SİBER SALDIRILAR - SİBER SAVAŞLAR

VE

ETKİLERİ

Mahruze KARA

111692025

İSTANBUL BİLGİ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

Yrd. Doç. Dr. Leyla KESER BERBER

2013

SİBER SALDIRILAR SİBER SAVAŞLAR VE ETKİLERİ

CYBER ATTACKS CYBER WARS AND EFFECTS

Mahruze KARA
111692025

Yrd. Doç. Dr. Leyla KESER BERBER :

Yrd. Doç. Dr. Nilgün BAŞALP :

Yrd. Doç. Dr. Bülent ÖZEL :

Tezin Onaylandığı Tarih :

Toplam Sayfa Sayısı : 74 sayfa

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) Siber Savaş	1) Cyber War
2) Siber Saldırı	2) Cyber Attacks
3) Bilgisayar Korsanı	3) Hacker
4) Kritik Alt Yapılar	4) Critical Infrastructures
5) İnternet	5) Internet

ÖZET

İnternetin ortaya çıkması ile yararlarından faydalanılmaktadır. Ancak internetin zararları da mevcuttur. İnternet, dünya dengelerini değiştirmektedir. İnternet, siber saldırılara ve siber savaşlara aracılık eden bir alan olmuştur. Siber saldırılar, ülkelerin ulusal ve ekonomik güvenliğini sarsmaktadır. Siber savaşlar 5. boyutta yapılmaktadır. Bu çalışmada siber silahlar ile siber saldırılar ve siber savaşların etkileri işlenmiştir. Siber güvenlik önlemleri için çözümler önerilmiştir.

ABSTRACT

With the emergence of the Internet is utilized benefits. However, the Internet is also available in losses. Internet, shifting the balance of the world. Internet, cyber attacks and cyber warfare have been receiving an intermediary. Cyber attacks, undermines countries' national security and economic security. 5 cyber wars size maintained. In this study, the effects of cyber weapons and cyber attacks and cyber warfare processed. Recommended solutions for cyber security measures.

İÇİNDEKİLER

KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
APT	Advanced Persistent Threat
ARPANET	Advanced Research Projects Agency Network
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi
bkz.	bakınız
BM	Birleşmiş Milletler
BOME	Bilgisayar Olaylarına Müdahale Ekibi
CERT	Computer Emergency Readiness Team
CERT/CC	Computer Emergency Readiness Team Coordination Center
ENISA	European Network and Information Security Agency
HRW	Human Rights Watch
IAEA	*International Atomic Energy Agency*
IDF	*Israel Defense Forces*
INCB	Israel National Cyber Bureau
NIST	National Institute of Standarts and Technology
NIS	Network and Information Security
PLC	Programmable Logic Controller
SCADA	Supervisory Control And Data Acquisition
SEA	Syrian Electronic Army
SGE	Siber Güvenlik Enstitüsü
TCP/IP	Transmission Control Protocol/Internet Protocol
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

KAYNAKÇA

(2012, Ağustos 15). Mayıs 9, 2013 tarihinde PASTEBIN: http://pastebin.com/HqAgaQRj adresinden alındı

ACAR, Ü., & URHAL, Ö. (2007). *Devlet Güvenliği İstihbarat ve Terörizm*. Ankara.

ALKAN, N. (tarih yok). *Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler*. Nisan 07, 2013 tarihinde http://www.caginpolisi.com.tr: http://www.caginpolisi.com.tr/20/41-43.htm#_ftn5. adresinden alındı

ALPEROVİTCH, D. (2011). *Revealed: Operation Shady RAT*. McAfee.

ASPAN, M., & SOH, K. (2011, Haziran 16). *Citi says 360,000 accounts hacked in May cyber attack*. Nisan 30, 2013 tarihinde Reuters: http://www.reuters.com/article/2011/06/16/us-citigroup-hacking-idUSTRE75F17620110616 adresinden alındı

AYBASTI, M. K. (Yöneten). (2013). *RED!* [Sinema Filmi].

