T.C.
KOCAELİ ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ

BİLİŞİM TEKNOLOJİLERİNİN TERÖR ve HARP AMAÇLI KULLANIMI

YÜKSEK LİSANS TEZİ

DEVRİM ÇINAR

ANABİLİM DALI :İLETİŞİM
PROGRAMI :İLETİŞİM BİLİMLERİ

KOCAELİ, 2006

T.C.
KOCAELİ ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ

BİLİŞİM TEKNOLOJİLERİNİN TERÖR ve HARP AMAÇLI KULLANIMI

YÜKSEK LİSANS TEZİ

DEVRİM ÇINAR

ANABİLİM DALI :İLETİŞİM
PROGRAMI :İLETİŞİM BİLİMLERİ

TEZ DANIŞMANI: YRD. DOÇ. DR. KERİM KARAGÖZ

KOCAELİ, 2006

T.C.
KOCAELİ ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ

BİLİŞİM TEKNOLOJİLERİNİN TERÖR ve HARP AMAÇLI KULLANIMI

YÜKSEK LİSANS TEZİ

Tezi Hazırlayan: DEVRİM ÇINAR
Tezin Kabul Edildiği Enstitü Yönetim Kurulu Tarih ve No:12.07.2006–2006/13

Doç. Dr. Füsun ALVER

Yrd. Doç. Dr. Kerim KARAGÖZ

Yrd. Doç. Dr. Betül PAZARBAŞI

KOCAELİ, 2006

SUNUŞ

İçinde bulunduğumuz çağda, bilişim teknolojileri her geçen gün daha fazla gelişmekte ve hayatımız her geçen gün daha fazla onlara bağımlı olmaktadır. Bilişim teknolojileri hayatımızı son derece kolaylaştırmaktadır. Ancak kötü niyetli ellerde bu sistemler birer silaha dönüştürülebilir.

Bilgi savaşı ve Siber Terörizm son zamanlarda çok sık kullanılan iki başlıktır. Benim de ilgimi çeken bu olmuştur. Kimler kullanır? Ne amaçla kullanır? Hepsinden öte Nasıl Kullanır? Sorularına cevap ararken konunun bir tez konusu olabileceğini düşündüm ve sonuçta bu çalışma ortaya çıktı.

Bilgi savaşı ve Siber Terörizm konuları yeni sayılabileceğinden Türkçe kaynak bulmak epey güç olmuştur. Konuyla ilgili yurt dışında yayınlanmış yayınlardan da çeviri yaparak oluşturduğum bu çalışmada en büyük problemlerden birisi de konunun kendisini sürekli yenilemesidir. Dolayısı ile çalışılan dokümanın sürekli güncel olması gerekiyor. Bir haftada en az on yeni bilgisayar virüsü piyasaya çıkıyor ve bir hafta önce üzerinde çalıştığınız yazı, güncelliğini yitiriyor.

Bilişim teknolojileri vasıtası ile yapılan yeni nesil savaşlar ve terörist saldırıları konu alan bu çalışmanın amacı, bilgi savaşı ve siber terörizm konularına dikkat çekmek, tehlikelerini, yöntemlerini ve korunma yollarını aktarmaktır.

İzmit, Mayıs 2006 Devrim ÇINAR

İÇİNDEKİLER

SUNUŞ…….. I

İÇİNDEKİLER…… II

ÖZET…… V

ABSTRACT……... VI

KISALTMALAR……... VII

GİRİŞ…….. 1

BİLGİ ÇAĞINA GİDEN YOL…….. 1

BÖLÜM 1…….. 6

SAVAŞ ve TERÖR……... 6

1.0 SAVAŞ OLGUSUNA KAVRAMSAL BİR BAKIŞ…….. 6

1.1 ÇOK BİLİNMEYENLİ DENKLEM: TERÖR…… 8

BÖLÜM 2…….. 11

ÇAĞIN KORKULARI: BİLGİ SAVAŞI ve SİBER TERÖRİZM……... 11

2.0 KAVRAMLAR ARASINDA SEÇİM……. 11

2.1 BİLGİ SAVAŞI NEDİR…….. 12

2.2 BİLGİ SAVAŞININ BÖLÜMLERİ…… 12

2.2.0 Bireysel Bilgi Savaşı……... 13

2.2.1 Tüzel Bilgi Savaşı……... 14

2.2.2 Global Bilgi Savaşı…… 15

2.2.3 Askeri Bilgi Harbi……... 16

2.3 HARP AMAÇLI BİLGİ SAVAŞI YÖNTEMLERİ…… 16

2.3.0 Komuta Kontrol Harbi (C2W)…… 17

A) Komuta Kontrol Taarruzu……. 17

i) Başı Yok Etme……... 17

ii) Gövdeyi Yok Etme……... 18

B) Komuta Kontrol Savunması……... 18

2.3.1 İstihbarat Temelli Harp (IBW)……... 18

A) Saldırı Amaçlı İstihbarat Harbi…….. 19

B) Savunma Amaçlı İstihbarat Harbi…….. 19
2.3.2 Psikolojik Harp……... 20
2.3.3 Simule Harp…… 21
2.4 ÇOK AMAÇLI BİLGİ SAVAŞI YÖNTEMLERİ……. 21
2.4.0 Ekonomik Bilgi Savaşı / Terörü (EIW)…….. 21
A) Bilgi Blokajı (Kesintisi)……. 22
B) Bilgi Emperyalizmi…… 22
2.4.1 Sayısal Bilgi Savaşı (DDW) / Terörü……. 23
A) Bilgisayar Korsan Savaşı / Terörü……. 23
i) Fingerprinting…… 24
ii) Port Scanning……... 25
iii) Network Sniffing……. 25
iv) DoS (Denial of Service)…….. 26
v) TCP / IP Hijacking……... 26
B) Semantik Hücumlar……... 27
C) Bilgi Terörizmi…….. 28
D) Siber Terör……. 28
2.5 VAROLAN ve OLASI SAYISAL BİLGİ SAVAŞI / TERÖRÜ SİLAHLARI……... 29
2.5.0 Bilgisayar Virüsleri……. 29
2.5.1 Kurtlar……. 30
2.5.2 Truva Atları……. 30
2.5.3 Mantık Bombası…….. 30
2.5.4 Tuzak Kapıları……. 31
2.5.5 Chipping (Mikroçipler)……... 31
2.5.6 Nano – Mekanikler ve Mikroplar…… 32
2.5.7 HERF (High Enery Radio Frequency) Topları……... 32
2.5.8 Eloktromanyetik Pals Bombası (EMP)……... 32
2.6 SAYISAL BİLGİ SAVAŞININ / TERÖRÜNÜN AMAÇLARI…… 33
2.6.0 Devre Dışı Bırakma…… 33
2.6.1 Zayıflatma……... 33
2.6.2 Aldatma……... 33
2.6.3 İstismar Etme…….. 33

2.7 SAYISAL BİLGİ SAVAŞININ / TERÖRÜNÜN EVRELERİ…….. 34
2.7.0 Bulaşma Evresi……... 34
2.7.1 Yayılma Evresi…… 34
2.7.2 Kuluçka Evresi…… 34
2.7.3 Faaliyet Evresi……. 35
2.7.4 Son Evre…….. 35
2.8 SAYISAL BİLGİ SAVAŞINDAN / TERÖRÜNDEN KORUNMA YOLLARI……... 35
2.8.0 Zararlı Yazılımın Sisteme Bulaşmasını Önleme……. 35
2.8.1 Zararlı Yazılımın Tespit Edilmesi ve Sistemden Silinmesi…… 36
2.8.2 Zararlı Yazılımın Yayılmasını Önleme……... 36
2.8.3 Sistemin Eski Haline Döndürülmesi……... 37
2.9 BİLGİ SAVAŞI / TERÖRÜ ve KİTLE İLETİŞİM ARAÇLARI…… 37
A) Gerçek Hayatla İlgili Mesajlardaki Şiddet……. 37
B) Gerçek Hayatla İlgisi Olmayan Mesajlardaki Şiddet……. 38
2.9.0 Terör Haberlerinin Kitle İletişim Araçlarında Sunumunun Olumsuz Yönleri…… 38
2.9.1 Terör Haberlerinin Kitle İletişim Araçlarında Sunumunun Olumlu Yönleri…… 39
2.10 BİLGİ SAVAŞI SENARYOSU……. 39

SONUÇ……... 41

YARARLANILAN YAYINLAR…….. 44

ÖZET

İçinde bulunduğumuz bilgi çağının bir sonucu olarak ortaya çıkan bilişim teknolojileri, artık hayatımızın her alanında aktif olarak yer almaktadır. Günümüzde bir kişinin evini hiç terk etmeden işini yapması, alış veriş yapması, yatırım hesapları arasında para transferinde bulunması, okula giden çocuğunun derslerindeki başarı durumunu takip etmesi, taraftarı olduğu takımın maçına yada gitmek istediği bir oyuna bilet alması, binlerce kilometre uzaktaki akrabaları ile görüntülü iletişim kurması vb. bir çok işlemi gerçekleştirmesi mümkündür.

Bilişim teknolojilerinin hızla gelişmesi, bizi gün geçtikçe onlara karşı daha bağımlı hale getirmektedir. Bu bağımlılık, hayatımızı çok kolaylaştırmıştır ancak farkında olmamız gereken bir şey vardır ki hayatımızı kolaylaştırmak için kullandığımız bu sistemler istendiğinde büyük birer silaha dönüşebilirler.

Bilgi savaşı ve siber terörizm çağın en büyük tehlikelerinden biridir. Bilişim sistemleri ordular tarafından harp amaçlı, devletler tarafından bilgi çalma amaçlı, teröristler tarafından eylem yapma amaçlı kullanılabilirler. Kişisel bilgisayarımıza bulaşan bir virüs sistemimize zarar verebilir, bütün bilgilerimizi bir anda yok edebilir yada istenmeyen kişilerin eline geçmesine neden olabilir.

Bilgi savaşları kişisel, tüzel, global ve askeri bilgi savaşı olarak dört alt başlıkta incelenebilir. Her bir başlığın kendine özel yöntemleri olabileceği gibi ortak olarak kullandıkları yöntemler de bulunmaktadır. Kullandıkları sayısal bilgi savaşı silahları ise aynıdır.

Siber terörizm ise terörün çağımızdaki yüzünü yansıtmaktadır ve eylem alanının daha büyük olması, daha çok insanı etkileyebileceği anlamına gelebilir. Günümüzde teröristlerin bilgisayar vasıtası ile gerçekleştirdiği eylemler her geçen gün daha tehlikeli hale gelmektedir.

Kişiler, devletler, şirketler ve ordular yeni nesil savaşlara ve terör saldırılarına hazırlıklı olmalı, sistemlerini saldırılara karşı korunmalı hale getirmelidirler.

ABSTRACT

As a result of the information age that we now live in, information technologies take an active place in our whole life. Today it is possible for a person to do his job, do shopping, transfer money in his financial accounts, see his child's success at the school, buy a ticket for his favourite team's match or for a play which he wants to go, have video conference with his parents who are thousands of miles away from him without leaving his home.

The fast growth of the information technologies is making us dependent to them. This dependence makes our life easier but we must see that, these systems - which we use to make our life easy- may turn to harmful weapons if wanted.

Information warfare (IW) and cyber terrorism are nearly the biggest danger in this age. Information technologies can be used as a war objective by the armies, as an information thief by governments and as an action objective by terrorists. A virus that infects your personal computer may give some damage to your system, delete all your data or send it to unwanted people.

Information warfare can be examined under four headings. Personal IW, corporate IW, global IW and military based IW. Each heading may have a special procedure while they have some common ones. The digital data warfare weapons they use are the same.

Cyber terrorism shows the new face of terrorism in this age and one can say the bigger is the action area, the more people are affected. The actions that terrorists make by using a computer are getting more dangerous day by day.

People, governments, companies and armies should be ready for the new generation of wars and terrorist attacks and they should have their systems shielded.

KISALTMALAR

BKZ. :	Bakınız
C2W:	Komuta Kontrol Savaşı (Command and Control Warfare)
IW:	Bilgi Savaşı (Information Warfare)
DDW:	Sayısal Bilgi Savaşı (Digital Data Warfare)
EIW:	Ekonomik Bilgi Savaşı (Economic Information Warfare)
EMP:	Elektromanyetik Pals
HERF:	Yüksek Enerjili Radyo Frekansı (High Energy Radio Frequency)
HW:	Hacker Savaşı (Hacker Warfare)
IBW:	İstihbarat Temelli Harp (Intelligence Based Warfare)
ÖR.	Örneğin
TEMPEST:	Elektromanyetik Sızıntı (Temporary Emanations and Spurious Transmission)
VB.	Ve bunun gibi

GİRİŞ

BİLGİ ÇAĞINA GİDEN YOL

İnsanoğlu yaratılışından bu yana sürekli bir ilerleme aşamasındadır. İlk insandan günümüze uzanan evrelerde insanlığın çok farklı şekillerde ilerlediğini görmek mümkündür. Bu ilerleme ve gelişme sırasında değişmeyen bazı unsurlar dikkat çekmektedir. Bunlardan biri insanoğlunun baskın (dominant) olma tutkusu ve bu tutkuyu gerçekleştirebilmek için bulduğu yöntemlerdir. İnsanlık büyük kabuk değişimlerini büyük devrimlerden sonra gerçekleştirmiştir. Baskınlık tutkusu da bu devrimlerde rolünü kusursuz olarak oynamıştır.

İlk insanın dönemine İlkel toplum denilebilir. Bu toplumda üretim aşaması yoktu. İnsanlar ya etraflarındaki ağaçlardan meyve topluyorlar, ya da avlanarak yaşamlarını devam ettiriyorlardı. Yaşam alanları mağara veya doğal sığınak ortamlarıydı. Toplu yapılan nadir işler vardı. Örneğin, başarılı bir av için hep birlikte avlanmak gibi. Yine de baskınlık tutkusu o dönemde bile ön plandaydı. İlkel insan, günümüzde belgesellerde seyrettiğimiz vahşi hayvanların yaptıkları gibi bir güç mücadelesi içindeydi. Kazanan en güzel mağarada barınır, avın en lezzetli tarafını sahiplenirdi.

Daha sonralarda tarımcılığın öğrenilmesi, sulu tarıma geçiş ve vahşi hayvanların evcilleştirilmesiyle başlayan ve adına tarım devrimi diyebileceğimiz dönem başlamıştır. Bu dönemde üretim ve baskınlık şekilleri değişmeye başladı. İnsanlar toplu halde üretime katılmaya başladılar. "Toprak ağaları, köleler, tüccarlar, küçük esnaf gibi kümeler toplumdaki yerlerini almaya başladılar."[1] Baskınlık bu sefer de maddi güç açısından değerlendirilmeye başlandı. Toprak sahipleri zincirin en üst halkasında yer aldılar.

"Binlerce yıllık bir süreden sonra, 18 inci yüzyılda, buhar makinesinin bulunması ile ilk teknolojik devrim, sanayi devrimi ve bu devrimin yapılandırdığı sanayi toplumu doğdu. Sanayi devrimi İngiltere'de başlamıştı. Diğer Avrupa ülkeleri de buna hızla ayak uydurdular ve dünyadaki kurulu dengeler altüst oldu. Tarım

[1] Harp Akademileri Komutanlığı, **Türk Silahlı Kuvvetleri Bilgi Harbine Nasıl Hazırlanmalıdır?**, İstanbul: Harp Akademileri Komutanlığı Yayınları, 1999, s. 1

toplumu aşamasında doğu ülkeleri Avrupa'nın ilerisinde iken, sanayi devrimi sonucu ileri geçen Avrupa ülkeleri, dünün egemen ülkelerini kendilerine sömürge kıldılar."[2] İşçi sınıfının ortaya çıkması bu döneme denk düşer.

