia Were It Hurts", 2007, **International Herald Tribune**, May 30.

LATHAM Rober, "Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security", The New Press.

MCSWEENEY Bill, **Security, Identity and Interests: A Sociology of International Relations**, Cambridge University Press, 1999, http://books.google.com.tr, (e.t. 31.12.2011).

MICHAELS Jim, "NATO to Study Defense Against Cyberattacks; Computer Assault Staggered Estonia", 2007, **USA Today**, June 15.

NISSENBAUM Helen, "Where Computer Security Meets National Security. Ethics and Information Technology", J. M. BALKIN, **Cybercrime: Digital Cops in a Networked Environment,** NYU Press, 2005, http://www.nyu.edu/projects/nissenbaum/papers/ETINsecurity.pdf, (e.t. 31.12.2011).

NYE Joseph S., William A. OWENS, "America's Information Edge", **Foreign Affairs**, 1996.

ÖZCAN Mehmet, "Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu", www.manisabilisim.org/dokuman/siberteror.pdf, (e.t. 16.02.2012).

ÖZEL Yücel, "Terörün Değişen Yapısı ve Asimetrik Harp İle İlişkisi", Harp Akademileri Bülteni, Kasım, 2003.

ÖZKAN Akdoğan, "Elektronik Beyinden Akıllı Kaleme", National Geographic Türkiye, Mart 2012.

PAMUK Osman, "Stuxnet'i Özel Yapan Ne?", http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/stuxneti-ozel-yapan-ne.html, (e.t. 23.10.2012).

QT Worldtel Inc., "Southeast Europe Cybersecurity Conference", C.O.B.A.S., (Centralized Out of Band Authentication System), Sofya, Bulgaristan, 8-9 Eylül 2003, http://www.cybersecuritycooperation.org/documents/QT_COBAS_White_Paper.pdf , (e.t. 13.04.2011).

SACO Diana, "Colonizing Cyberspace: National Security and the Internet", Jutta Weldes-Mark Laffey- Hugh Gusterson-Raymond Duvall, **In Cultures of Insecurity:States, Communities, and the Production of Danger**, 1999, Minneapolis: University of Minnesota Press, http://books.google.com.tr, (e.t. 30.12.2011).

SALTÜRK Metin, "Bilgi Toplumu", **Harp Akademileri Bülteni**, Kasım 2003.

SANDIKLI Atilla, Bilgehan EMEKLİER, "21. Yüzyılda Yeni Güvenlik Anlayışları ve Yaklaşımları", **Uluslararası Balkan Kongresi**, 2011, Kocaeli, http://www.bilgesam.org/tr/index.php?option=com_content&view=frontpage&Itemid=251, (e.t. 04.02.2012).

SÜTALAN Z., "Current and future trends in terrorism," **COE-DAT Newsletter,** vol.3 issue.16 p.37-49, July-September 2010.

TATAR Ünal, "Dünyada ve Türkiye'de Siber Güvenlik Tatbikatları", Ankara, Haziran 2011.

TAYLOR John, "Bilgi Çağı ve Teknolojik Gelişmelerin Devlet Yönetimine Etkileri", **Üçüncü Uluslararası Sempozyum Bildirileri**, Genelkurmay Basım Evi, İstanbul, 12–13 Mayıs 2005, SAREM.

The New York Times, "A Cyberblockade in Estonia", 2007, June 2.

TSUCHIYA Motohiro, "Siber Terörizm Tehdidi ve Önlemler", Küresel Terörizm ve Uluslararası İş Birliği, **II. Uluslararası Sempozyum Bildirileri**, Ankara, 10–11 Mart 2008.

TÜRKÖZ Tahsin, "Bilişim Güvenliği Testlerinde Başarının Sırları", TÜBİTAK, UEKAE, http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/bilisim-guvenligi-testlerinde-basarinin-sirlari.html, (e.t. 06.02.2012).

ÜÇÜNCÜ Murat, "Siber Savunmada Mücadele Alanları ve Sistem Yönetiminin Önemi", Küresel Terörizm ve Uluslararası İş Birliği, **III. Uluslararası Sempozyum Bildirileri**, Ankara, 15–16 Mart 2010.

WAEWER Ole, "Toplumsal Güvenliğin Değişen Gündemi", **Uluslararası İlişkiler,** çev. Birgül Demirtaş COŞKUN, Cilt 5, Sayı 18 (Yaz 2008),

http://www.uidergisi.com/wp-content/uploads/2011/06/Toplumsal-Guvenligin-Degisen-Gundemi.pdf, (e.t. 23.12.2011).