Ayyıldız Tim. (2012, Ocak 27). *Basındaki Video ve Haberlerimiz*. Mayıs 1, 2013 tarihinde Ayyıldız Tim Web Sitesi: http://www.ayyildiz.org/portal/index_videolb/player.swf?url=video/ayyildiztim1d.flv&volume=100 adresinden alındı

BBC. (2011, MAYIS 24). *Suriye'deki tesis muhtemelen nükleer reaktördü*. NİSAN 27, 2013 tarihinde BBC TÜRKÇE: http://www.bbc.co.uk/turkce/haberler/2011/05/110524_syria_nuclear.shtml adresinden alındı

BERMAN, I. (2013, MART 20). *The Iranian Cyber Threat, Revisited.* MAYIS 31, 2013 tarihinde http://docs.house.gov/: http://docs.house.gov/meetings/HM/HM08/20130320/100523/HHRG-113-HM08-Wstate-BermanI-20130320.pdf adresinden alındı

BIÇAKCI, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler* , 210-211.

Bilimania. (tarih yok). *Siber Saldırılar, İran, Elektrik Şebekeleri*. Mart 27, 2013 tarihinde Bilimania: http://www.bilimania.com/bilisim-teknolojileri/35-bilisim-teknolojileri/3117-siber-saldirilar-iran-elektrik-sebekeleri adresinden alındı

Budapest University of Technology and Economics Department of Telecommunications, Laboratory of Cryptography and System Security. (2012). *sKyWIper (a.k.a. Flame a.k.a. Flamer):A complex malware for targeted attacks.* Budapeşte: http://www.crysys.hu/, http://www.bme.hu/ .

CLARKE, R. A., & KNAKE, R. K. (2011). *Siber Savaş.* İstanbul: İstanbul Kültür Üniversitesi.

COMMISSION OF THE EUROPEAN COMMUNITIES . (2004). *Critical Infrastructure Protection in the fight against terrorism* . Brüksel.

CSIS Security Group A/S and Trend Micro Incorporated . (2012). *W32.Tinba (Tinybanker) The Turkish Incident.*

Cyber Warrior. (tarih yok). *Cyber Warrior TİM olarak neler yaptık?* Mayıs 1, 2013 tarihinde Cyber Warrior hacktivist grup web sitesi: http://www.cyber-warrior.org/Hacked/index.htm adresinden alındı

DÜĞEN, T. (2012, MART 28). *Dar Alanda Büyük Pazarlık: Kırgızistan'da ABD ile Rusya'nın Üs Mücadelesi*. NİSAN 30, 2013 tarihinde 21. Yüzyıl Türkiye Enstitüsü: http://www.21yyte.org/arastirma/kirgizistan/2012/03/28/6545/dar-alanda-buyuk-pazarlik-kirgizistanda-abd-ile-rusyanin-us-mucadelesi adresinden alındı

Dünyaca Ünlü "5 Siyah Şapkalı Hacker". (2012, Haziran 06). Nisan 07, 2013 tarihinde http://www.imajweb.com: http://www.imajweb.com/dunyaca-unlu-5siyah-sapkali-hacker.html adresinden alındı

EMRE, B. (2013, Ocak 2). *5.Boyutta Savaş:Siber Savaşlar-II*. Mayıs 26, 2013 tarihinde TÜBİTAK-BİLGEM: http://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html adresinden alındı

European Commission . (2010, Ağustos 17). *Critical infrastructure protection*. Mayıs 11, 2013 tarihinde Europa Summaries of EU legislation: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm adresinden alındı

GÖK, M. S. (2012). *5651 Sayılı Kanun ve Bilgi Güvenliği İlişkisi.* İstanbul: On İki Levha Yayıncılık A.Ş.

HALICI, N. (2002, Mart 22). *Enformasyon Savaşı İçin Ağır Silahlanma*. Nisan 13, 2013 tarihinde bianet: http://bianet.org/bianet/bianet/8406-enformasyon-savasi-icin-agir-silahlanma adresinden alındı

HALTAŞ, F. (2011, Kasım 14). *DUQU:Yeni Nesil Keşif Uçağı*. Mayıs 10, 2013 tarihinde TÜBİTAK-BİLGEM: http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/duqu-yeni-nesil-kesif-ucagi.html adresinden alındı

İstanbul Bilgi Üniversitesi. (2012). *Siber Güvenlik Raporu.* İstanbul.

KARAKUŞ, C. (tarih yok). *Kritik Alt Yapılara Siber Saldırı*. Mart 24, 2013 tarihinde http://ylt44.com/: Kritik Alt Yapılara Siber Saldırı, http://ylt44.com/bilimsel/siber.html Cahit KARAKUŞ, İstanbul Kültür Üniversitesi, Erişim, 24/03/2013 adresinden alındı

Kaspersky. (tarih yok). *Bilgisayar Korsanlığı.* Nisan 07, 2013 tarihinde www.kaspersky.com.tr: http://www.kaspersky.com.tr/hacking adresinden alındı

LEWIS, J. A., & TIMLIN, K. (2011). *Cybersecurity and Cyberwarfare.* Washington: The Center for Strategic and International Studies (CSIS) .