"İkinci Dünya Savaşı'nı izleyen yıllarda, teknolojideki gelişmeler sonucu tarım ve sanayi toplumlarının artık çok yeni bir aşamaya geldiğini görüyoruz; uzaya gidiş, atom bombası, jet motoru, nükleer enerji, cep telefonu, televizyon ve bilgisayar ortaya çıktı."[3] Bütün bu yenilikler beraberinde yeni bir devrimi ve çağı da getirdi. Bilgi devrimi ve bilgi çağı.

Cep telefonları, bilgisayarlar, dijital ortam, geniş veri depolama aygıtları, dünyayı sonsuz bir bilgi ortamına soktu. Artık bu aletler olmadan dünyanın kusursuz olarak işlemesi neredeyse imkansız görünmektedir. İnsanlara daha çabuk, daha hızlı ve daha *az kusurlu*[*] bir hizmet sunmanın yolları da yine bilgi ve iletişim sistemlerinden geçmektedir. ATM cihazları, Uydu telefonları, GPS aletleri, Avuç içi bilgisayarlar vb., aletlerin her biri teknolojiye dayalı, hayatımızı kolaylaştıran aletlerdir.

Artık evimizden hiç ayrılmadan ofisimizdeki bilgisayarı kullanmamız, vapurda yolculuk yaparken bankalar arası hesaplarımızdan para aktarımı yapmamız, evdeki veya okuldaki çocuğumuzu kendi kişisel bilgisayarımızdan saniye saniye izlememiz, uydu görüntüleriyle bir ay sonraki hava durumu tahminlerini elde etmemiz, bizden binlerce kilometre uzakta oturan kişilerle etkileşimli iletişim kurabilmemiz ve dosya alışverişinde bulunabilmemiz, İnternet vasıtasıyla bilgiye ulaşabilmemiz ve kredi kartı ile alışveriş yapabilmemiz mümkündür.

Acaba bütün bunları yaparken tek başımıza mıyız? Birileri bizim adımıza bu işlemleri gizli yollarla yapamaz mı? Kişinin bir sabah kalktığında bankalardaki bütün yatırımlarının başka hesaplara aktarıldığını görmesi, kamu kayıtlarında bir anda azılı bir terörist olarak görünmesi mümkün müdür? "Bilgi çağıyla birlikte her geçen gün

---

[2] Harp Akademileri Komutanlığı, a.g.e., ss. 1-2
[3] Harp Akademileri Komutanlığı, a.g.e., s. 2
[*] Bu çalışmada bu tip sistemlerin kusurları olabileceği, ve saldırıya açık oldukları savunulacağından yazar *"az kusurlu"* tanımını *"kusursuz"* tanımlaması yerine kullanmayı daha uygun bulmuştur.

daha "akıllı" hale gelen teröristlerin teknolojiyle kurdukları ilişki geliştikçe, eylemlerdeki uzmanlıkları da artıyor."[4]

Bilginin bu denli kolay bir biçimde paylaşılmasını sağlayan İnternet, bilişim sistemleri güvenliğini konu eden çok yüksek miktarda bilgiye de ev sahipliği yapıyor. Yalnızca İnternet' ten ve herkese açık bilgileri toplayan bir saldırgan, çok kısa sürede İnternet'e bağlı pek çok bilgisayar sistemine saldırabiliyor ve ciddi zararlar verebiliyor. İnternet üzerinde bugün gerçekleşen ve gazetelere de yansıyan siber saldırılar gelecek bilişim savaşlarının bir habercisidir. Bu konuda herkes hemfikir olsa da merak sürüyor; 'ilk savaş hangi ülkeler arasında ve ne zaman gerçekleşecek?'. Bazı uzmanlar, daha ileri giderek, bilişim savaşlarının 'toplu-tüfekli' geleneksel savaşların yerini alacağını ve önümüzdeki yüzyılda geleneksel savaşlar ile giderek daha az karşılaşacağımızı öne sürüyorlar. "Amerikan ordusunun 'information warfare - IW olarak anılan bilişim savaşlarına yönelik çok ciddi hazırlıklarının olması da bu beklentiyi doğrular niteliktedir."[5] Amerika ile birlikte dünyada yirmi kadar farklı ülkenin bilişim savaşlarına yönelik hazırlıkları olduğu İnternetteki çeşitli kaynaklarca öne sürülmektedir. Medyanın, finans kuruluşlarının, kamu hizmetlerinin ve iletişimin neredeyse tümüyle bilgisayarlı ortamda gerçekleştirildiği ülkeler giderek artan biçimde siber tehdit altındadırlar. Bir ülkenin bilişim altyapısı ele geçirildiğinde ya da çalışamaz hale getirildiğinde, ülkenin yaşamsal faaliyetleri durdurulmuş olacaktır. Böylesine büyük çaplı bir saldırı, başarılabildiği takdirde, ülkenin haritadan silinmesine kadar giden bir çöküşün başlangıcı olabilir. Medyanın çalışamadığı, iletişimin gerçekleşemediği, banka hesaplarının boşaltıldığı ve kamu hizmetlerini veren bilgisayarların durduğu bir ülke varlığını sürdürebilir mi?

Kabul etmek gerekir ki yukarıdaki kötü durumun gerçekleşme olasılığı vardır. "Olanaklarını önümüze sakınmadan sunan teknoloji, teröristlerden de kendini esirgemiyor."[6] İçinde bulunduğumuz çağ, yani bilgi çağı, bize güzellikler yanında bazı büyük tehlikeler de sunmaktadır. Diğer devrimlerde ve çağlarda olduğu gibi insanoğlunun baskın olma tutkusu içinde bulunduğumuz çağda da ön plana çıkmıştır. Kişiler ve / veya devletler kendi bilgilerini korumaya çalışırken diğer kişi ve / veya

---

[4] Ayşenur Topçuoğlu, **Siber Terörizm,** Bilim – Teknik Dergisi, 2001, s. 39
[5] Burak Dayıoğlu, **Bilişim Savaşlarına Hazırmısınız?,** Olympos Security Güvenlik Portalı URL:http://www.olympos.org/article/articleprint/161/-1/10/bilisim_savaslarina_hazirmisiniz
[6] Topçuoğlu, a.g.m., s. 39

devletlerin bilgilerini elde edip onlara karşı üst duruma geçmek istemektedirler. "Bilgisayar dünyasındaki gelişmeler insanoğlunun yaşamını kolaylaştırmanın yanında, amacı başka insanlara zarar vermek olan suçlulara da büyük imkanlar sunmaktadır. Farenin bir hareketiyle ya da bir düğmeye basıldığında dünyanın herhangi bir köşesine istediğimiz gibi ulaşabiliyorsak, bu ilişki suç dünyasının üyeleri ve teröristler için de geçerlidir. Bu çerçevede, amaçları hedef aldıkları ülkeleri, ekonomik, sosyal, kültürel, siyasi ve teknolojik açıdan yıpratarak çökertmek olan terör örgütleri, eylem koyacakları hedefler hakkında bilgi toplamaktan, haberleşmeye ve propagandaya kadar İnternet'in tüm imkanlarından sınırsızca faydalanabilmektedirler."[7] Bu durum bu çalışmada ele alacağımız çağımızın en tehlikeli ve en sinsi iki sorununu ortaya çıkarmaktadır. Bilgi harbi (savaşı) ve Bilgi Terörü.

Bu çalışmada bilgi savaşı ve bilgi terörü konuları ele alınacak, bunların nasıl uygulandığı, ne sonuçlar doğurduğu, kim yada kimler tarafından ve ne amaçla gerçekleştirilebileceği, olumlu ve olumsuz yanları, kimlerin ne kadar etkilenebileceği ve korunma yolları üzerinde durulacaktır.

"Tarihte ilk olarak şifreleme yöntemleriyle başlayan güvenli bilgi aktarımı günümüz dijital ortamında daha büyük önem taşıyor."[8] İnsanlığın geçirdiği diğer baskınlık mücadelelerinden farklı olarak bilgi savaşı/terörü çok daha acımasız ve çok daha zararlı olabilir. Kişilerin yaşama haklarına direk olarak bir etkisi olmasa da dünya ekonomisini alt üst edecek sonuçlar doğurabilir. Örneğin 2002 yılında bir üniversite öğrencisinin yazdığı bir kurtçuk (worm) bir günde bütün dünyanın İnternet erişimini bloke etmiş; borsaların, bankaların, hastanelerin, hava, deniz ve kara taşımacılık sistemlerinin, enerji sistemlerinin birbirleri ile olan bağlantılarını koparmıştı. Bu bir günün sadece Amerikan ekonomisine verdiği zarar milyarlarca dolardır. "Belli başlı bilgisayar kurumlarına giriş bir suçlu için de, iyi bir vatandaşa olduğu kadar açık. Bu nedenle "elektronik teröristler" için bazı güvenlik

[7] Necati Alkan, **Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler,** http://www.caginpolisi.com.tr/20/41-43.htm, 17/08/2003
[8] **Siber terör: Gerçek tehdit,** http://www.ntvmsnbc.com, 17/10/2003

sistemlerinin en zayıf noktalarına yönelik stratejik planlar kurmak zor olmayacaktır."[9]

Bilgi, diğer güç kaynaklarından çok farklıdır. "Bilgiyi diğer güç kaynaklarından ayıran hususlar; tükenmez olması, aynı anda karşılıklı, hem olumlu hem de olumsuz olarak kullanılabilmesi ve en önemlisi, kuvvetin ve servetin aksine, zayıfların ve yoksulların da sahip olabileceği bir unsur olmasıdır. Küçük bir doğru bilgi parçası büyük stratejik veya taktik üstünlük sağlayabilir. Küçük bir bilgi kırıntısının olmaması felaketli sonuçlar doğurabilir. Bilginin kontrolü, yarının tüm kurumlarında yer alacak, dünya çapındaki güç mücadelesinin özünü oluşturmaktadır."[10]

Bilgi ve iletişim sistemlerinin günümüz askeri operasyonlarında ve sıcak savaşlarında da kullanılması mümkündür. Körfez savaşları sırasında Irak, Amerikan ordusunun ileri teknoloji silahlarını deneyebilmesi ve bilgi harbi senaryolarını uygulayabilmesi için kusursuz bir eylem sahası olmuştur. "Körfez Savaşı süresince, harekat alanı üzerinde bulunan, bilgi çağı teknolojileri ile donatılmış uydu sistemleri, muharebe sahasının gözetlenmesi ve muharebenin yapısına yeni bir boyut kazandırmış, kızıl ötesi ve gece görüş sistemleri ile gece hakimiyeti temin edilmiş ve gerçek zamanlı keşif-gözetleme yapılarak süratli reaksiyon, doğru angajman ve isabetli nokta atış yapma imkanı her an sağlanmıştır. Akıllı silah sistemleri, muharebe sahasının derinliğinden, muhasımın silah menzilinin çok ötesinden hedeflerini büyük bir hassasiyetle bulmuşlardır."[11]

"İletişim imkanlarının gelişimi, Körfez Savaşını televizyonlar vasıtasıyla evlerimize naklen ulaştırmış, harekat dünya kamuoyu tarafından takip edilmiş, medya psikolojik harbin bir vasıtası haline gelmiştir."[12]

---

[9] Topçuoğlu, a.g.m., s. 39
[10] Alvin ve Heidi Toffler, **21. Yüzyılın Şafağında Savaş ve Savaş Karşıtı Mücadele,** Sabah Kitaplarından Harp Akademileri Komutanlığı, a.g.e., s. 2
[11] Harp Akademileri Komutanlığı, a.g.e., s. 4
[12] Harp Akademileri Komutanlığı, a.g.e., ss. 4-5

BÖLÜM 1

SAVAŞ ve TERÖR

1.0 SAVAŞ OLGUSUNA KAVRAMSAL BİR BAKIŞ

İnsanoğlu yıllardan beri hayatla, kendisiyle ve diğerleriyle bir mücadele içerisindedir. Hayat ve kendisiyle yaptığı mücadele içsel bir mücadeledir. Ancak diğerleriyle yaptığı mücadele çok basit olabileceği gibi; bunun tam tersine çok çetin, zarar verici, sinir bozucu, yıpratıcı, şiddet içeren ve hatta ölümcül olabilir. İnsanoğlunun diğerleriyle yaptığı mücadele kimi zaman yiyecek, kimi zaman su, kimi zaman para, kimi zaman toprak, kimi zaman özgürlük ve kimi zamanda günümüzde yaşandığı gibi bilgi için olabilir. Mücadele büyüdükçe büyüyebilir ve sonunda bin yıllardır olduğu gibi, o korkunç son karşımıza çıkar: Savaş

Savaşlar insanlık tarihinin başlangıcından bu yana hep varolmuşlardır ancak savaşların gerçekleşme koşulları, amaçları ve sonuçları insanların içinde bulundukları döneme göre farklılıklar göstermektedir. Çalışmanın giriş bölümünde de değinilen tarım, sanayii ve bilgi devrimleri dönemlerinde gerçekleşen savaşlara dikkat edildiğinde görünüyor ki insanların savaş stratejileri oluş, gelişme sonuç açılarından bazı farklılıklar göstermektedir. (Bkz. Tablo 1, s, 7)

Savaş günümüzde bütün modern toplumların karşı çıktıkları bir olgu olsa da dikkat etmek gereken bir husus var ki; bütün bir ömrü boyunca hiç savaş yüzü görmemiş insan sayısı yok denecek kadar azdır. Kişiler savaşı bizzat yaşamasalar dahi görsel-işitsel ve / veya yazılı basın vasıtası ile mutlaka savaşlara tanık olurlar. Bugün dünyanın çoğu yerinde ilk okula giden çocukların dahi kullandığı bir kelime ve gördüğü bir gerçektir savaş. Peki ama nedir bu savaş? Nasıl tanımlamak gerekir?

"Batı düşünce tarihinde savaşı evrene egemen bir güç olarak ilk kez dile getiren Herakleitos olmuş. Ona göre, savaş evrensel döngüyü sağlar ve olmazsa oluş durur. Savaş her şeyin kralı, babasıdır. Hegel ise savaşı tarihe özgü olarak görür. Darvin, savaşı canlılar dünyasında hayat savaşı ya da varolma savaşı olarak ele alır. Büyük Larousse savaşı, "Uluslar veya aynı ülkelerdeki iki teşkilatın (iç savaş) arasında, başka bir yolla elde edemediği şeyi kuvvet zoruyla almak, istediklerini

kabul ettirmek ve başkasının isteklerine boyun eğmemek amacıyla girişilen kuvvet denemesi" olarak tanımlar. "[13]

Görünüyor ki savaş, eski dönemlerde bir zorunluluk olarak, bir yaşama amacı ve aracı olarak algılanmıştır. Günümüzde savaşın tamamıyla içindeki bir ülkenin vatandaşları bile bunun zalimlik olduğunu savunabilmektedir. Örneğin Amerikan vatandaşlarının hatırı sayılır bir yüzdesi Irak savaşına olumsuz bakmaktadır. Kitle imha silahlarının gelişmesi ve savaşların her geçen gün daha fazla can almaya başlaması da toplumları savaşlar ve sonuçları konusunda endişeye sevk etmiştir.