WALKER R. B. J. "Security, Sovereignty, and the Challenge of World Politics", 1990, Peace Research Centre, Research School of Pacific Studies, Australian National University.

WALLER Douglas, "Onward Cyber Soldiers", **TIME**, 21 Ağustos 1995, http://www.time.com/time/magazine/article/0,9171,983318,00.html, (e.t. 24.01.2012).

WARREN M. J., "Terrorism and the Internet," **Cyber Warfare And Cyber Terrorism, Information Science Reference**, 2008.

YAVUZ Celalettin, "Wikileaks'in Tunus'tan Mısır'a Domino Etkisi ve Türkiye, Ortadoğu ve Afrika", 28 Ocak 2011, http://www.turksam.org/tr/a2313.html, (e.t. 08.01.2012).

YOULD Rachel E., "In Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security", **Beyond the American Fortress: Understanding Homeland Security in the Information Age,** , 2003, Haz. Robert LATHAM, New York, The New Press.

Diğer Kaynaklar

2009 CSI Computer Crime and Security Survey, http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey09_Executive-Summary.pdf (e.t. 13.02.2012).

Anadolu Ajansı (AA), "Mısır - Siber Militanlar: Ordu ile Demokratik Reformları Görüştük", 14.02.2012, www.aa.com.tr, (e.t. 24.01.2012).

APEC Cyber Security Strategy, "APEC Telecommunications and Information Working Group 26th Meeting" 19-23 Ağustos 2002, Moskova, Rusya http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan012298.pdf, (e.t. 22.04.2011).

BBC, "Çin'de İnternet Denetimi İçin Yeni Kurum", 04.05.2011.

Bilgi Teknolojileri ve İletişim Kurumu ,"Bilgi Güvenliği: Riskler ve Öneriler Ağustos 2010 Raporu", Ankara, www.btk.gov.tr., (e.t. 14.03.2011).

BLOMFIELD Adrian, "Estonia Calls For a NATO Strategy on 'Cyber-Terrorists' After Coming Under Attack", 2007, **The Daily Telegraph**, May 18.

BUKSUR Resul, "NATO'nun ODTÜ'lü Siber Savaş Komutanı", Röportaj, 20 Ekim 2010, http://www.ntvmsnbc.com/id/25142902/#storyContinued, (e.t. 30.07.2012).

Deniz Kuvvetleri Dergisi, EKİM 2001.

Dünya Bilgi Toplumu Zirvesi, Tunus, Kasım 2005, http://www.bilgitoplumu.gov.tr/Documents/5/Documents/080100_DBTZNihaiDokumanlari.pdf, (e.t. 16.02.2012).

G8 Principles for Protecting Critical Information Infrastructures (Adopted by the G8 Justice & Interior Ministers, May 2003), http://www.justice.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf, (e.t. 14.05.2011).

http://datalossdb.org/statistics, (e.t. 13.02.2012).

http://gundem.milliyet.com.tr/bm-internet-temel-bir-insan hakki/gundem/gundemdetay/06.06.2011/1398967/default.htm, (e.t. 06.02.2012).

http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html, (e.t. 23.10.2012).

http://www.cnnturk.com/2011/dunya/05/30/irandan.internete.dev.filtre/618337.0/index.html, (e.t. 15.02.2012).

http://www.dw-world.de/dw/article/0,,14872470,00.html, (e.t. 10.01.2012).

http://www.ekds.gov.tr/ekds/tanitim.jsp, (e.t. 14.02.2012).

http://www.gen.hun.edu.tr/genom, (e.t. 10.09.2012).

http://www.hurriyet.com.tr/teknoloji/19921755.asp, (e.t. 15.02.2012).

http://www.mgk.gov.tr/Turkce/basinbildiri2010/27ekim2010.html , (e.t. 14.02.2012).

http://www.sabah.com.tr/Ekonomi/2012/07/17/ulusal-siber-guvenlik-stratejisi-hazirlandi, (e.t. 23.07.2012).

http://www.sondakika.web.tr/263093/internetten-dogan-guc-ispanya-yi-salliyor.html, (e.t. 08.01.2012).

http://www.voanews.com/turkish/news/Amerikan-Hukumetinden-Yeni-internet-Stratejisi-121969104.html, (e.t. 15.01.2012).

http://www.voanews.com/turkish/news/Washingtondan-Sanal-Saldirilara-Karsi-Silahli-Misilleme-Uyarisi-122917363.html, (e.t. 15.01.2012).