MANDIANT. (2013). *APT1 Exposing One of Chine's Cyber Espionage Units.*

MİTNİCK, K. D., & SIMON, W. L. (2013). *Sızma Sanatı.* Ankara: ODTÜ Yayıncılık.

National Cyber Security Strategies in the World. (2013, NİSAN). MAYIS 7, 2013 tarihinde ENİSA: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world adresinden alındı

NCI Agency. (tarih yok). Mayıs 25, 2013 tarihinde NCIA: http://www.ncia.nato.int/About/Pages/default.aspx, adresinden alındı

ÖZDEMİR, D. H. (2009). *Elektronik Haberleşme Alanında Kişisel Vrelierin Özel Hukuk Hükümlerine Göre Korunması.* Ankara.

Profile:Gary McKinnon. (2012, Aralık 14). Nisan 07, 2013 tarihinde http://www.bbc.co.uk/: http://www.bbc.co.uk/news/uk-19946902 adresinden alındı

RedHack. (2013, Şubat 17). Ezber Bozanlar. (E. ERDEM, Röportajı Yapan)

SANGER, D. E. (2012, HAZİRAN 1). *Obama Order Sped Up Wave of Cyberattacks Against Iran*. HAZİRAN 1, 2013 tarihinde nytimes: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=2& adresinden alındı

STEWART, P., & COONEY, P. (2012, Ekim 11). *Reuters*. Mayıs 8, 2013 tarihinde The "Shamoon" virus that attacked Saudi Arabia's state oil company, ARAMCO, was probably the most destructive attack the business sector has seen to date, U.S. Defense Secretary Leon Panetta said on Thursday.: http://www.reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012 adresinden alındı

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.*

The Comprehensive National Cybersecurity Initiative. (tarih yok). Mayıs 21, 2013 tarihinde National Security Council: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative adresinden alındı

The United States Department of Defense. (2013). *Military and Security Developments Involving the People's Republic of China.* Washington.

TÜBİTAK-BİLGEM. (2011). *Ulusal Siber Güvenlik Tatbikatı 2011 Sonuç Raporu.*

UÇKAN, Ö. (tarih yok). *SOKAK + (DİJİTAL) İLETİŞİM = AKTİVİZM.* Mart 29, 2013 tarihinde http://www.politus.org.tr: http://www.politus.org.tr/Detay2.aspx?id=105 adresinden alındı

Uluslararası Stratefik Araştırmalar Kurumu. (2011). *Kritik Enerji Alt Yapı Güvenliği Projesi Sonuç Raporu.*

Velayet 91 uzmanlık saha tatbikatında siber saldırı başarı ile denendi. (2012, ARALIK 30). HAZİRAN 1, 2013 tarihinde İslâmi Davet: http://www.islamidavet.com/2012/12/30/velayet-91-uzmanlik-saha-tatbikatinda-siber-saldiri-basari-ile-denendi/ adresinden alındı.

§ 1. GİRİŞ

20. yüzyılda bilgisayarın ve internetin ortaya çıkışı ile ülkelerin savaş, saldırı ve savunma teknikleri değişiklik göstermiştir. İnternetin gelişimi tarihi seyrinde öncelikle askeriyede kullanılmıştır. Askeriyeden sonra ticarette kullanılmış ve kişisel kullanıma kadar yaygınlaşmıştır. Şimdi her evde bir veya birkaç bilgisayar bulunmaktadır.

Kamu ve özel kuruluşları, tüm faaliyetlerini kolaylaştırmak, hızlandırmak ve etkinleştirmek için mümkün olduğunca hızlı bir şekilde bilişim teknolojilerini özümseyip uyarlayarak yaygınlaştırılmalarını sağlamaktadır. Hayatımızın her alanında bilişim sistemlerine dair kolaylıklardan faydalanılmaktadır.