Tablo 1: Tarım, Sanayi ve Bilgi Devrimleri Dönemlerinde Gerçekleşen Savaşların Özellikleri ve Birbirlerinden Farklılık Gösterdikleri Yönler

Hareket Tanımı	Tarım Hareketi	Endüstri Hareketi	Bilgi Hareketi
Güvenlik Sağlayıcı	Savaşçı sınıf, paralı askerler, milisler	Profesyonel askerler, vatandaşlar	Bilgi sahibi liderler
Baskın topluluk, siyasi, ekonomik, güç	Kabile, şehir, devlet, aile	Milli-Devlet, fabrikalar	Global Şirketler
Baskın ekonomi	Ticaret	Para	Semboller (ör.:veritabanı)
Savaş Karakteristiği	Birebir katılımcı çarpışma	Kalabalık ordular, büyük kayıplar	Bilgi Saldırıları, en az kayıp
En yüksek yok etme gücü	Barut	Kitlesel yok ediciler (nükleer, kimyasal silahlar)	Önemli veri yok edilmesi
Liderlik	Hiyerarşi	Emir komuta zinciri	Düz yapılanmalar, en alt düzeyde güç odakları
Bilgi gerektiren savaşlar	evet	evet	evet
Savaşta bilgi teknolojisi	hayır	evet	evet
Bilgi Savaşı	hayır	hayır	evet

Kaynak: http://www.sanalteror.gen.tr

"Daha öldürücü silahlar bulunup kullanıldıkça savaş yöntemleri çağlar boyunca sürekli olarak değişmiştir. Günümüzdeki savaşlar eski çağlardaki savaşlardan, bir güdümlü füzenin mızraktan farklı olduğu kadar farklıdır. Bu

[13] **Dünyada Savaşın Tarihçesi,** http://www.dunyaonline.com/48535.asp, 18/10/2003

değişikliğin yanı sıra, insanların savaş konusundaki görüşleri de değişmektedir. Eskiden bir yaşam biçimi ya da bir zorunluluk olarak görülen savaş, günümüzde uygar dünyada, kaçınılması gerekli büyük bir kötülük olarak kabul edilir."[14]

1.1 ÇOK BİLİNMEYENLİ DENKLEM: TERÖR

Terör günlük hayatta çok sık kullanılan bir kelime olmasına rağmen, ortak kabul görür bir karşılığını bulmak çok zordur. Bu durum kişilerin terörü kendi bakış açılarıyla ve dünya görüşleriyle tanımlamalarından kaynaklanmaktadır. Bir kişinin terör olarak tanımladığı bir eylem diğer bir kişi tarafından özgürlük savaşı olarak tanımlanabilir. Yine bir kişinin terörist diye tanımladığı bir insan başkası tarafından özgürlük savaşçısı olarak tanımlanabilir.

Konu devletlerarası tartışıldığı zaman hepten çıkmaza girmektedir. Devletler, karşı bir devlete yapılan terörist bir saldırıyı terör olarak adlandırmaktan kaçınabilirler. Kaçınabilirler, çünkü bazı durumlarda meydana gelen bir terör eylemi, bir başka ülkenin çıkarlarına hizmet edebilir. Bir devlet, diğer bir devletin terör örgütü olarak tanımladığı bir grubu belirli yönlerden destekleyebilir.

11 Eylül'de Amerika Birleşik Devletleri'ne yapılmış olan saldırılardan sonra, Amerikanın baskı ve çabalarıyla terör konusunda ortak söylemler doğmuş olsa da, ortak bir eylem gösterildiğini söylemek zordur.

Ansiklopedik karşılığına baktığımızda terör: "Bireylerin, grupların yada devletin siyasal bir amaçla başka kişi ve gruplara karşı giriştiği, savaş dışı sistemli şiddet eylemleri"[15] olarak tanımlanmaktadır.

Yukarıdaki tanımlamada geçen şiddet kelimesi dikkat çekicidir. Çünkü şiddet korkuyu doğurur. Halk arasında paniğe yol açar. Terörist grupların ulaşmak istedikleri asıl amaç da budur. Halkı şiddet eylemleriyle korku ve isyana sürükleyerek elde etmek istedikleri siyasi hedefe yasadışı yollardan ulaşmak ya da kendi görüş ve düşüncelerini baskıda bulundukları kişilere benimsetmek.

---

[14] Savaş ve Savaş Araçları, **Temel Britannica,** Cilt 15, İstanbul: Ana Yayıncılık, 1993
[15] Terörizm, **Temel Britannica,** Cilt 17, İstanbul: Ana Yayıncılık, 1993

"Bir cinayette esas amaç öldürmek iken, teröristin insan öldürme eyleminde amaç, birini öldürmekten çok belirli mesajlar vermek, kitlelere korku salmak, insanları terörize etmektir. Bu, terörizmin çok önemli bir unsurudur. Terörizm sadece bir grup militanın şiddet eylemleriyle oluşmaz, bu eylemler sonucunda doğan panik, belirsizlik, korku atmosferi de terörizmin parçalarındandır."[16]

12/04/1991 tarih ve 3713 sayılı Terörle Mücadele Kanunu terörü şöyle tanımlar: "Terör, baskı, cebir, şiddet, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değiştirmek, devletin ülkesi ve milleti ile bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyeti'nin varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü eylemlerdir."[17]

Emre Kongar, Küresel Terör ve Türkiye adlı kitabında teröre sosyolojik açıdan bakar ve şöyle der. "Terör, toplumbilim açısından, siyasal yapıda, yani egemenlik ilişkisi içinde yer alan bir etkinliktir. Esas olarak hedeflediği kişinin, grubun ya da toplumun ardındaki yönetim felsefesine, yani meşru ya da gayri meşru olarak belirlenmiş olan egemenlik ilişkisine saldırır. Otoriter rejimlerde, kimi zaman haklı bir tepki imiş gibi algılanan terörist eylemlerin, demokrasilerde lanetlenmiş olmasının nedeni demokratik rejimlerdeki egemenlik ilişkisinin yani yönetim felsefesinin halkın iradesine ve onayına bağlı olmasından dolayıdır."[18]

"Terörün en önemli özelliklerinden biri hedefini rasgele seçmesidir."[19] Kurbanın toplum içinden herhangi biri olması, hatta direk kurban olarak seçilmese de bir terör eyleminin gerçekleştiği sırada tesadüfen o bölgede bulunması nedeniyle kurban olması insanlarda korkunun yayılmasına neden olur. Halk içinde tedirginlikler, huzursuzluklar yaşanır. Terörist kurbanını ve / veya eylem alanını kendi düşünce ve hayat tarzına göre yargılar ve öyle seçer. Bu da her bir bireyin terör

---

[16] Bozkurt Zakir Avşar, **Kitle İletişim Araçları ve Terör,** İstanbul: Kamer Yayınları, s. 15
[17] **Terör Nedir?,** http://www.iem.gov.tr/teror/index.asp#not1, 20/10/2003
[18] Emre Kongar, **Küresel Terör ve Türkiye,** 1. b., İstanbul: Remzi Kitabevi, 2001, ss. 73-74
[19] **Terörün Tanımı,** http://www.teror.gen.tr/turkce/teror_nedir/tanimi.html

kurbanı olabileceği anlamına gelir. Bir gün alışverişe ya da işe giderken terör kurbanı olmayacağını insanlara kimse garanti edemez.

Bununla birlikte terör ve şiddet eylemlerinin bilişim teknolojileri vasıtasıyla tüm dünyaya kısa sürede duyurulması bireylerin korkularını üst safhaya çıkarmaya kolaylıkla yetmektedir.

Bugün artık, bizim dışımızdaki bir şiddet olayı bize ya anında ya da çok kısa bir süre sonra, ayrıntıları ile sözlü, görüntülü ya da yazılı olarak ulaşabilmektedir. Bilişim sistemlerinin en yoğun biçimde tüketildiği dönem olan günümüzde de haber niteliği olan her şiddet olayı, her terör olayı, o olayın dışındakilere de ulaşabilmektedir. Bir anlamda şiddet olayları ulusallıktan çıkarak evrenselliğe bürünebilmektedirler. Özellikle elektronik kitle iletişim araçlarındaki gelişmeler bu tür mesaj ve haberlerin çok daha hızlı yayılmasına sebep olurken bunları takip eden insanların bundan etkilenme seviyeleri çok daha artmıştır.

Her ne amaçla olursa olsun terör insanlık dışı bir eylem çeşididir. Terör masum insanların ölümüne, yaralanmasına ve acı çekmesine yol açar. Terörün bütün biçimleri için ortak olan özellikleri vardır ki bunlarda terörün acımasız, tahrip edici ve ahlak dışı olmasıdır.

"Sağlıklı bir değerlendirme yapıldığında terör örgütleri ileri sürdükleri şekilde, hedeflerine ulaşamayacakları gibi zamanla marjinalleşmeye de mahkumdurlar. Buna rağmen toplumlardaki dengesizlik ve aksaklıkların, hoşnutsuz kişilerin ortaya çıkmasına yol açtığı ve birtakım güçler ve devletlerin terörü, hedeflerine ulaşmada bir araç ve baskı unsuru olarak gördükleri müddetçe terörizm varlığını devam ettirecektir."[20]

[20] **Terör Nedir?,** http://www.teror.gen.tr/turkce/teror_nedir/nedir.html

BÖLÜM 2

ÇAĞIN KORKULARI: BİLGİ SAVAŞI ve SİBER TERÖRİZM

2.0 KAVRAMLAR ARASINDA SEÇİM

Bilişim teknolojileri söz konu olduğu zaman bilgi savaşı, siber savaş, bilgi terörü, siber terör terimleriyle sıkça karşılaşırız. Konunun yeni olması ve birbirleriyle iç içe kavramlardan oluşması nedeniyle günümüzde her bir terim neredeyse birbirinin yerine kullanılmaktadır. Dünya ve Türk medyasında, hatta yapılan akademik çalışmalarda da durum aynıdır.

Çalışmanın ikinci bölümünde aktarılmış olan savaş ve terör olguları birbirlerinin yerine kullanılacak kadar yakındır. Kişi gerçekleştirdiği bir eylemde kendini haklı görüyorsa bunu savaş; kendine karşı gerçekleştirilen bir eylem de de kendini mağdur yada kurban yerine koyuyorsa bunu terör olarak adlandırır. Örneğin, son Körfez savaşında A. B. D. gerçekleştirdiği eylemleri savaş olarak adlandırırken 11 Eylül de kendisine karşı yapılan eylemi terör olarak tanımlamıştır. Amerikanın savaş düşüncesinin aksine Irak hükümeti ve savaş karşıtları, Amerikanın yaptıklarını terör, şiddet, işgalcilik olarak tanımlamışlardır.

Emre Kongar, Küresel Terör ve Türkiye Kitabında konuya değişik bir açıdan yaklaşır ve her iki olgunun da aslında terör olduğundan şöyle bahseder: "Devletler ve toplumlar arası savaşlar, doğrudan doğruya egemenlik ilişkisini değiştirmeye ve bu ilişkiye el koymaya yönelik olduklarından ve sivillerin de ölümüne yol açtıklarından, zaten tanım gereği terörist nitelik taşırlar."[21]

Savaş sadece askerler arasında meydana gelen bir kavram değildir. Sözlükten savaşın yan anlamlarına baktığımız zaman çekişme, mücadele, rekabet, vb. kelimeleri görürüz. Bu da kelimenin hem asker hem sivil tabanlı konuları içine alabileceğini gösterir.(Ör: Körfez Savaşı[*], Enflasyonla Savaş[**], vs.) Konu bilişim teknolojileri ve bilgi savaşı olduğunda da durum aynıdır. Kavram kargaşalarını ortadan kaldırmak amacıyla bu çalışmada konu başlıkları belirlenirken sadece askeri alanı ilgilendiren başlıklarda "savaş" kelimesi yerine "harp" kelimesi kullanılacaktır.

---

[21] Kongar, a.g.e., s. 74

[*] Kelimenin 1. anlamında kullanılmış hali

[**] Kelimenin yan anlamıyla kullanılmış hali

2.1 BİLGİ SAVAŞI NEDİR?

Bilgi savaşının tam ve ortak kabul görür bir tanımı henüz bulunmamaktadır. "Bu yeni bir sanat mıdır? Savaşın zamana göre değişikliğe uğramış en yeni şekli midir? İnsan beyninin yarattığı, bugünün küresel bilgi ortamı veya bilgi teknolojilerinin oluşturduğu çatışma ortamı mıdır?"[22]

Günümüzde sıklıkla kullanılan "Bilgi Savaşı" deyimi çoğunlukla yanlış anlaşılmakta ve daha çok büyük ordularda bulunan üstün teknoloji silahları ile yapılan savaşları çağrıştırmaktadır. Bilgi savaşı aslında; "kendi sistemlerini koruma altına alırken karşı tarafa ait bilgiyi, bilgi tabanlı işlemcileri ve bilgi sistemlerini etkileyecek bir hareket gerçekleştirmek anlamına gelmektedir."[23] Yani kendi bilgilerimizi sonuna kadar korurken karşımızdakinin bilgilerini elde etme mücadelesi.

Aslında askeri anlamda çok eski olan bilgi savaşı terimi bilişim teknolojilerindeki gelişme nedeniyle günlük hayata girmiş oldu. Eskiden karşı tarafın bilgisini elde etmek için casus ve ajanlar kullanılırken günümüzde evimizde bulunan bilgi sistemleri kullanılır hale geldi.

İnternet sayesinde bütün dünya ağına bağlı olan bilgisayarlar eskiye oranla çok daha çabuk bilgi sunabiliyor ve hatta çalabiliyorlar. Bu durum normal vatandaşları da saldırıya açık hale getirdi. Artık evde, okulda veya işyerinde kullandığımız bilgisayar dünyanın en gelişmiş silahlarından biridir.

2.2 BİLGİ SAVAŞININ BÖLÜMLERİ

Bilgi savaşını bireysel bilgi savaşı, tüzel bilgi savaşı, global bilgi savaşı askeri bilgi harbi başlıkları altında dört ana gruba toplayabiliriz. Bu başlık altındaki bölümler (askeri bilgi harbi hariç) aynı zamanda bilgi terörü eylemlerinde de kullanılabilirler.

---

[22] Martin Libicki, **What Is Informatıon Warfare?,** National Defense University, 1995, http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html, s. 1

[23] Reto E. Haeni, **Information Warfare,** http://www.islab.oregonstate.edu/documents/Papers/iware.pdf, s. 2

2.2.0 Bireysel Bilgi Savaşı

Bu grupta yer alan saldırılar bir bireyin elektronik mahremiyetini hedef almaktadır. Bir kişiye ait tüm, dijital kayıtları ve veri tabanlı girişleri tehdit eden bu saldırılar; bilgi nerede saklı olursa olsun onu bulup zarar vermeye yöneliktir. Ortalama bir bilgisayar kullanıcısının sakladığı bilgi üzerindeki kontrolü ne yazık ki çok fazla değildir. Bizi ilgili olan, doğru yada yanlış bilgilerin tamamını kontrol edemeyiz. "ABD'de yapılan bir araştırmaya göre, bilgisayar kullanıcılarının %78'i böyle bir saldırı sonucu bilgi kaybına uğramıştır."[24]

Geçmişte, bir kişi hakkında bilgi almak için çalışan bir ajan, minyatür kamera ya da mikrofon kullanmak zorundaydı. Günümüz ajanları ise, o cihazların daha da küçülmüş modellerini kullanmakla beraber, çoğunlukla zaten varolan verilere ulaşarak, her türlü bilgiyi edinmektedir. Artık ajanların bilgiye ulaşmak için kişinin yakınına veya hayatının içine girmesine bile gerek yoktur. İnsanlar bilişim sistemlerini kullandıkları her anda farkında olmadan arkalarında kendi hayatlarına dair bilgiler ve ipuçları bırakır. Birisine şantaj yapmak için artık onu aylar boyu takip etmek gerekmiyor, telefon hatlarının ucunda bulunan bir bilgisayardan pek çok şey öğrenmek mümkün.