II. Ulusal Siber Güvenlik Çalıştayı, 29 Eylül 2011, Ankara, http://www.iscturkey.org, (e.t. 16.02.2012).

KÜÇÜKŞAHİN Ahmet, Tamer AKKAN, "Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit", http://vizyon21yy.com/documan/genel_konular/Milli%20Guvenlik/Strateji/Degisen_Guvenlik_Algilamalari_Isiginda_Tehdit_ve_Asimetrik_Tehdit.pdf, (e.t. 30.12.2011).

Malicious Software (Malware): A Security Threat to the Internet Economy Report, Organisation For Economik Co-Operation and Development(OECD), 17-18 June 2008, http://www.oecd.org/dataoecd/53/34/40724457.pdf, (e.t. 12.11.2011).

NATO, 2008, **Defending Against Cyber Attacks**, http://www.nato.int/issues/cyber_defence/practice.html, (e.t. 10.01.2012).

New York Times, North Atlantic Council 2007, 2 Haziran, http://www.nytimes.com/, (e.t. 31.12.2011).

NICKOLOV E., 7-8 Ekim 2008, **Modern Trends In The Cyber Attacks Against The Critical Information Infrastructure**, Regional Cybersecurity Forum, Sofia, Bulgaria.

OBAT., "Cyberterrorism seen as future threat," **Computer Crime Research Centre Tech. Report**, April 2004, http://www.crime-research.org/news/2003/04/Mess0103.html (e.t. 11.08.2011).

QT. Worldtel Inc., **C.O.B.A.S., (Centralized Out of Band Authentication System)**, "Southeast Europe Cybersecurity Conference", Sofya, Bulgaristan, 2003, http://www.cybersecuritycooperation.org/documents/QT_COBAS_White_Paper.pdf , (e.t. 13.04.2011).

SAĞIROĞLU Ş., **Bilgi Güvenliği ve Yapılması Gerekenler Sunumu**, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

SAREM, **Üçüncü Uluslararası Sempozyum Bildirileri**, İstanbul, 12–13 Mayıs 2005, "Bilgi Çağı ve Teknolojik Gelişmeler Işığında Toplum, Yönetim, Yönetici ve Lider Yaklaşımları", Ankara, Genelkurmay Basımevi, 2005.

Siber Güvenlik Hukuku Çalıştayı 2012, http://www.iscturkey.org/calistay/2/, (e.t. 16.02.2012).

Silahlı Kuvvetler Dergisi, Ekim, 2001.

Symantec Security Technology and Response, **Symantec Global Internet Security Threat Report Trends for 2008 (2009)**.

Tehdit ve Asimetrik Tehdit, 27 Nisan 2007, http://vizyon21yy.com/documan/genel_konular/Milli%20Guvenlik/Strateji/Degisen_Guvenlik_Algilamalari_Isiginda_Tehdit_ve_Asimetrik_Tehdit.pdf, (e.t. 30.12.2011).

The Daily Telegraph, "Under Attack", 2007, May 18.

The White House, **The National Strategy to Secure Syberspace**, Washington D.C., Feb. 2003, http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20GAO-Powner-SFR_10Mar09.pdf, (e.t. 18.11.2011).

ULAŞANOĞLU M. Emin, Ramazan YILMAZ, M. Alper TEKİN, **Bilgi Güvenliği: Riskler ve Öneriler**, Bilgi Teknolojiler ve İletişim Kurumu(BTK), 2010, Ankara.

Unites States Secret Service, **Annual Report**, 2009.

ÜNVER Mustafa, Cafer CANBAY, Hüseyin Burhan ÖZKAN, "Kritik Altyapıların Korunması", Mayıs, 2010, http://www.cybersecurity.gov.tr/publications/CIP_Rapor.pdf, (e.t. 29.10.2012).

Verizon Business, 2009 Data Breach Investigations Report , http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf, (e.t. 13.02.2012).

www.resmigazete.gov.treskiler20121020121020-18-1.pdf, (e.t. 29.10.2012).

Avrupa Konseyi Siber Suçlar Sözleşmesi, (Convention on Cybercrime), www.imef.org.tr, (e.t. 01.11.2012).