İnternetin kişisel kullanımda faydalanılmasına başlanmasıyla, kendi içinde yeni bir lisan oluşturmuştur. Hacker olarak bilinen bilgisayar korsanları, bilgisayar programlarına vakıf, yetenekli kişiler olarak internetin gizemli dünyasını aralamış ve internet aracılıyla neler yapılabileceğini göstermişlerdir. Bilgisayar korsanlarının, hacking işlemlerinde hedef kimi zaman tekil bir internet kullanıcısı, kimi zaman ise şirketler veya ülkelerin önemli kurum ve kuruluşları olmuştur. 1990'lı yıllarda ilk hacking işlemleri kişisel menfaatler için yapılırken şimdi ise ülkeleri tehdit eden bir siber silah haline gelmiştir.

Değişen dünya değerleri arasında ilk sırayı alan bilgiyi, koruma ve muhafaza etme biçimi de değişiklik göstermiştir. Elektronik ortama entegre olan bilgiyi korumak için de elektronik ortam muhafazası gerekmektedir. Gizlilik arz eden şirket sırlarının sanayi casusları aracılığıyla rakip şirketlerce ele geçirilmesi maddi zarara sebep olmaktadır.

Gizli sistemlere, sistem açıklarından faydalanarak sızan ve önemli sırları ele geçiren hackerlar artık birer siber savaşçı olarak devlet adına çalışmaktadır. Siber saldırılarla devlet sırları ve devlet savunma sisteminin diğer ülkelerce ele geçirilmesi ise devlet savunma sisteminin birer parçası haline gelmiştir.

Bu çalışma internetin gelişim süreci içinde hayatımıza kattığı değerleri ve sorunları ortaya koymaktadır. Sivil hacker gruplarının faaliyetleri sonucunda toplum hayatına etkileri ve zararları incelenecektir. İnternetin nasıl bir silaha dönüştürülerek, siber savaş tehdidi olduğu sorgulanacaktır. Günümüze kadar yaşanan siber savaşlarda, ne tür siber silah uygulamalarının kullanıldığı ve savaşlara olan etkisine dikkat çekilecektir. Çalışmada dünya ülkelerinde ve ülkemizde siber tehdide karşı geliştirilen siber güvenlik stratejileri incelenecektir. Siber savaşlarda kritik altyapıların önemi vurgulanarak, korunması için çözüm önerileri sunulacaktır.

§ 2. SİBER ORTAM KAVRAMLARI

Avrupa Birliği (AB) tarafından kurulan, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA-European Network and Information Security Agency)'nın Mayıs 2012'de yayınladığı Ulusal Siber Güvenlik Stratejileri raporuyla tavsiyelerde bulunmuştur. Siber güvenliğin sağlanmasının, hem ulusal hem de uluslar arası düzeyde devletin, iş dünyasının ve toplumun ortak sorunu haline geldiğini belirten raporda AB'ye, AB'ye üye olan ve üye olmayan ülkelere ulusal siber güvenlik stratejilerini belirlemelerini tavsiye etmiştir.

AB, 07/02/2013 tarihinde AB'nin siber güvenlik stratejisini belirlemiş ve aynı tarihte Avrupa Komisyonu, birlik genelinde ortak bir ağ ve bilgi güvenliğinin (NIS-Network and Information Security) sağlanmasına ilişkin tedbirlere dair direktif teklifi yayınlamıştır.

Bilgisayar, internet ve cep telefonlarının kullanımı, bilişim sistemlerindeki hızlı gelişimi takip etmek, insanlar tarafından yaygınlaşmıştır. Bilişim sistemleri, kamu kurumlarına ilave olarak enerji, haberleşme, su kaynakları, tarım, sağlık, ulaşım, eğitim ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlarda da yoğun olarak kullanılmaktadır.

Bilişim sistemlerinin hızlı gelişimi, gerçek dünyaya sunduğu hizmet ve oluşturduğu riskler nedeniyle, siber güvenliğin sağlanması için stratejiler

belirlemeyi gerektirmiştir. Özellikle 20.yüzyılın son 10 yılında ve 21.yüzyılda yaşanan siber savaşlar, gerginlikler ve haktivist hareketler, bilişim sistemlerinin beraberinde tehlikeleri de geliştirdiğini göstermiştir. Dünya'da birçok ülke Ulusal Siber Güvenlik Stratejilerini belirlemiştir. Türkiye'de de hem ulusal güvenliğin, hem de rekabet gücünün önemli bir boyutu olan bilgi ve iletişim sistemlerinin güvenliğinin sağlanması için Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı Ocak 2013'te hazırlanmıştır.