Hakkımızdaki bilgilerin, çevreye yayılmasından endişe duymak zorunda mıyız? Dürüst olmak gerekir ki; hiçbirimiz kredi kartı borçlarımızın, banka hesap numaralarımızın, kullandığımız krediler gibi finans yatırımlarımızın, tıbbi kayıtlarımızın, sabıka kaydımızın, mahkeme kayıtlarımızın, kiraladığımız video kaset ve CD kayıtlarımızın yada herhangi bir kişisel bilgimizin gazetede yayınlanmasını, arkadaşlarımıza ve ailemize yayılmasını veya internet üzerinden tüm dünyada dağıtılmasını istemeyiz. Daha da kötüsü ya birisi hakkımızda bir bilgi yaratıp, bunun doğru olduğunu söylerse, bütün ömrümüzü bunu temizlemek için harcayabiliriz.

Bir sabah uyandığımızda kredi kartı hesaplarımızın tükendiğini, numaralarımızın geçersiz olduğunu, artık sigortalı olmadığımızı, sahibi olduğumuz evin hiç tanımadığımız bir kişiye ait olduğunu görebiliriz. Evinizin, İnterpol' ün

[24] Haeni, a.g.m., s. 4

bilgisayarlarında azılı bir terörist olarak göründüğünüz için polis tarafından basıldığını düşünün. Aleyhinizdeki onca delile rağmen, terörist olmadığınızı nasıl ispatlardınız?

Yukarıda aktarılanlar abartılmış bir bilim kurgu hikayesi olarak görülebilir. Ancak şunu unutmamak gerekir ki günümüz teknolojisiyle bunu yapmak mümkündür. Hatta konusunda uzmanlaşmış bir kişi için çocuk oyuncağı bile sayılabilir.

Kendimizi bilgi savaşına / terörüne karşı korumalıyız. Unutmamalıyız ki bilişim sistemleri masum amaçlarla kullanılsa dahi, kullanıcıyla ilgili bilgileri dışarı sızdırırlar.[*] Elimizdeki bilginin sızmasını veya biz farkında olmadan çalınmasını engelleyebilmek için almamız gereken önlemler çalışmanın ilerleyen bölümlerinde aktarılacaktır.

2.2.1 Tüzel Bilgi Savaşı

Bu grup rekabeti tanımlar. Daha iyi bir deyişle, tüzel bilgi savaşı terimi dünyadaki şirketler ve kuruluşlar arasında geçen günümüz savaşını tanımlar. Rakip kuruluşların birbirlerine yaptıkları saldırılar bu gruba girmektedir.

Bir milyon dolarlık yatırım yapan bir şirketin, rakibinin sistemini kırarak, on beş milyon dolar değerindeki projesini ele geçirmesi ve rakibini ortadan kaldırması mümkündür. Ayrıca, rakibinin projesini ele geçirmekle kalmayıp, rakip şirketin yeni ürünle piyasaya ilk giren şirket olmamasını sağlamak için kaza ya da virüs süsü vererek, rakip şirketin konuyla ilgili tüm verilerini de yok edebilir.

"Bu tarz savaş aslında yeni değildir. Geçmişi Amerika-Rusya arasındaki soğuk savaş dönemine uzanmaktadır. O dönemki ajanların bilgi toplama çalışmalarına benzemektedir."[25]

Bu grupta yer alan savaş sadece bilgi edinmek üzerine değil doğru yada yanlış bilgi yaymak üzerine de kurgulanmaktadır. Bilgisayar ve donanımlarını üreten iki

[*] Bilgi işleyen elektriksel ve elektronik teçhizattan istenmeyen sızıntılar TEMPEST (Temporary Emanations and Spurious Transmission) olarak adlandırılır. Bir diğer adı da "Elektromanyetik Sızıntı" dır.

[25] Haeni, a.g.m., s. 5

şirketi ele alalım. X şirketi, rakibi olan Y şirketinin ürettiği ve çok satılan bir otomobil markasında kullanılan mikroçiplerin doğru hesaplamalar yapmadığını ve yanlış sonuçlar doğurduğu yalanını, medyaya ve internete isimsiz e-maillerle el altından yayar. Haberin kişiden kişiye yayılmasıyla gazeteler ve dergiler bahsedilen mikroçipleri kullanan otomobil fabrikasının ürettiği araçların %60'ında mikroçipteki hata nedeniyle hava yastıklarının kaza sonrasında açılmadığını yazmaya başlar... Otomobil firması aksini nasıl ispatlar? Siz olsanız bu otomobili satın alırmısınız? Sistemin çalışıp çalışmadığını kendi kendinize test etme şansınız yoktur. Üretici firmaya güvenmek zorundasınız. Peki siz üretici firmanın genel müdürü olsanız araçlarınızda bu mikroçipi kullanmaya devam edermisiniz? Eğer şirketler müşterilerinin güvenini kaybederlerse aynı zamanda milyon dolarlar da kaybederler.

Mikroçipin kullanıldığı aracın satışları birden alt üst olur. Bilgisayar şirketiyle otomobil üreticisi arasındaki bağlar kopar ve X şirketi tek bir kuruş bile harcamadan pazardaki payını hızla arttırır.

2.2.2 Global Bilgi Savaşı

Bu grupta yer alan saldırı türleri, endüstri, global ekonomi güçlerini, tüm ülke ve devletleri hedef almaktadır. Tüzel bilgi savaşından farkı sadece araştırma verileri üzerine değil, devletler arası sırların çalınmasına kadar uzanan bir çizgide gelişmesidir.

Dünya için en tehlikeli olabilecek tür bilgi savaşı da bu gruptur. Artık konu para kaybı ya da kişisel bilgi kaybından öte tüm dünyayı etkileyecek zararları içermektedir. İkinci ve üçüncü dünya ülkeleri silahlanmaya her yıl milyarlarca dolar harcıyorlar. Peki ya bir gün bir ülke bu harcadığı rakamın onda birini bilgi savaşı silahlarına yatırırsa?

Bilgi savaşı her geçen gün, teröristlere ve birbirine düşman devletlere yeni ufuklar açmakta, yeni yok etme olanakları sunmaktadır. Örneğin, gerekli donanıma sahip bir diktatör Amerika'nın banka sistemini göçertip, Wall Street'i yok edebilir.

2.2.3 Askeri Bilgi Harbi

"Bir ordu kendisi ve düşman hakkında ne kadar çok bilgi sahibi olursa, harpte o kadar başarılı olur". – Sun Tzu[*]

Düşman yada olası düşman hakkında bilgi edinmenin önemi çok eskilere dayanır. Konunun bu çalışmayı ilgilendiren bölümü ise askeri bilgi harbinin de artık günümüz bilişim teknolojileriyle yapılıyor olmasıdır. Ordular artık düşmanlarıyla ilgili bilgiyi casus ve ajanlar vasıtasıyla değil uzaydan düşman bölgelerini seyreden uydular, küresel yer tespit sistemleri, aldatma-karıştırma sistemleri ve bilgi iletişim sistemleri gibi modern ve teknolojik aygıtlarla elde etmektedir.

Ordular, karşılarındaki kuvvetle ilgili ne kadar çok bilgi sahibi olursa gerçekleşecek olan harpten o kadar başarılı çıkarlar. Körfez savaşlarında Amerikan ordusunun Irak ordusuyla ilgili bilgileri üstün teknolojili aygıtlarla elde ettiğini biliyoruz. Bu durum Amerikan ordusuna hedef olma sahasına girmeden, binlerce kilometre uzaktan Irak'ın askeri ve stratejik hedeflerini mümkün olan en az sivil can kaybıyla vurma imkanı sağlamıştır.

Düşmanın savaş alanı ve muhtemel karşı koyma silahları önceden biliniyorsa savaşta sürprizlerle karşılaşma ihtimali azalır. Günümüzde bütün ordular olası düşmanlarına karşı bir bilgi savaşı içindedir. Bilgi çağında bir ülkenin ne kadar tankı ve / veya uçağı olduğu değil, bilgi harbinde ne kadar gelişmiş olduğu ön planda tutulacaktır. Günümüz teknolojisiyle, bir kurşun bile kullanmadan düşman bir ülkeyi alaşağı etmek mümkündür. (Bkz. Bilgi Harbi Senaryosu, s.34)

2.3 HARP AMAÇLI BİLGİ SAVAŞI YÖNTEMLERİ

Bilgi savaşlarında kullanılan çeşitli yöntemler mevcuttur. Bunların bazıları harp amaçlı bazıları ise terör amaçlıdır. Harp amaçlı yöntemlerde gerçekleştirilen eylemler silah tabanlı görünse de, asıl hizmeti bu silahların kusursuz çalışmalarını sağlayan bilişim teknolojileri vermektedir. Çalışmanın önceki bölümlerinde de belirtildiği gibi savaş kelimesinin yan anlamlarıyla (mücadele, rekabet, vb.)

[*] Çinli savaşçı, filozof. Çin'de i.ö. 5 ile 3. yüzyıllar arasında yaşadığı sanılıyor. "Savaş sanatı" adlı eserin sahibi.

karışmaması amacıyla, bu bölümdeki alt başlıklarda "savaş" yerine "harp" terimi kullanılacaktır.

2.3.0 Komuta Kontrol Harbi (C2W)

"Komuta kontrol harbi bilgi savaşını harp sahasında uygulayan ve fiziksel imhaya entegre eden bir askeri stratejidir."[26] Amacı, düşmanın komuta heyeti ile kuvvet arasındaki komuta zincirinin kırılmasıdır. Uygulama iki türlü yapılmaktadır. Bunlar; Komuta heyeti / merkezinin imhası veya elektronik olarak devre dışı bırakılması ve muhabere ve link devrelerinin imhası / elektronik olarak devre dışı bırakılmasıdır.

Komuta Kontrol harbinin en yakın uygulaması körfez savaşında izlenmiştir. Amerikan ve İngiliz birliklerince fiili saldırı öncesinde komuta yapısındaki bağlantının bozulması maksadıyla, komuta yerleri, komuta kontrol sistemleri ve bu sistemin düğüm noktaları yüksek isabetli bombalar vasıtasıyla imha edilmiştir.

Komuta Kontrol harbi, Komuta Kontrol Taarruzu ve Komuta Kontrol Savunması olarak ikiye ayrılır.

A) Komuta Kontrol Taarruzu

Taarruza yönelik komuta kontrol harbinin amacı; hem bilgi akışı, hem de durum kavrayışı açısından düşman komuta kontrolünün felç edilmesidir. Komuta kontrol taarruzunu iki alt başlığa ayırabiliriz.

i) Başı Yok Etme

Savaşlar komutanların öngördüğü şekilde gerçekleşir. Bir ordunun harp sahasında gerçekleştireceği manevralara komutanlar karar verir. Eğer komutanla alt birimler arasındaki iletişim kesilirse düşmana büyük bir zarar verilmiş olur.

Komutanın başına nişan alma aslında eksi bir harp stratejisidir. Yeni olan ise komutana ulaşılabilirlikte meydana gelen değişimdir. Artık komutanı harp sahasında bulmaya çalışmak yerine, iletişimini kesmek daha kolay ve daha akılcıdır. Komutanın merkezle olan ilişkisini kesmek onun nerede olduğundan daha önemlidir.

[26] Libicki, a.g.m., s. 5

"Komuta Kontrol Merkezinin yerinin tespit edilmesi yeni hedeflerin ortaya çıkmasına neden olur. Zamanında yapılan bir taarruz imhanın ani etkisinin ötesinde harekata etki eder. Sistemler güç sistemlerinin kesilmesiyle devre dışı bırakılabilir, elektromanyetik karıştırmayla veya bilgisayar virüsleriyle güvenilmez hale getirilebilir."[27]

ii) Gövdeyi Yok Etme

"Modern silahlı kuvvetler 19. yüzyılın ortalarından itibaren elektronik ve 1920 den bu yana telsiz muharebesine bağımlı hale geldi. Bu muharebeyi kesersek, komuta ve kontrol sistemi devre dışı kalır"[28] Baş ve gövde arasındaki bağı keserseniz gövde hareketsiz kalır. Alt birimlerdeki askerler ne yapacaklarını şaşırmış durumda iken kolay birer av haline gelir. Körfez savaşında müttefik güçlerinin uyguladığı en büyük strateji budur. Uydulardan aldıkları kesin görüntüler vasıtası ile modern füzeler bilgisayarlar vasıtasıyla Irak'ın iletişim sistemlerini vurdu. Komuta kontrol sistemini kaybeden Irak komutanları alt birimlere bilgi aktaramaz hale geldi. Baştan ayrılmış hareketsiz gövde ise Amerikan güçleri için basit birer av haline geldi. Libicki makalesinde Irak ön saflarındaki iletişimi kesilmiş askeri güçleri *oturan ördek*[*] olarak tanımlar.

B) Komuta Kontrol Savunması

Komuta kontrol savunması, dost kuvvetlerin komuta kontrol sisteminin korunması ve düşmanın bozucu çalışmalarının etkisiz kılınmasını hedefler. Burada amaç; düşman mukavemeti ile karşılaşıldığında dahi, dost kuvvetlerin zaiyatını asgaride tutmaktır. Ayrıca dost kuvvetlerin harekatı sırasında, kamuoyunu ve personelin moralini etkilemeye yönelik düşman propagandasını önlemek de komuta kontrol savunmasının amacıdır.

2.3.1 İstihbarat Temelli Harp (IBW)

İstihbarat temelli harp; taktik resmin elde edilmesi maksadıyla kullanılan tüm vasıtalar ve sensörler ile bu bilgileri işleyen, değerlendiren ve birliklere yayan sistemleri kapsamaktadır.

---

[27] Libicki, a.g.m., s. 5
[28] Libicki, a.g.m., s. 7
[*] Front line troops were sitting ducks for U.S. air and ground attack.

İstihbarat temelli harbin amacı; savaşın bilinen bir parçası olan sürprizleri engellemek ve komutana harekat planlarının şekillendirilmesinde yardımcı olmaktır. İyi bir istihbarat, harekatın koordinasyonunu ve senkronizasyonunu sağlar, muharebe başladığında; bir tarafta görevi anlamış ve yürütmeye hazır birlikler varken, diğer tarafta, karışıklık ve şok yaşayan birlikler yer alır.

Bugünün bilgi sistemleri geçmişin çok ilerisine gitmiş ve harp sahasıyla ilgili anlık bilgileri verebilecek duruma gelmiştir. Geleceğin harp sahası ortamında harp sahasını bütünü ile kapsayacak çeşitli seviyelerde sensörler yer alacaktır.

İstihbarat temelli harp başlığı, saldırı amaçlı ve savunma amaçlı olmak üzere iki alt başlığa ayrılabilir.