Çözüm üretilebilmesi için öncelikle sorunların belirlenmesi ve sorunlara ortak bir dil kullanılması gerekmektedir. Siber sorunların farklı kavramlarla dile getirilmemesi ve ortak bir dil kullanılması çözüm üretmekte fayda sağlayacaktır.

I. Türkiye Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Türkiye, siber güvenlik konusunda stratejisini belirlemiş ve 2013-2014 yıllarında gerçekleştirmeyi hedeflediği eylemlerin planını yapmıştır. Ulusal Siber Güvenlik Stratejisi, siber güvenliğe dair kavramları tanımlamış ve siber güvenlik terminolojisini oluşturmuştur. Siber güvenlik terminolojisinin ve sözlüğünün oluşturulması da, belirlenen eylem planına göre Türk Dil Kurumunun sorumluluğundadır. (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013)

A- Bilişim Sistemleri

Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda yer alan sistemleri ifade eder[1]. Bilişim sistemlerinin tanımlanması kamu, gerçek ve tüzel kişilere ait bilişim sistemlerinin tanımlanmasını da kolaylaştırmıştır.

Ulusal Siber Güvenlik Stratejisi, kamu bilişim sistemlerini, Türkiye Cumhuriyeti kamu kurum ve kuruluşlarına ait olan ve/veya kamu kurum ve

[1] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Ocak 2013

kuruluşları tarafından işletilen bilişim sistemleri olarak tanımlamaktadır. Gerçek ve tüzel kişilere ait bilişim sistemlerini ise, Türkiye Cumhuriyeti kanunlarına tabi olarak gerçek ve tüzel kişilere ait olan ve/veya gerçek ve tüzel kişilerce işletilen bilişim sistemleri olarak ifade edilmiştir. (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2013)

B- Siber ortam

Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamdır[2].

"Siber Uzay" terimi ilk kez, yazdığı bilim kurgu romanlarıyla tanınan William Gibson tarafından 1980'li yılların başında kullanılmıştır ve dilimize de giren terim halen kullanılmaktadır. Siber uzay teriminin yerine Ulusal Siber Güvenlik Stratejisinde siber ortam terimi tercih edilmiş ve tanımlanmıştır.

Dünyada her türlü hizmet ve faaliyet siber ortamda gerçekleşmektedir. Siber ortam, insanlığın faydasına birçok hizmeti sunmaktadır. Kamu ve özel kuruluşlar, hizmet alanı olarak siber ortamdan faydalanmaktadır. Faydalı birçok faaliyeti de içinde barındıran siber ortam, kötü niyetli amaçlar içinde kullanılabilmektedir.

C- Siber Güvenlik Olayı

Siber güvenlik olayında, gizlilik, bütünlük ve erişilebilirlik unsurlarının önemi üzerinde durulmuştur. Bu 3 unsurun tanımları da siber güvenlik stratejisinde yapılmıştır.

Gizlilik, bilişim sistem ve verilerine sadece yetkili kişi veya sistemlerce erişilebilmesini; bilişim sistemlerine ait veya sistemdeki gizli verinin yetkisiz kişi veya sistemlerce ifşa edilmemesini ifade eder. Bütünlük, bilişim sistemlerinin ve

[2] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Ocak 2013

bilginin sadece yetkili kişilerce veya sistemlerce değiştirilebilmesini ifade eder. Erişilebilirlik ise, yetkili kişilerin ve işlemlerin ihtiyaç duyulan zaman içerisinde ve ihtiyaç duyulan kalitede bilişim sistemlerine ve bilgiye erişebilmesini ifade etmektedir.

Siber Güvenlik Olayı, bilişim sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesidir[3].

Genellikle siber saldırı olarak kullandığımız terimin yerine siber güvenlik olayı tanımlanmıştır. Gizlilik, bütünlük veya erişilebilirlik unsurlarının ihlal edilmesi olarak açıklanmıştır.

Siber ortamı oluşturan bilişim teknolojileri, saldırılarda aracı olarak kullanılabilmektedir. Saldırılar, hackerlar aracılığıyla kişisel menfaat veya internet mafyasına hizmet etmek için yapılabilmektedir. Haktivist gruplar, saldırılarını siyasi hedeflerine propaganda yapmak, gürültü çıkarmak ve dikkatleri üzerlerine çekmek için yapmaktadır. Devlet destekli saldırılar genellikle inkar edilse de, hedef ülkenin siber ortamına müdahale etmek, ekonomik zarar vermek ve istihbari bilgilerini ele geçirmek amaçlanmaktadır. Siber ortamda yaşanılan saldırılarla genellikle zarar vermek amaçlanmıştır ve ulusal bir güvenlik sorunu haline gelmiştir.