A) Saldırı Amaçlı İstihbarat Harbi:

Harp sırasında yapılacak karşı saldırılar çok önemlidir. Ancak körü körüne girişilecek bir saldırı büyük kayıplara neden olabilir. Bilişim sistemlerinin istihbarat alanında kat ettiği yol artık teknolojiyi elinde bulundurana büyük avantajlar sağlamaktadır. Eskiden ordular karşı tarafla ilgili bilgiyi günümüzdeki kadar net elde edemezlerdi. Karşı tarafın tank birliğini tespit eden tarafın çatışmaya girmek için hazırda beklemekten başka yapacağı bir şey yoktu. Günümüzde ise bilişim sistemlerinin sunduğu imkanlardan faydalanan bir ordu karşı tarafın her bir tankını ve tam mevkiini ayrı ayrı elde edebilir. Bunu yapabilen taraf çatışma mesafesine hiç girmeden diğer tarafın bütün silahlarını akıllı füzelerle yok edebilir.

B) Savunma Amaçlı İstihbarat Harbi

Yukarıda aktarılan başlığın tam tersine bir mantıkla işler. Ordular kendilerine veya müttefiklerine karşı yapılabilecek her türlü saldırıya önceden hazırlıklı olmak durumundadırlar. Hazır olmanın en önemli evresi ise kendisine ve müttefiklerine karşı ne yapılabileceği hakkında bilgi sahibi olmaktır. Donanımlı bir ordu düşmanın bütün hareketlerini uydu görüntüleriyle izleyebilir, sistemlerine yerleştirmiş olduğu virüsler vasıtası ile bilgilerini elde edebilir ve düşmanın gerçekleştirmesi muhtemel bir saldırıyı daha düşünce aşamasında iken bertaraf edebilir.

2.3.2 Psikolojik Harp

Bu harp çeşidinde bilginin insan fikir ve düşüncelerinde belirli istekler doğrultusunda işlenmesi mantığı yatmaktadır. Psikolojik harp bir çok vasıta ile gerçekleştirilebilir. En önemli iki olgusu halka karşı yapılan ve askerlere karşı yapılan psikolojik harptir.

Halka karşı yapılan psikolojik harpte en önemli araç medyadır. Bir ülkenin lideri küresel yayın şirketlerinin ağlarını kullanarak binlerce kilometre uzaktaki düşman ülke halkına seslenebilir ve belirli yöntemler kullanarak halkı kendi yanına çekmeyi deneyebilir. Bunun en yakın örneğini son Körfez savaşında gördük. A. B. D başkanı Bush CNN den yaptığı konuşmalarla Irak halkına seslendi ve bölgeye savaşmak için değil, Irak halkına yardım için gittiklerini, onlara özgürlüklerini vereceklerini belirterek halktan Amerikan güçlerine karşı koymamalarını ve onlarla beraber Saddam'a karşı hareket etmelerini istedi. Amerika tarafında yaptığı konuşmalarda ise kendi halkına terörü ortadan kaldırmak amacıyla savaşacaklarını belirtiyordu.

Uygulanabilecek bir başka taktik ise ülkenin gelişmiş silah sistemlerini yayınlarda kullanarak karşı ülkede bir korku, endişe ortamı yaratmaktır. Körfez savaşları öncesinde ve süresince CNN vtr lerinde hep Amerikan silahlarının hedefi tam 12'den vurması vb. görüntüler kullanılmıştır.

Askerlere karşı yapılan psikolojik savaşlarda ise yine medya ön safhayı almaktadır. Değişik yayınlarla karşı ülke askerlerinin zihinlerine ne için ve kimin için savaştıkları sorusu sokulmaya çalışılabilir. Alternatif bir yol ise göz korkusu vermek veya ödüllendirmek olabilir. "Körfez savaşında koalisyon güçleri Iraklı askerleri, kullandıkları savaş araçlarını saf dışı bırakmaları halinde daha uzun yaşayacakları konusunda ikna ettiler. Koalisyonun ikna yöntemi az evvel bir çatışma sırasında benzeri bir askeri aracı imha etmiş olan silahlarla destekleniyordu"[29]

[29] Libicki, a.g.m., s. 19

2.3.3 Simule Harp

Simule harp kavramı tamamı ile olmasa da kısmen psikolojik harbin bir alt başlığı olarak da kullanılabilir. Simule harbin amacı, harbin daha oluşmadan taraflara ait bilgilerle bilgisayarda simule edilerek oynanması ve sonucun karşı ülkenin aleyhine gerçekleşeceği izlenimini vermektir.

Simule harp aynı zamanda orduların askerlerini savaş ortamına hazırlaması ve eğitmesi açısından da çok önemlidir. Askerlerin harp oyunu diye adlandırdıkları bu olgu günümüzde birçok modern ordu tarafından kullanılmaktadır. Bilgisayar ortamında yaratılan sanal harp sahasında gerçeğini aratmayan harp senaryoları yazılmakta ve bu senaryoların gerçekleşmesi durumunda alınacak tedbirler ve sergilenecek savaş taktikleri belirlenmektedir.

Gerçek savaş kirli, sıkıcı ve tehlikelidir. Simule edilmiş çatışma bunlardan hiçbiri değildir. Simule savaşta ölüm riski yoktur. Bu yüzden taraflar yapacakları mantıklı hamlelerin yanı sıra alabilecekleri azami riski de üzerlerine alırlar. Amaç gerçek bir savaş ortamında kusursuz kararlar verebilecek mükemmel askerler yaratmaktır.

2.4 ÇOK AMAÇLI BİLGİ SAVAŞI YÖNTEMLERİ

Başlıktan da anlaşılacağı gibi bu başlık altında toplanan bilgi savaşı yöntemleri birden fazla amaca hizmet etmektedir. Bunlar harp amacı, rekabet - mücadele amacı ve terör amacı güdebilir.

2.4.0 Ekonomik Bilgi Savaşı / Terörü (EIW)

Bu savaş şekli bilgi savaşıyla ekonomik savaşın bir birleşimidir. Devletler askeri alanda olduğu kadar ekonomik alanda da büyük mücadele içerisindedir. Küresel şirketler de rakipleri ile ekonomik alanda mücadele ederler. Bu mücadele sırasında rakibine yada düşmanına karşı üstün duruma gelip ona pes dedirtmek için uygulanacak çeşitli yöntemler vardır. Ekonomik bilgi savaşı bu yöntemlerden biridir.

Konuyu iki alt başlığa ayırabiliriz. Bilgi blokajı ve Bilgi emperyalizmi.

A) Bilgi Blokajı (Kesintisi)

Bilgi blokajı, ekonomik blokajın bir varyantıdır. Bilgi blokajının amacı, hedefteki ülkeyi yada şirketi bir bilgi karanlığında bırakmak ve uzun vadede bilgi alış verişinin faydalarından yararlanmasını engellemektir.

"Bilgi satışı ve bilgi erişimi günümüzde ülkelere yüklü miktarda ekonomik değer olarak yansımaktadır. Bilgi kaynağına erişimi engellemek ülkelerin bu suretle ekonomik çöküntü içerisine girmesine neden olacaktır."[30]

Bir ulusun ya da bir şirketin fiziksel akışına dokunmayıp sadece bilgi akışını bloke etmek, ticari alanda ona bir tek zarar verir. Elektronik ortamdaki ticareti yok olur. Bu duruma düşmüş bir ülkenin yazılı alandaki fiziksel akış materyalleri sağlam kalır, bilgiler CD-ROM'lar ile aktarılabilir, ancak gerçek zamanlı etkileşimler ortadan tamamı ile kalkar. Bankalar, borsalar, polis ofisleri, hastaneler, taşımacılık sistemi, enerji sistemi, vb. sistemler üstleriyle ve birbirleriyle olan anlık bağı tamamı ile kaybederler. Bunun gibi bir durum bir ülke ekonomisine çok büyük zararlar verebilir. Hatta ekonomik durumuna göre bir ülkeyi tamamıyla batırabilir. Amerika'da bilgi iletişim sistemlerine bulaşan herhangi bir virüsün bilgi akışını sadece bir günlüğüne bloke etmesinin bedeli milyar dolarlarla ölçülmektedir. Organize bir saldırı ile bilgi akışının bir aylığına kesildiğini düşünün. Acaba dünyadaki kaç ekonomi bu durumu etkilenmeden atlatabilir?

B) Bilgi Emperyalizmi

Bilgi emperyalizmine inanmak demek günümüzün ekonomik emperyalizmine inanmak demektir. Ülkeler ya da şirketler bazı belirli endüstrilerde diğerlerine göre daha uzman hale gelirler. O endüstri dalında daha kusursuz hizmet sunup çalışanlarına daha iyi bir çalışma ortamı ve daha iyi maaşlar sunarlar.

Belirli bir endüstri konusunda en iyi olan ülkeyle / şirketle çalışmak sizi müşteriye en yakın hale getirir. Bu tip endüstrilerde görev almak ise insanların en büyük ideali haline gelir. Amerika'daki silikon vadisini ele alalım. Dünyanın bilişim konusundaki bütün lider şirketleri bu bölgededir. Silikon vadisinden bir şirketle çalışmak size çok büyük avantajlar sağlayabilir. Konuda uzman olan insanlar da bu

[30] Harp Akademileri Komutanlığı, a.g.e., s. 14

bölgede iş bulmak isterler (kalifiye bir programcının sıradan bir yazılım şirketinde çalışmak yerine Microsoft ta çalışmak istemesi gibi).

Bu durum bir zaman sonra bir tekelleşmeyi meydana getirir. Belirli konudaki bilgi tek bir noktadan yayılmaya başlar ve diğerlerini kendine bağımlı bırakır. Bir ülkenin en iyi olduğu endüstri alanı onu piyasada tek yapar. Örneğin dünyadaki en iyi yazılımcılar Hintlilerdir, ancak Hindistan dünyanın en iyi yazılım üreten ülkesi değildir, çünkü eğitimini tamamlayanlar soluğu hep Amerika'da alırlar. Hindistan ise bilgi işlem eğitimi alnında lider olmuştur. Günümüzde yazılım konusunda uzmanlaşmak isteyen insanların çoğu eğitimini Amerika'da değil Hindistan'da almak istemektedir.

2.4.1 Sayısal Bilgi Savaşı (DDW) / Terörü

"Sayısal bilgi savaşı askeri, politik, ekonomik ya da kişisel amaçların elde edilmesi için bir bilgisayar sistemine yada ağına gizlice zararlı bilgisayar yazılımı sokulmasıdır."[31] Konu dört alt başlığa ayrılabilir. Bu başlık altında toplanan tüm bölümlerde sayısal bilgi savaşı / terörü silahları kullanılır. Bu silahlar çalışmanın ilerleyen bölümlerinde aktarılacaktır. (Bkz. Sayısal bilgi savaşı / terörü silahları, s.29)

A) Bilgisayar Korsan Savaşı / Terörü (HW)

Hacker denilen bilgisayar korsanlarının gerçekleştirdiği, işlemci temelli sistemlere yapılan saldırıları içeren savaş türüdür.

Hacker savaşının hedefi ülkeler, ordular, şirketler ve hatta bireyler olabilir. Asıl varoluş amacı bilgi edinmek olsa da günümüzde konuda uzmanlaşmış kişiler tarafından saldırı amaçlı olarak kullanılmaktadır.

Hacker savaşına karşı korunma zorunluluğu hacker'lık olgusunu ikiye bölmüştür. Günümüzde hacker'lar siyah hacker ve beyaz hacker olarak (white and black hacker) ikiye ayrılır.

---

[31] Lawrence G. Downs. Jr., **Digital Data Warfare: Using Malicious Computer Code As A Weapon,** Air University, 1995, s. 1

Beyaz hacker'lar büyük bir şirketin ana bilgisayarı vb. işlemci tabanlı sistemleri dışarıdan gelecek saldırılara karşı korumakla görevli kişilerdir. Savundukları sistemin sahibi tarafından maaş karşılığı çalıştırılırlar. Yaptıkları iş bir saldırıyı bertaraf edip gerekirse karşı saldırıyla cevap vermektir.

Siyah hacker'lar olarak adlandırılan grup ise bilişim teknolojileri alanındaki uzmanlıklarını bilişim kaosu yaratmak için kullanırlar. Kim olduklarını saklı tutmak için eylemlerini çoğu zaman takma isimle (nickname) gerçekleştirirler. Bu tip hacker'lar kimi zaman bir terör örgütü üyesi[*], kimi zaman intikam almaya çalışan bir çılgın ya da kendi deyimiyle bir kahraman, kimi zaman sadece hoşuna gittiği için bunu yapan bir kişi, kimi zamansa neler yapabileceğini merak ettiği için sistemlere saldıran kişiler olabilir. Türkiye'de henüz büyük bir örgütlenme olmamakla birlikte (var olan birkaç tanesi hariç), yurt dışında bazı büyük hacker örgütlerinin bulunduğu bilinmektedir. İsteklerini yerine getirtmek veya tepkilerini dile getirmek için belirli bir adrese sistemli olarak saldırabilirler. Yaptıkları eylem hacklemek olarak adlandırılır ve çoğu zaman sızdıkları sistemin açılış sayfasını mesajlarını içeren başka bir sayfa ile değiştirirler.

Türk hacker'lar tarafından gerçekleştirildiği bilinen son saldırılardan birisi Cezayir depremi nedeniyle yurtdışı internet bağlantımızın kopması üzerine Türk Telekom'a ceza vermek amacıyla Türk Telekom'a ait web sitesinin hack edilmesi olayıdır. "Yakın geçmişte olan bir başka saldırıda da, "Unknown Deface Team"adlı bir Türk hacker grubu Irak'ta 11 askerimizin esir alınmasına misilleme olarak NASA'nın sayfasını hacklemiştir."[32]

Hackerların saldırı yöntemlerine genel bir bakış sergilersek başlıca şu yöntemler karşımıza çıkar.

i) Fingerprinting

Fingerprinting tanımı aslında karşı taraf hakkında bilgi toplamaktan ibarettir. Bir saldırı yöntemi değildir sadece karşı sistem hakkında bilgi verir ve saldırı için doğru seçimlerin yapılmasına olanak sağlar. Çalışan işletim sistemi, çalışan

[*] Bkz. Siber Terör, s. 28

[32] Turgay Seçen, **Türk Hacker'lar - 1,** turk.internet.com, 19.09.2003
URL:http://turk.internet.com/haber/yazigoster.php3?yaziid=8249

programlar, işletim sistemi versiyonu gibi bilgiler sayesinde karşı sistemin güvenlik açıkları kolayca tespit edilip saldırı uygulanabilir. Bir çok çeşidi ve yöntemi vardır. En basit örneği, FTP Server'larından vermek mümkündür. FTP formatına göre karşı tarafa gönderilen "SYST" mesajı karşı tarafın işletim sistemi hakkında bilgi verir. "Örneğin; "anonymous" (anonim) olarak ftp.sau.edu.tr adresine bağlanıp, "command" (komut) ekranına SYST yazılırsa sonuç aşağıdaki gibi olacaktır:

Connected to ftp.sau.edu.tr

SYST
215 UNIX Type: L8
Host Type (S): UNIX Standart"[33]

Bu sayede karşı tarafta UNIX Standart yüklü bir makinenin olduğunu öğrenmiş bulunmaktayız.

ii) Port Scanning

Port Scanning (Port Tarama) adı verilen yöntem de karşı taraf hakkında bilgi toplamayla alakalı bir işlemdir. Bu işlemde aynı Fingerprinting gibi protokol formatına dayanır ve karşı sistemde açık olan portları bulmamızı sağlar.Bu sayede Fingerprinting 'ten elde edemediğimiz bilgileri bulabiliriz. Örneğin karşı tarafın 135 no'lu portu açıksa muhtemel bir Windows İşletim sistemiyle karşı karşıya olduğumuzu varsayabiliriz. Ya da bir başka örnek olarak karşı tarafın eğer 80'inci portu açıksa bu makinenin da bir HTTP Server olduğunu varsayabiliriz. Port Tarama yönetimde bilgi toplama portların ne işe yaradıklarını ve genel kullanımlarını bilmekle alakalıdır. Bu şekilde karşı sistemin zayıflıkları bile bulunabilir.

iii) Network Sniffing

Network Sniffing adı verilen yöntem ağda dolaşan paketlerin görüntülenmesi ve kaydedilmesine olanak sağlayan bir yöntemdir. Bilindiği gibi çoğu yerel ağ sisteminin (LAN) temelini Ethernet oluşturmaktadır. Ethernet ilk tasarlanırken mühendisler kendi protokollerini test etmek için sniffer programlarını

[33] Sümer Cip, **Hacking Yöntemlerine Genel Bir Bakış,** Olympos Security Güvenlik Portalı URL:http://www.olympos.org/article/articleprint/1440/-1/10

kullanıyorlardı. Fakat günümüzde Network Sniffing genellikle kötü amaçlara hizmet ediyor. Ethernet protokolü veriyi olduğu gibi gönderir, yani veriye herhangi bir şifreleme uygulamaz. İşte bu aşamada Sniffing daha da kolaylaşır. Ayrıca Ethernet protokolü gönderilen bu şifrelenmemiş veriyi bağlı olan tüm düğümlere (node) gönderir. Yani aslında aynı non-switched bir LAN da birbirlerine bağlı iki bilgisayarın birbirlerinin ağ trafiğini incelemeleri, sadece NIC (Network Interface Card) bir değişikliğe bağlıdır. Bu değişikliğin uygulandığı bir NIC üzerine gelen tüm bilgiyi filtrelemeden alır. Yani bağlı olduğu tüm ağ trafiğini inceleyebilir. Bu duruma gelmiş bir NIC 'e "promiscuous mode"'a geçmiş denilir. NIC'in farklı amaçlara hizmet etmesi için farklı filtrelerine metotları vardır.

iv) DoS (Denial of Service)

DoS saldırıları günümüzde en yaygın kullanılan saldırı biçimlerinden biridir. Çünkü bir çok saldırı yöntemini içinde barındırır. DoS saldırıları genelde bir ağa ya da kaynağa ulaşımı engellemek için kullanılır. Kendi içinde mantıksal olarak ikiye ayırmak mümkündür: Program tabanlı DoS saldırıları ve Network tabanlı DoS saldırıları. Bu iki saldırıda da iki yöntem kullanılabilir birisi "flooding" diğeri "exploiting". FIooding'te kullanıcı kurbana çok sayıda paket yollayarak belli bir işlemi çalışamaz duruma getirir. Exploiting yönteminde ise kurbanda çalışan herhangi bir program hedef alınıp bu programın açıklarından faydalanarak program, kullanılamaz hale gelir.

v) TCP/IP Hijacking

TCP/IP Hijacking bir A sisteminin B sistemi ile C sistemi arasında kurulan bağlantıya sızarak kendini C sistemine B sistemi olarak göstermesi demektir. Bu işlemi uygulamak için öncelikle A sistemi ile B sistemi aynı ağ üzerinde olmalıdır. TCP her paketin karşı tarafa ulaşıp ulaşmadığını kontrol eden ve 2. olarak gitmesi gereken paketin 1. olarak gitmesi gerekenden daha önce gitmesi gibi senkronizasyon problemlerinin aşılması için her pakete belli senkronizasyon numaraları (sequence number) veren güvenilir bir protokoldür. Bu numaralar sayesinde iletişimde bulunan iki program gelen giden paketleri sırasına göre alıp sırasına göre işleyebilir. Eğer A sistemi "network sniffing" sayesinde B sisteminin tüm gelen giden paketlerini incelerse, B sisteminin C sistemiyle olan bağlantısında o andaki "sequence

number"'ını tahmin edebilir. Bu hesapladığı sequence number ve B sisteminin IPadresini source IP olarak kullanarak karşı tarafa bir paket yollarsa, C sistemi doğal olarak artık A sistemini B sistemi olarak algılayacaktır. Bu sırada B sistemi C sistemine bir paket gönderse bile aralarındaki senkronizasyon numaralarında hata oluştuğu için artık C sistemi B sistemini tanımayacaktır.

B) Semantik Hücumlar

Semantik hücuma uğramış bir bilgisayar sisteminin arızalı olduğu çoğu zaman farkına varılamaz. Amaç sistemin yanlış sonuç vermesini sağlamaktır. Semantik hücum bu yüzden daha çok karar verme sistemlerine uygulanır.

"Semantik hücuma maruz kalan sistem çalışmaya devam edecek ve doğru olarak çalıştığını kabul edecek (aksi takdirde semantik hücum bir hatadır), fakat gerçekle değişken olarak cevaplar üretecektir."[34]

Türkiye'de de 1999 depreminden sonra kurulması sıkça tartışılan deprem erken uyarı sistemini ele alalım. Bu sistem dünyanın gelişmiş diğer ülkelerinde olduğu gibi bilgisayar tabanlı olacak ve bilgiyi Türkiye geneline yayılmış sensörlerden alacak.

Bu tip sistemler depremi, gerçekleşmesinden birkaç saniye evvel farkına varır ve zararı en aza indirmek için bölgedeki tüm elektrik, doğal gaz vb. hatları keser. Deprem sonrası ise sensörlerden gelen verilere göre, kurtarma ekiplerine en büyük hasarın nerede oluşmuş olabileceğini bildirir.

Eğer bu sistem semantik bir hücuma uğrar ise eylemcinin planladığı ana kadar bunu anlamak neredeyse imkansızdır. Sistem sanki normal çalışıyormuş gibi görünür. Bir gün eylemcinin bilgisayarı başından tek bir tuşa basması ile normalde hiçbir şey olmadığı halde sistem deprem olduğunu varsayarak bölgedeki -yada eylemin büyüklüğüne göre tüm ülkedeki- elektriği, doğal gazı vb. hatları keser. Üretim durur. Bölgeye / ülkeye bir ölüm sessizliği hakim olur. Bölgede tam bir kaos ortamı yaşanır.

[34] Libicki, a.g.m. , s. 36

Bununla birlikte sistemin bu tip bir saldırıya uğradığını hemen olay anında belirlemek imkansız olabilir. Çoğu zaman alınan tedbir iş işten geçtikten sonra yürürlüğe girer. Saldırıya uğramış sistemin ve saldırının büyüklüğüne göre; sistemi ilk haline döndürmek günler alabilir.

C) Bilgi Terörizmi

Kişilere ait bilgilerin yasal olmayan yollarla çalınması demektir. Hacker savaşıyla çok karıştırılan bir kavramdır, ancak bilgi terörizmi hacker savaşından çok farklıdır. Bilgi terörizminin amacı hacker savaşında olduğu gibi sistemleri bozmak değil, sistemlerdeki açıkları kullanarak kişilere, şirketlere, ülkelere ait gizli bilgileri açığa çıkarmaktır.

"Bilgi terörizmini iletmekteki problem toplanan bilgilerin ne yapılacağının bilinmemesidir."[35] Bu bilgiler daha sonra tehdit ve şantaj amaçlı kullanılabilir. Çoğu insan kendine ait özel bilgilerin halka sunulmasını istemez.

D) Siber Terör

Siber terör, "bilgi sistemleri doğrultusunda elektronik araçların bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş amaçlı eylem ve etkinliktir."[36]

Eylemler, bilişim teknolojileri konusunda uzmanlaşmış hackerlar tarafından gerçekleştirilebilir ancak hacker savaşı ile farklıdır çünkü burada eylemi gerçekleştiren bir teröristtir. Hacker savaşında ise terör amacı gütmeyen sıradan insanlar da yer alabilirler.

Siber terör çağımızda terörizmin yeni yüzünü yansıtacaktır. Günümüz teknolojileri sayesinde teröristlerin bilgisayarları başından yapacakları bir saldırı ile "bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğal gazı kapatabilecekleri, bilgisayar sistemlerini

[35] Libicki, a.g.m. , s. 36
[36] Bünyamin Atıcı ve Çetin Gümüş, **Sanal Ortamda Gerçek Tehditler; Siber Terör – 1,** turk.internet.com, 08/12/2003 URL:http://turk.internet.com/haber/yazigoster.php3?yaziid=8838

karmakarışık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve finans sektörünü çökertebilecekleri, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dahilindedir."[37]

Günümüzde siber terörle mücadele etmek için bir çok ülkenin kurduğu resmi birimler görev yapmaktadır.

2.5 VAROLAN ve OLASI SAYISAL BİLGİ SAVAŞI/TERÖRÜ SİLAHLARI

Bilgi savaşları sırasında karşı tarafın sistemlerine sızmak, bilgilerini çalmak, terör eylemi yapmak vb. amaçlarla kullanılan yazılımlara ve diğer aygıtlara verilen ortak addır. Genelde bilgisayar tabanlıdırlar. Bilinen başlıca silahlar şunlardır:

2.5.0 Bilgisayar Virüsleri

"Virüs, kendisini daha geniş bir programın içine kopyalayan, ve bu programı değiştiren kod parçasıdır. Virüs ancak içinde bulunduğu program çalışınca aktif hale geçer. Program çalışınca, virüs kendisini tekrar etmeye başlar ve başka programlara da yayılarak, onları da etkiler."[38]

Bilgisayarların çökmesine, sabit diskleri silerek tüm bilgilerin kaybolmasına vb. bir çok soruna neden olabilirler.

Virüsler, bütün bilgisayar ve işlemci tabanlı ortamlara yayılabilirler. Bilgi Savaşlarında, sıklıkla kullanılan bir savaş aleti olmaları da bu anlamda şaşırtıcı değildir. İstihbarat teşkilatlarının ya da orduların, düşmanlarının telefon sistemlerine virüs yaymaları mümkündür. Bilgi savaşlarında kişisel bilgisayarlardan çok karşı tarafın iletişim sistemlerini (dijital telefon ağı gibi) hedef alabilirler.

---

[37] Mehmet Özcan, **Siber Terör,** turk.internet.com, 25/03/2002
URL:http://turk.internet.com/haber/yazigoster.php3?yaziid=4038
[38] Haeni, a.g.m., s. 10

2.5.1 Kurtlar

"Kurt bağımsız bir programdır. Genellikle kendisini, network (ağ) üzerindeki bir bilgisayardan ötekine kopyalayarak çoğalır. Virüslerden farklı olarak, diğer programlara etki etmez."[39]

Networklerin çökmesine, bilgilerin kaybolmasına, bağlantıların kesilmesine neden olabilir.

Kutlar, veri yok etmezler ancak, network içinde dolaşarak, iletişimi yok edebilir. Bir kutrun karakteri istendiği zamanda onu yazan ve yayan kişi tarafından değiştirilebilir. Böylelikle veri kaybı hatta daha kötüsü gerçekleşebilir.

2.5.2 Truva Atları

"Truva Atı, bir program içinde gizlenen ve gizli bir işlev yapan bir kod parçasıdır. Virüsleri ya da kurtları saklamak için kullanılan popüler bir mekanizmadır."[40]

Çoğunlukla e-maillerin içine yerleştirilerek yollanan truva atları, bir programın içine yerleşir ve o program çalıştırılana kadar, aktif hale geçmez. Truva atı aktif hale geçince, bir sistemdeki korunmasız host ve serverler hakkındaki bilgileri ele geçirir ve karşı tarafa bulduğu bilgileri yollar. Böylece eğer bilgisayarınıza bir truva atı gönderilirse, bilgisayarınız tamamıyla başka birisinin kontrolü altına geçer. Truva atını yollayan kişi, e-maillerinizi okuyabilir, CD-ROM'unuzu açıp kapatabilir, her türlü belgenize ulaşabilir, parolalı bilgilerinizi dahi kolaylıkla okuyabilir. Zekice yazılmış bir truva atı, kendisini asla belli etmeyeceği ve hiçbir iz bırakmayacağı için, onun nerede olduğunu bulmak neredeyse imkansızdır.

2.5.3 Mantık Bombası

"Bomba, virüs, kurt ya da başka bir sistemi yaymak için kullanılan bir truva atı türüdür. Bağımsız bir program ya da bir sistem programcısı tarafından yazılmış,

---

[39] Haeni, a.g.m., s. 10
[40] Haeni, a.g.m., s. 11

bir kod olabilir."[41]

Esas amaçları önceden üretilmiş virüs, kurt gibi programları aktif hale getirmektir.

Dışarıdan çalıştırılması mümkün olan mantık bombası, bir bilgisayarın hard disk ya da posta dokümanlarının formatını etkileyebilir.

Hemen hemen tüm dünyada yaygın olarak kullanılan network işletim sistemlerine üretici firma tarafından yerleştirilebilecek mantık bombaları aktif hale geldiklerinde söz konusu network işletim sisteminin kullanıldığı, banka ATM şebekesi, borsa bilgisayar ağı gibi, sistemlerin çökmesine yada bu sistemlerdeki gizli bilgilerin istenmeyen ellere geçmesine neden olabilecektir.

2.5.4 Tuzak Kapıları

"Tuzak kapısı ya da arka kapı, bir sistemin içine yaratıcısı tarafından yerleştirilen bir mekanizmadır. Tuzak kapısının fonksiyonu, yaratıcısının sistemin içine, normal sistem koruyucularını aşarak, sızmasını sağlamaktır."[42]

Mantık Bombalarında olduğu gibi, tüm sistem üreticilerinin böyle bir mekanizmayı başka ülkelere ihraç ettikleri yazılımların içine yerleştirmeleri mümkündür.

2.5.5 Chipping (Mikroçipler)

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

Günümüzde, içinde 5.000.000 transistör bulunduran devreler üretmek mümkündür. Bu fonksiyonlardan, kullanıcı yalnız teknik kataloğunda belirtilen

[41] Haeni, a.g.m., s. 11
[42] Haeni, a.g.m., s. 11

özellikleri kullanabilir ve bilebilir. Üretici tarafından ilave edilmiş diğer fonksiyonların, tespit edilmesi imkansız denecek kadar zordur.

Entegre devrelerin kullanıldığı her türlü elektronik cihaz, üretici firma tarafından kazandırılabilecek ilave fonksiyonlar yoluyla bilgi savaşına açıktır. Bu ilave fonksiyonlar, belirli bir radyo sinyali ile harekete geçirilebilir ve entegre devrenin bulunduğu kartı yakarak sistemi devre dışı bırakabilir.

2.5.6 Nano-Mekanikler ve Mikroplar

Günümüzde var olduklarına dair sağlam bir kanıt bulunmasa da karıncadan küçük mekanik robotlar ve silisyum yiyen mikroplar da geleceğin bilgi savaşı silahları olarak düşünülmektedir. Ayrıca NASA' da uzay araştırmaları için nano teknoloji üzerinde çalışmaktadır.

2.5.7 HERF (High Energy Radio Frequency) Topları

Belirli bir hedefe yüksek güçte yönlendirilmiş radyo sinyali göndererek hedefi elektronik olarak köreltebilen silahlardır. HERF silahları herhangi bir elektronik sisteme / bilgisayar sistemine karşı kullanılabilmekte, yüksek yoğunluklu elektromanyetik enerjiyi yönlendirilmiş olarak göndermekte ve o sistemde bulunan elektronik devreleri yakarak devre dışı bırakmaktadır.

HERF topu bir minibüsün içine monte edilebilir ve telefon santralleri, televizyon verici istasyonları ya da bir bilgisayar network sisteminin ana bilgisayarı üzerinde kullanılarak söz konusu sistemleri devre dışı bırakabilir.