D- Siber Güvenlik

Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade eder[4].

[3] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Ocak 2013
[4] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Ocak 2013

Siber saldırılara karşı alınabilecek önlemleri ortaya koymaktadır. Siber güvenlik, gerçekleşen saldırılarla verilebilecek zararlar en aza indirilebilir veya tamamen önlenebilmektedir.

E- Ulusal Siber Güvenlik

Ulusal siber ortamda bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem ve verinin ve bunların sunumunda yer alan sistemlerin siber güvenliği olarak tanımlanmaktadır[5].

Ülkelerin uğrayacağı siber saldırılar ülkedeki yaşamı durdurma noktasına getirebilecek tehlikededir. Nitekim yakın tarihte Estonya ve Gürcistan'a yapılan saldırılar tehlikenin boyutunu göstermiştir. Ülkelerin, saldırılardan korunmak için strateji belirleme ve tedbir alma gerekliliğini ortaya koymuştur.

§ 3. İNTERNET

İnternet, hayatımıza girmesiyle en etkin kitle iletişim araçlarından biri haline gelmiştir. Kişisel kullanım aracı olan cep telefonları bile internet ortamına entegre olmuştur. Günümüzde birçok sosyal ağ uygulamaları bulunan akıllı telefonlar çocuklardan yetişkinlere kadar, nerdeyse her elde gezmektedir. Web sitelerinde yayımlanan yazıları sadece okumakla kalmayıp, yazılanlara ve görüntülenenlere yorum yapılabilmektedir. Böylece internet, milyonlarca kullanıcının içeriğine katkı sağladığı sanal bir ortam haline gelmiştir.

İnternetin hayatımıza girmesiyle hayatı kolaylaştıran birçok özelliği bulunmaktadır. Bilgisayar başından, uzaktan eğitim yapılabilmektedir. Mağazalara gitmeden dünyanın her yerinden alışveriş imkanı sağlanmaktadır. EFT, havale gibi işlemlerde zamandan tasarruf edilmekte ve paranın elde dolaşımına gerek kalmadan bankacılık işlemleri yapılabilmektedir. Birçok bilgiyi içinde barındıran internetten istifade edilebilmektedir[6]. (GÖK, 2012)

---

[5] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Ocak 2013

[6] Mehmet Salih GÖK, 5651 Sayılı Kanun ve Bilgi Güvenliği İlişkisi, 1.Baskı, İstanbul, Eylül 2012

İnternetin faydaları yanında birçok zararının da olduğu görülmüştür. İnternet, art niyetli düşüncenin faaliyetlerini sürdürmek için aracı olarak kullandığı bir alan haline de gelmiştir. Terör örgütlerinin iletişimini sağlamaktadır. Sadece faydalı eğitim için kullanılmayan internet, terör örgütlerinin planlarını gerçekleştirmede, militanlarını eğitmede kullandığı bir ders aracı olarak kullanılmaktadır.

Terör örgütleri yaşamlarını propaganda ile sürdürürler. İnternet ise propagandanın daha ucuz ve kolay yapılmasına, daha kısa sürede büyük bir kitleye ulaşmasına olanak sağlar. İllegal dergi, gazete ve kitapları internet ortamında yayınlayarak üyelerini ve düşünceye yakınlık duyanları eğitmektedirler. Polis takibinden nasıl kurtulabilineceğinden, bomba yapımına kadar bütün bilgileri internet ortamında bulmak mümkündür. Terör örgütlerinin internet ortamını propaganda, bilgi toplama ve haberleşme amaçlı kullandıkları gözlenmektedir[7]. (ALKAN)

I. İnternetin Ortaya Çıkışı

1957 yılında Sovyet Sosyalist Cumhuriyetler Birliğinin ilk yapay uydusu Sputnik'i uzaya göndermesine tepki olarak, ABD Savunma Bakanlığına bağlı ARPA (Advanced Research Projects Agency) adında bir birim oluşturulmuştur. Birbirinden bağımsız bilgisayarların birbirine bağlanarak oluşturulduğu, bilgisayar ağı ileri araştırma projesi ajansına (ARPANET-Advanced Research Projects Agency Network) adı verilmiştir. ABD tarafından geliştirilen ve askeri bir projeye dayanan bu birim 1969 yılında ilk bilgi transferini gerçekleştirmiştir. ABD Savunma Bakanlığınca kullanılan ARPANET, 1974-1976 yılları arasında araştırma amaçlı olarak INTRANET şeklinde kullanılmıştır.

[7]Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler, http://www.caginpolisi.com.tr/20/41-43.htm#_ftn5. Necati ALKAN, Erişim, 07/04/2013

ARPANET beklenenden daha fazla büyümüş ve askeri kısmı MILNET olarak ayrılmıştır. ARPANET gelişerek INTERNET adını almıştır. İnternet, büyük küçük binlerce ağın birleşmesinden oluşmuş en büyük ağdır[8].

1 Ocak 1983 tarihinde TCP/IP (Transmission Control Protocol and Internet Protocol) protokoküne geçiş yaparak internet ticari amaçlı olarak kullanılmaya başlanmıştır. TCP/IP standart protokolü karşılıklı birbirine bağlanmış bilgisayar ağı anlamına gelmektedir.

Web'in babası olarak kabul edilen ve interneti küreselleştirerek geniş kitlelere kullanıma sunan İngiliz fizikçi Tim Berners-Lee, World Wide Web'i (www) 1989 yılında icat etmiştir. Hiypertext olarak bilinen http sistemini geliştirmiştir. Cenevre'de ki Avrupa Parçacık Fiziği Laboratuarında (CERN) çalışan Berners-Lee'nin amacı, çalıştığı laboratuardaki elektronik belgelere kolayca ulaşabilmek ve bu belgeler ile çoklu kullanıcılı ortamda aynı anda birçok kişinin çalışmasını ve hataları düzeltebilmesini sağlamaktır[9]. İnternet teknolojisinde, ilk web sitesini CERN'de açarak bir devrim yaratmıştır. İnternetin ortaya çıkışını ve gelişmesini sağlayan ARPANET 1990 yılında lağvedilmiştir[10].

En duyarlı konularda, ABD yönetiminin üst kademelerinde yıllarca görev yapmış ve 2001 yılında ABD Başkanının siber güvenlik danışmanlığına atanan Richard A. Clarke Siber Savaş (Cyber War) isimli kitabında deneyim ve düşüncelerini paylaşmıştır. Clarke, internetin, askeriyenin bir icadı zannedilse de, aslında bunu yapanların 60'lı yıllarda MIT, Stanfort ve Berkeley Üniversitelerinde okumuş olan ve şimdilerde yaşlı insanlar olan hippilerin icadı olduğunu belirtmiştir[11]. (CLARKE & KNAKE, 2011)

---

[8] Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler, http://www.caginpolisi.com.tr/20/41-43.htm#_ftn5. Erişim, 13/04/2013

[9] İnternet ve Hactivizm Yeni Toplumsal Muhalefet Bişimleri, http://www.izinsizgosteri.net/new/?issue=64&page=1&content=539#, Ali PEKŞEN, Erişim 07/04/2013

[10] Brief History of the Internet http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#origins Erişim, 01/04/2013

[11] Richard A. Clarke, Robert K. Kanke, Siber Savaş (Cyber War), (çeviren:Murat Erduran) İstanbul Kültür Üniversitesi, Basım 2011, s.47

İnternetin askeri alanda kullanılmak üzere icat edildiğine dair genel yargı mevcuttur. Clarke, genel yargıdan farklı olarak internetin hippiler tarafından icat edildiğini savunsa da, internet askeri alanda kullanılmaya başlanılmış ve geliştirilmiştir.

İnternetin kullanılmaya başlanması ve toplum hayatına girmesiyle sürekli büyüyen internetin, denetimi zor bir hale gelmiştir. Denetimi zor bir hale gelen internet, faydasını ve zararlarını da beraberinde getirmiştir.

Devlet kurumlarında, özel şirketlerde internet ağından faydalanılmaktadır. Vatandaş-devlet ilişkisi internet üzerinden devam ettirilmeye çalışılmaktadır.