"HERF Silahlarının Amerika Birleşik Devletleri ve Rusya Federasyonu'nda bulunduğu bilinmektedir."[43]

2.5.8 Elektromanyetik Pals Bombası (EMP)

"Elektro Manyetik Pals etkisi ilk kez nükleer silahların yüksek irtifa infilakında gözlemlenmiştir."[44] Elektro Manyetik Pals, nano saniyelerle ifade edilen kısa zaman dilimlerinde, çok yoğun olarak ortaya çıkan ve geniş bir sahaya yayılan

[43] Harp Akademileri Komutanlığı, a.g.e. s. 18
[44] Harp Akademileri Komutanlığı, a.g.e. ss. 18-19

bir elektromanyetik şok dalgası olarak tanımlanabilir. Bu şok dalgasının meydana getirdiği güçlü manyetik alan, etki sahası içindeki elektronik devreler, kablolar ve her türlü iletken madde üzerinde kilo voltlar seviyesinde voltaj oluşturmaktadır.

Elektro Manyetik Pals etkisine maruz kalan bilgisayar sistemleri, muhabere cihazları, radarlar ve bünyesinde elektronik devre bulunan, her türlü cihaz hasara uğrayacaktır. Elektronik cihazların Elektro Manyetik Pals etkisine karşı yalıtılmaları da oldukça zordur. Muhabere ve radar cihazlarının antenleri, bilgisayar networklerinin kabloları ve modemlerin bağlı olduğu telefon hatları, Elektro Manyetik Pals etkisini, bağlı oldukları cihazlara, elektromanyetik olarak yalıtılmış ortamlarda bulunsalar dahi taşıyacaklardır.

2.6 SAYISAL BİLGİ SAVAŞININ / TERÖRÜNÜN AMAÇLARI

2.6.0 Devre Dışı Bırakma

Hedef alınan sistemin, yazılım ya da donanım olarak kullanım dışı bırakılmasıdır. Bu amaç, yazılıma ya da donanıma hasar veren bir sayısal bilgi savaşı silahı kullanılarak elde edilebilir. Örneğin bir virüs, işlemcinin çalışma frekansını artırarak (overclock) aşırı ısınmasına ve yanmasına neden olabilir.

2.6.1 Zayıflatma

Hedef alınan sistemin işlevini gereği gibi yapamaz hale getirilmesidir. Örneğin 1998 yılında internette yayılan bir kurt, internete bağlı 6000 bilgisayarın 12 saat süre ile kilitlenmesine neden olmuştu.

2.6.2 Aldatma

Hedef alınan sistemin, farkında olmadan yanlış bilgi üretmesi ve üretilen bu bilginin doğruymuş gibi işlem görmesi durumudur. Çalışmanın önceki bölümlerinde aktarılan semantik hücumlar vasıtası ile gerçekleştirilir. Başarılı bir semantik saldırı çok büyük zararlar verebilir.

2.6.3 İstismar Etme

Hedef alınan sistemden fark ettirilmeden bilgi sızdırılması durumudur.

2.7 SAYISAL BİLGİ SAVAŞININ / TERÖRÜNÜN EVRELERİ

Sayısal bilgi savaşına maruz kalan bir sistemdeki evreler, bulaşıcı hastalıkların insanlar üzerinde gösterdikleri evrelerle neredeyse aynıdır. Bu evreler şu şekilde sıralanabilir:

2.7.0 Bulaşma Evresi

Sayısal bilgi savaşı silahının, sisteme en zayıf noktasından sokulması evresidir. Sayısal bilgi savaşının belki de en zor kısmıdır. Dikkat edilmesi gereken iki konu, bulaşma yeri ve bulaşma şeklidir.

Sisteme bulaşma yeri bakımından incelendiğinde, zararlı yazılım, sisteme direk olarak ya da çevre birimleri vasıtasıyla girebilir.

Sisteme bulaşma şekli bakımından incelendiğinde, "Ön Kapı Tekniği" ve "Arka Kapı Tekniği" nin kullanıldığını görürüz. Ön Kapı tekniğinde, yazılım, sisteme üretim amacına uygun bir ürünle bulaştırılır. Örneğin, disket ya da CD-Rom ile.

Arka Kapı tekniğinde yazılım sisteme üretim amacının dışında bir şekille bulaşır. Sisteminizdeki açıklardan faydalanıp internet ortamından bulaşan virüsler gibi.

2.7.1 Yayılma Evresi

Sisteme giren yazılım, sistem içerisindeki belirli bir hedefe ulaşmak üzere yayılır. Bu hedef yazılım, donanım, sistem içinde belirli bir ana bilgisayar ya da network üzerindeki bilgisayarlardan biri olabilir.

2.7.2 Kuluçka Evresi

Sisteme giren yazılım, önceden ayarlanmış olduğu çalışma zamanı gelinceye kadar (saatli bomba virüsleri gibi) yada belirli bir ikaz alıncaya kadar sistemin içinde kuluçkaya yatar. Gizlenmek için genellikle bir truva atını kullandığından fark edilmesi neredeyse imkansızdır.

2.7.3 Faaliyet Evresi

Faaliyet evresi, yazılımın tetikleme mekanizması tarafından harekete geçirilmesiyle başlar. Bu tetikleme mekanizması zaman ayarı, mantık bombası, özel bir kullanıcı adı ve parola kombinasyonu yada belirli bir veri girişi şeklinde olabilir.

Sisteme bulaşan yazılım, verilen bir ikaz üzerine ya da zaman ayarlı olarak, bir önceki bölümde açıklanan "Devre Dışı Bırakma", "Zayıflatma", "İstismar Etme" gibi amaçların elde edilmesi için faaliyete geçer.

Bazen, bulaşan yazılım herhangi bir tetikleme mekanizmasına ihtiyaç duymadan, sisteme girer girmez faaliyete geçer. Örneğin telefon ağları için geliştirilmiş bir yazılım, sisteme girmesiyle birlikte kendi kendini kopyalayarak çoğalır ve sistemi aşırı yükleyerek çökmesine neden olur.

2.7.4 Son Evre

Amacını elde eden yazılım tekrar pasif duruma döner ya da hiç iz bırakmamak üzere kendisini sistemden siler. Böylece, saldırının kim tarafından ve ne şekilde yapıldığı konusunda bir iz bırakılmamış olur. Eğer istismar etme yöntemi ile sistemden bir takım kritik veriler elde edildi ise, durumun hiç farkına dahi varılamayabilir.

2.8 SAYISAL BİLGİ SAVAŞINDAN / TERÖRÜNDEN KORUNMA YOLLARI

Sayısal bilgi savaşından korunmanın kesin bir çözümü yoktur. Ancak riskleri azaltmak için alınması gereken önlemleri aşamalarla sıralayabiliriz.

2.8.0 Zararlı Yazılımın Sisteme Bulaşmasını Önleme

Son kullanıcının donanım alanında yapabileceği çok fazla şey yoktur. Kişinin yapabileceği en önemli şey sistemini tanımasıdır. Örneğin kişi işlemcisinin kaç Mhz. de çalıştığını bilirse sistemi olması gerekenden daha hızlı çalıştırmaya (overclock) kalkan bir virüsün varlığını daha çabuk tespit edebilir. Eğer bir kamu kuruluşunda yada bir şirketteki çok önemli dosyaları saklayan bir sistem söz konusu ise en kesin çözüm sistemin izole edilmesidir. Gerekirse bilgisayar ağdan çıkarılabilir. Dış dünya

ile hiçbir bağı olmayan bir bilgisayarın saldırıya uğraması olasılığı çok daha düşüktür.

Yazılım konusunda alınması gereken en önemli tedbir kullanıcı adlarının ve parolalarının kimseyle paylaşılmamasıdır. Ayrıca sistemde mutlaka bir güvenlik programı çalıştırılmalı ve bu program haftada en az bir kere güncellenmelidir. İşletim sistemindeki olası açıklara karşı ürün güncellemesi titizlikle yapılmalıdır. Emniyetli olmayan hatlardan sisteme giriş kesinlikle yasaklanmalıdır. Bir kamu kuruluşu çok önemli dosyaları emniyetli olmayan hatlardan gönderecekse dosyalar mutlaka şifrelenmeli hatta mümkünse kriptolanmalıdır. Yazılım konusunda bir kişi yetkili olmalı, o kişinin haricinde kimse sisteme müdahale etmemelidir.

Kamu kuruluşu yada özel şirket yöneticileri, sayısal bilgi savaşı konusunda personelinin bilgi sahibi olmasına özen göstermelidir. Yönetici, sistem emniyetinin ve personel bilgisinin bilirkişiler tarafından test edilmesini sağlamalı, konu ile ilgili gelişmeleri takip edecek birimler kurmalıdır.

2.8.1 Zararlı Yazılımın Tespit Edilmesi ve Sistemden Silinmesi

Zararlı yazılım tespit edilmiş ise bunu belirli tarayıcı / temizleyici yazılımlar kullanarak temizlemek en çabuk çözümdür. Ancak truva atlarını bulmak çok zordur. Bulunmuş olan bir truva atının da kendisini sistem içinde başka bir yere kopyalamış ve kuluçkaya yatmış olması ihtimali çok büyüktür. Sistemi garantiye almak için en kesin yol sistemin formatlanması ve yeniden kurulmasıdır. Hatta bir çok güvenlik programı üreticisi, sistem taramasında bir virüs bulunmasa dahi truva atlarına karşı tedbir olarak sistemin belirli aralıklarla formatlanmasını önermektedir.

Yöneticiler bu aşamada personelin zararlı yazılım taranması ve sistemden kaldırılması konusunda bilgilendirilmesini sağlamalıdır.

2.8.2 Zaralı Yazılımın Yayılmasını Önleme

Zararlı yazılımın tespit edildiği sistem bir ağ üzerinde ise diğer sistemlerle olan iletişimi mutlaka kesilmeli ve ağ üzerinde de zararlı yazılım taraması yapılmalıdır. Virüsün bulaştığı tüm bilgisayarlar derhal izole edilmelidir. Bu sistemlerde kullanılmış olan disket vb. medyalar kontrol edilmeli, gerekiyorsa imha

edilmelidir. Virüsler kendilerini diğer programlara kopyalayabildikleri için vakit kaybetmeden sistem temizliği yapılmalıdır.

2.8.3 Sistemin Eski Haline Döndürülmesi

Bütün zararlı yazılımlar temizlendikten sonra sistem eski haline döndürülebilir. Bunu yapabilmek için düzenli olarak dosya yedeklemesi yapılmış olması gerekir. Düzenli olarak yedekleri alınan sistemlerde oluşan arızalar sonrası işler kaldığı yerden devam edebilir. Sistem yedeği alınması konusunda yöneticiye büyük görevler düşer. Yönetici yedeklemenin düzenli olarak yapılmasını sağlamalı ve bunu kontrol etmelidir. Yedekleme işlemi yapılmamış sistemlere bilginin yeniden aktarılması aylar sürebilir.

2.9 BİLGİ SAVAŞI / TERÖRÜ ve KİTLE İLETİŞİM ARAÇLARI

Kitle iletişim araçlarınca doğruların kamuoyuna aktarılması günümüz haberciliğinin en temel ilkesidir. İster devletin ister özel teşebbüsün elinde bulunsun, kitle iletişim araçları ile verilen haberler doğru, eksiksiz, tarafsız ve hızlı olmalıdır. "Ancak şiddetin amacının eylemin gerçekleştirilmesi veya sessizce gerçekleştirilmesi değil, mümkün olan en büyük yankıyı yapması olduğunun hesaba katılarak şiddetin yerleştirmek istediği korkudan kurtulma yolunun şiddet olayını tanımadan geçtiği gözden uzak tutulmamalıdır."[45]

Bu noktadan itibaren büyük sorumlulukları olan kitle iletişim araçlarının şiddet olaylarını abartısız ve tarafsız olarak kitlelere ulaştırma görevini yerine getirme mecburiyetleri vardır. Ancak içeriğinde şiddet içeren mesajların kamuya yansıtılırken bu mesajların ulaşacağı geniş kesimde yaratacağı korku ve infial durumu da göz önünde tutulmalıdır. Zakir Avşar kitabında şiddet içeren mesajları şöyle guruplar:

A) Gerçek Hayatla İlgili Mesajlardaki Şiddet

Bunların en olağanı haberlerde yer alan şiddet içerikli mesajlardır. Kitle iletişim araçlarının varlık sebebi "haber verme" olduğundan, doğal olarak şiddet içerikli haberler de bu araçlarda sık sık yer almaktadır. Daha doğrusu, şiddet içerikli

[45] Avşar, a.g.e. s.56

haberler oluştukça bunlar kitle iletişim araçlarında verilmektedir. Savaş haberleri, kriminal hadiseler, giderek dozu artan terör olayları kitle iletişim araçlarının "haber olduğu için" sunma durumunda bulundukları şiddet içerikli mesajlardır.

B) Gerçek Hayatla İlgisi Olmayan Mesajlardaki Şiddet

Kitle iletişim araçlarında gerçek hayatla ilgili mesajlar yanında, gerçek hayattan alınmayan hayal ürünü, fantazi olan mesajlar da verilmektedir. Bu tür mesajlarda şiddet içerikli olanlara çoklukla ve sıklıkla rastlanabilir. Cinayet dizileri, işkence, yıldızlararası savaşlarla ilgili gerçek olmayan ama tiyatral olarak, gerçek hayattaymış gibi sunulduğu için çok fazla etkili olan mesajlardır.

Toplumlarda bezginlik, umutsuzluk, endişe ve şaşkınlık etkisi uyandırma şüphesiz ki, terörün en önemli işlevlerinden bilişidir. Bu etki ne kadar geniş kitlelere ulaştırılabilirse amaca da o kadar yaklaşılmış iyi ulaşılmış olunacaktır. İletişim teknolojisindeki hızlı gelişmeler bu amaca ulaşmayı kolaylaştırıcı yöndedir. Amacı yalnızca mala ve cana zarar vermek olmayan terör hadisesini gerçekleştirenler, şiddetlerinin duyulması / duyurulması ve bu yolla psikolojik bir korkutma, ürkütme havası yaratmak isterler. Bunun için de kitle iletişim araçlarını kullanmaları gerekir. Kitle iletişim araçları yapıları gereği, doğal olarak bu havanın doğmasına sebep olurlar. Örneğin, 1968-1978 yılları arasında meydana gelen 3100 dolayında terörle ilgili uçak, diplomat, siyasi, işadamı kaçırma, rehin alma, siyasal cinayet, bombalama gibi olay meydana gelmiş ve bu olaylar haber niteliği taşıdığından hemen hemen tüm kitle iletişim araçlarında haber olarak yer almıştır.

2.9.0 Terör Haberlerinin Kitle İletişim Araçlarında Sunumunun Olumsuz Yönleri

Terör haberleri kitle iletişim araçlarında yer aldıkça halkta bir bezginlik, yılgınlık, korku ve şaşırmışlık duygusu yer alacaktır. Bununla birlikte kitle iletişim araçlarında terör olaylarının tüm detayıyla verilmesi, birey ya da gruplarca yapılan şiddet olayları ile ilgili tekniklerin çok geniş kitlelerce öğrenilmesine yol açmaktadır. Bir anlamda terörün nasıl yapıldığı konusundaki bilgiler, bu araçlarla bu teknikleri bilmeyenlere ulaşmakta; bu haberlerin arkasından daha çok bombalama, daha çok uçak kaçırma, vb. olaylara neden olunabilmektedir. Örneğin; geçtiğimiz yıllarda Beyaz Saray'a Molotof kokteyl'i ile saldıran bir eylemci, sorgusunda bomba

yapımını internetten öğrendiğini itiraf etmiştir. Yine, kitle iletişim organlarında yer alan terör ve şiddet olayları ile ilgili haberler birbirleriyle rekabet halinde bulunan örgütlerde geride kalmama; karşıt görüşlü örgütlerde ise misilleme yapma duygularını uyandırmaktadır.

2.9.1 Terör Haberlerinin Kitle İletişim Araçlarında Sunumunun Olumlu Yönleri

"İlk olarak, kitle iletişim araçlarının işlevlerinden birinin kamuoyu oluşturmak olduğu bilindiğinden, terör haberleri de diğer haberler gibi serbestçe sunularak, hem halkın özgürce haber almasına imkan verilmekte, hem de kamuoyunun serbestçe oluşumu sağlanmaktadır."[46]

Kitle iletişim araçlarının, terör olaylarında yetkililer ile geniş halk kitleleri arasında hayati bir bağ kurduğu kesindir. Zira bazı terör olaylarında basının, radyo ve televizyonun olayları çözümleyici bir konumu bulmaktadır. Yine kitle iletişim araçlarında verilen terör haberleri bu konuda halk arasındaki söylentileri, huzursuzluk doğurabilecek asılsız haberleri ve bunların olumsuz etkilerini ortadan kaldırır. Böylece halkın yönetime ve güvenlik güçlerine güvenleri artar ve bu güvenin zedelenmesi engellenir.

2.10 BİLGİ SAVAŞI SENARYOSU[47]

Tarih 17 Şubat 2001,

KAHVERENGİ Ülke, komşusu MAVİ 'nin uluslararası platformda gittikçe yalnızlığa itildiğini değerlendirmekte ve kendisinin bağlı bulunduğu siyasi ve ekonomik paktların desteğini alarak MAVİ ülkeye karşı tarihi bir fırsat ele geçireceğini düşünmektedir.

KAHVERENGİ Ülke başbakanı, ülkesinin beyaz denizdeki hak ve menfaatlerinin korunması maksadıyla meclisinin hükümete verdiği yetkiye dayanarak karasularını genişletme kararını 22 Şubat 2001 tarihinden itibaren yürürlüğe sokacağını açıklamıştır.

---

[46] Avşar, a.g.e. s.63
[47] Harp Akademileri Komutanlığı, a.g.e., s. 35-36

MAVİ Ülke başbakanı ise bu kararın ülkesinin beyaz denizdeki egemenlik haklarının ihlali anlamına geleceğini ve bunun engellenmesi için her şeyi göze alacağını ifade etmiştir. İki ülke arasında başlayan gerginlik sıcak bir çatışma ihtimaline doğru hızla ilerlemektedir.

20 Şubat tarihinde MAVİ medyası vasıtası ile yapılan bir açıklamada KAHVERENGİ ülke hükümetinin çıkabilecek bir savaş ihtimaline karşı bankalardaki hesaplara el koyduğu duyurulur. Panik içerisinde bankalara hücum eden KAHVERENGİ ülke vatandaşları hükümetin yalanlamasına rağmen banka hesaplarının gerçekten sıfırlanmış olduğunu görürler.

KAHVERENGİ Ülke başkent havaalanı bilgisayar sisteminde meydana gelen bir arıza nedeniyle iniş yapmakta olan iki uçak alan üzerinde çarpışır. Havaalanı trafiğe kapatılır.

KAHVERENGİ Ülke borsası bilgisayar sistemlerini kilitleyen bir virüs nedeniyle günlük seansını icra edemez.

İlerleyen saatlerde sinyalizasyon sistemindeki bir arıza nedeniyle iki tren çarpışır. Ülkede baş gösteren anormal olaylara karşı önlem almak maksadıyla yapılmak istenen bakanlar kurulu toplantısı dijital telefon santrallerinin kilitlenmesi sebebiyle kurul üyelerine haber ulaştırılamadığından yapılamaz.

Gece elektrik santrallerinde arka arkaya meydana gelen arızalar neticesinde büyük şehirler karanlığa gömülür.

Tüm KAHVERENGİ Ülkede büyük bir kaos başlar.

SONUÇ

İçinde bulunduğumuz bilgi çağının bir sonucu olarak ortaya çıkan bilişim teknolojileri, artık hayatımızın her alanında aktif olarak yer almaktadır.

Bilişim teknolojilerinin hızla gelişmesi, bizi gün geçtikçe onlara karşı daha bağımlı hale getirmektedir. Bu bağımlılık, hayatımızı çok kolaylaştırmıştır; ancak farkında olmamız gereken bir şey vardır ki hayatımızı kolaylaştırmak için kullandığımız bu sistemler kötü niyetli kişilerin elinde büyük birer silaha dönüşüverirler.

Çalışmanın önceki bölümlerinde de aktarıldığı gibi bu sistemler vasıtası ile kişisel bilgilerimiz açığa çıkarılabilir, ülkeler savaş haline gelebilir, dünya ekonomisi dibe vurdurulabilir ve teröristler insanların hayatlarını alt üst edebilir.

Bilgi savaşları ve siber terörizm bugün insanlığın önünde duran en büyük tehlikelerden biridir. Günümüzde çoğu gelişmiş ülke geleceğe dair savaş planlarını bilişim sistemleri üzerine dayandırmaktadır. Aynı durum terör örgütleri için de geçerlidir. Konu öylesine ciddi ki, askeri literatüre Bilişim Harekatı (Information Operations) olarak girdi bile. NATO belgelerinde bu tamlamaya sıkça rastlamak mümkün hale geldi. Hızlı ve etkin çözümlerin üretilememesi bir felakete neden olabilir. Bir bilişim harekatı yalnızca düşman bir ülkeden gelmek zorunda değil; terörist gruplar da güçleri ölçüsünde bir bilişim harekatına teşebbüs edebilirler.

Hayatımızın vazgeçilmez parçaları olan bu sistemlerden göreceğimiz zararı en aza indirmek için siber terörizmin ne olduğunu ve bizi nasıl etkileyebileceğini çok iyi anlamamız gerekir. Konu artık bir bilim kurgu olmaktan çıkıp, hayatın bir gerçeği haline gelmiştir. Evimizden çıkarken nasıl kapıyı açık bırakmıyorsak, bilişim teknolojileri konusunda da ön tedbirleri almamız gerekmektedir. Evimizde, işyerimizde kullandığımız bilgisayarları, her alanda olmasa da küçük ve orta boydaki saldırılara karşı kendini savunacak hale getirmemiz mümkündür.

Kişisel korunmanın yanı sıra, şu günlerde E-Devlet uygulamasına geçiş sürecini yaşayan ülkemizde de hükümetlerin almaları gereken tedbirler vardır. Bu tedbirler askeri alana, eğitim alanına, sosyal alana, kamu kurum ve kuruluşlarına

yayılmalıdır. Türk Silahlı Kuvvetlerinin bilgi harbi konusunda ön çalışmaları olduğu bilinmektedir ancak geriye kalan alanlarda gözle görülür bir çalışma yoktur. Konunun bu hayati önemine rağmen Türkiye'de bu konuya yönelik çalışmalar son derece kısıtlı kalmıştır. Pek çok ülkenin aksine, ülkemizde ulusal ölçekte bir Bilgisayar Acil Durum Müdahale Ekibi (Computer Emergency Response Team - CERT) bulunmamaktadır. Böylesi bir ekip, bilişim güvenliği konularında ulusal bir iletişim noktası oluşturulması, acil durumlara hızlı ve etkin müdahalenin sağlanması ve kurumlar arası koordinasyonun sağlanması anlamlarında oldukça faydalı olacaktır.

Kamu alanında, siber terörle ilgili eğitim bir zorunluluktur. Kamu kuruluşlarımızın neredeyse hiç birisinin bir bilişim güvenliği programı yoktur; güvenlik politikaları, beklenmedik durum planları, eğitim ve teknolojik katkı gibi alanlarda hemen hiçbir hazırlık mevcut değildir. Kuruluşlarımızın büyük bir çoğunluğu, İnternet bağlantısının önüne yerleştireceği bir güvenlik duvarının bilişim güvenliği ile ilgili konularda tek başına yetkin bir çözüm oluşturacağını öngörmektedir. Günümüzde içinde önemli kamu bilgileri taşıyan bilgisayarların öğlen tatillerinde internette sohbet etmek amacı ile kullanıldıkları bir gerçektir. Oluşabilecek zararlar bir yana henüz sistemleri kullanmayı bile yeterince bilmeyen kişilerin bu tip amaçlarla bilgisayar başına geçmeleri son derece tehlikeli sonuçlar doğurabilir. Kamuda hizmet içi eğitimlerle konunun hassaslığı mutlaka belirtilmeli, çalışanlara korunma yolları anlatılmalı ve korunma kamu yöneticileri tarafından mutlaka denetlenmelidir.

Özel sektör, personel seçimlerinde bilgisayar kullanımına daha fazla özen gösterdiğinden ve güvenliği kamuya göre biraz daha ciddiye aldığından daha şanslı sayılabilir. Ancak unutulmamalıdır ki en ufak bir hatadan dolayı ağa bulaşan bir sayısal bilgi savaşı silahı bütün verilerin yok olmasına neden olabilir.

Konunun önemi acil çözümlerin oluşturulmasını gerektirmektedir. Çözümler oluşturulurken göz ardı edilmemesi gereken belki de en önemli nokta bilişim güvenliğinin 'Sonuç değil Süreç' olduğudur. Bilişim güvenliği ulaşılabilecek bir hedef değildir, bir süreçtir. Güvenliği sağlamak ve korumak düzenli ve planlı bir çalışmayı gerektirir.

Artık aracımızı rot balans ayarı yaptırmak için götürdüğümüz küçük bir tamirhanede bile bilişim sistemleri kullanılmaktadır. Günümüzde bilişim sistemlerini kullanmayan sektör sayısı yok denecek kadar azdır. Bu yüzden geleceğin çalışanları olacak üniversite ve yüksek okul öğrencilerine verilen bilgisayar derslerine ek olarak bilgi savaşı ve siber terörizmle ilgili dersler branş ayrımı gözetmeksizin verilmelidir.

Unutmamamız gereken bir şey vardır. Bilişim sistemleri artık hayatımızın olmazsa olmaz bir parçasıdır. Ancak hayatımızın bu parçası kötü niyetli kişilerin hizmetine de açıktır.

Siz evinizdeki ekmek bıçağını sadece ekmek kesmek için kullanıyorsunuz diye herkesin onunla ekmek kesmesini beklemek yanlıştır.

YARARLANILAN YAYINLAR

1. Alkan,Necati , **Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler,** http://www.caginpolisi.com.tr/20/41-43.htm

2. Atıcı,Bünyamin ve Gümüş,Çetin , **Sanal Ortamda Gerçek Tehditler; Siber Terör – 1,** turk.internet.com, URL:http://turk.internet.com/haber/yazigoster.php3?yaziid=8838

3. Avşar, Bozkurt Zakir, **Kitle İletişim Araçları ve Terör,** İstanbul: Kamer Yayınları, s. 15

4. Cip, Sümer, **Hacking Yöntemlerine Genel Bir Bakış,** Olympos Security Güvenlik Portalı URL:http://www.olympos.org/article/articleprint/1440/-1/10

5. Dayıoğlu, Burak, **Bilişim Savaşlarına Hazırmısınız?,** Olympos Security Güvenlik Portalı URL:http://www.olympos.org/article/articleprint/161/-1/10/bilisim_savaslarina_hazirmisiniz

6. Downs Jr,Lawrence G. , **Digital Data Warfare: Using Malicious Computer Code As A Weapon,** Air University, 1995

7. **Dünyada Savaşın Tarihçesi,** http://www.dunyaonline.com/48535.asp

8. Haeni,Reto E., **Information Warfare,** http://www.islab.oregonstate.edu/documents/Papers/iware.pdf

9. Harp Akademileri Komutanlığı, **Türk Silahlı Kuvvetleri Bilgi Harbine Nasıl Hazırlanmalıdır?**, İstanbul: Harp Akademileri Komutanlığı Yayınları, 1999

10. Kongar,Emre , **Küresel Terör ve Türkiye,** 1. b., İstanbul: Remzi Kitabevi, 2001

11. Libicki,Martin , **What Is Informatıon Warfare?,** National Defense University, 1995, http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html

12. Özcan,Mehmet , **Siber Terör,** turk.internet.com, URL:http://turk.internet.com/haber/yazigoster.php3?yaziid=4038

13. Savaş ve Savaş Araçları, **Temel Britannica,** Cilt 15, İstanbul: Ana Yayıncılık, 1993

14. Seçen, Turgay , **Türk Hacker'lar - 1,** turk.internet.com, URL:http://turk.internet.com/haber/yazigoster.php3?yaziid=8249

15. **Siber terör: Gerçek tehdit,** http://www.ntvmsnbc.com

16. **Terör Nedir?,** http://www.iem.gov.tr/teror/index.asp#not1

17. **Terör Nedir?,** http://www.teror.gen.tr/turkce/teror_nedir/nedir.html

18. Terörizm, **Temel Britannica,** Cilt 17, İstanbul: Ana Yayıncılık, 1993

19. **Terörün Tanımı,** http://www.teror.gen.tr/turkce/teror_nedir/tanimi.html

20. Toffler,Alvin ve Heidi , **21. Yüzyılın Şafağında Savaş ve Savaş Karşıtı Mücadele,** Sabah Kitapları

21. Topçuoğlu,Ayşenur , **Siber Terörizm,** Bilim – Teknik Dergisi, 2001

22. www.sanalteror.gen.tr

ÖZGEÇMİŞ

Yazar 18/10/1976 yılında İzmit – Kocaeli'nde doğmuştur.

İlk öğrenimini İzmit Ulugazi İlk Öğretim Okulu'nda yaptıktan sonra orta okul ve lise eğitimini Özel Kocaeli Koleji'nde tamamlamıştır. 1994 yılında liseden mezun olan yazar aynı yıl Eskişehir Anadolu Üniversitesi Eğitim Fakültesine girmiş ve İngilizce öğretmenliği eğitimi almıştır.

1998 yılında üniversiteden mezun olduktan sonra öğretmenlik hayatına başlayan yazar, Kocaeli ilinde özel bir eğitim kurumunda sırasıyla öğretmenlik, bölüm başkanlığı ve idarecilik görevlerinde bulunmuştur. Bu dönem içinde bazı özel eğitim kurumlarına da bilgisayar ve İngilizce eğitimi konusunda danışmanlık yapmıştır.

1999 yılında Kocaeli Üniversitesi Rektörlüğü'nün açtığı Okutmanlık kadrosu sınavlarına başvuran yazar bu sınavlarda başarılı olmuş ve aynı yıl içinde Kocaeli Üniversitesi Yabancı Diller Bölümünde Okutman olarak çalışmaya başlamıştır. 17 Ağustos 1999 depreminden sonra kurulan Hereke kampusunda bölüm koordinatörü olarak görevlendirilen yazar bu görevini 2003 yılına kadar sürdürmüştür. 2005 Yılında Uzunada Deniz Komutanlığı'nda (İzmir) askerlik hizmetini yerine getiren yazar aynı yılın sonunda Kocaeli Üniversitesi'ndeki görevinden ayrılmıştır.

Şu an halen kurucu ortağı olduğu bir inşaat firmasında yönetici olarak görev yapmakta olan yazar evli ve bir kız çocuğu babasıdır.