II. Hacker

Hacker, İngilizce bir kelimedir. Türçe karşılığı ise bilgisayar korsanıdır. Hackerlar, bilgisayar programlarına vakıf, yetenekli kişiler olarak tanınmaktadır. Hack, kelimesi Türkçe olmamakla birlikte, beraberinde birçok terimi getirmiştir. Örneğin, hacker, hacking, hacktivism gibi. Bu nedenle anlatımda bütünlüğü sağlamak için hack kelimesi ve türevlerine yer verilecektir.

Hacker, şahsî bilgisayarlara veya çeşitli kurum ve kuruluşlara ait bilgisayarlara ve ağlara izinsiz olarak giriş yapan kişidir[12]. Basit manada hacker, dijital alemin güvenlik kusurlarını kullanarak bu işten ekonomik gelir elde eden kişilerdir[13]. Bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standardın üzerinde beceriye sahip bulunan ve böylece ileri düzeyde yazılımlar geliştiren ve onları kullanabilen kişilerdir[14].

Hackerlar için farklı tanımlar yapılmıştır. Genel olarak hacker, bilişim sistemleri konusunda yetenekli, sistem açıklarını arayan ve açıklardan izinsizce sisteme sızan kişilerdir. Bilgisayar konusunda eğitim almak kişiyi hacker yapmamaktadır. Hackerların yeteneklerini farklı kılan özellikleri vardır. Gizemli

[12] http://tr.wikipedia.org/wiki/Hacker Erişim, 07/04/2013
[13] Beyaz Şapkalı Hackerlar, http://www.imajweb.com/beyaz-sapkali-hackerlar.html Erişim, 07/04/2013
[14] Hackerlar? Sanal Dünyanın Yaramaz Çocukları, http://internethukuku.net/hackerlar-sanal-dunyanin-yaramaz-cocuklari/ Erişim, 07/04/2013

olan durumlara merakı, sistemlere sızmak için duyduğu heyecanı, bazen bir sisteme sızmak için 2 yıl boyunca sistem açıklarını kollayabilecek sabrı ve arzusu, hackerları farklı kılmaktadır. Aksi taktirde bilgisayar mühendisliğinden mezun her kişiye hacker denmesi gerekmektedir.

Hackerlar, düzenli olarak hem bağımsız bilgisayarlara hem de büyük ağlara girebilecek yetenektedirler. Bir kez eriştiklerinde, kötü amaçlı programlar yükleyebilir, gizli bilgileri çalabilir veya gizliliği ihlal edilen bilgisayarları spam dağıtmak için kullanabilmektedir[15]. (Kaspersky)

Hackerlar, sosyal mühendislik yaparak veya internetin açıklarından faydalanarak sosyal uygulama ve e-posta hesaplarının şifrelerini kırabilir, sistemlere izinsiz sızabilir, ulusal ve uluslar arası güvenlik sırlarına kadar erişip, eriştikleri bilgileri çalabilirler.

Devletler ve şirketler hacker avına çıkmış durumdalar. Eski hackerlar artık beyaz şapkalı veya etik hacker oldular. Beyaz şapkalı hackerlar bankalarda, ilaç şirketlerinde, üniversitelerde, devlet kuruluşlarında, çok uluslu şirketlerde Bilişim Başkanı veya Bilişim Güvenliği Başkanı olarak görev yapmaktadır. Yıllardır yapılan Black Hat konferanslarında hackerlar bilişim sistemlerindeki açıkları paylaşmaktadır. Amerika bu hackerlara iş teklif etmektedir. Amerika olarak bu hackerlara ihtiyacı olduğunu ve birlikte çalışmak istediğini açıkça belirtmektedir.

III. Hacking

Hacking, bir sistemin gizli, ulaşılamayan bilgilerini ele geçirmek demektir[16]. Hacking işlemi aynı zamanda haklamak olarak da tabir edilmektedir. Sistemin engellerini aşarak, sisteme sızmak ve sistem sorumlularını devre dışı bırakmaktır. Sisteme giren hacker sistem üzerinde izinsiz dolaşabilir, bilgisayara erişim şifrelerini elde edebilir, bulduğu bilgileri çalabilir ve istediği değişikliği de yapabilmektedir.

---

[15]Bilgisayar Korsanlığı, http://www.kaspersky.com.tr/hacking, Erişim, 07/04/2013
[16] Hacklemek nedir? http://www.genzom.8k.com/hackleme.htm Erişim, 01/04/2013

Hacking işleminde, hacker eve giren hırsızdan farklı olarak, bilgisayarınıza girip, sizin veya şirketinizin mahremini ihlal etmiştir. Bu işlem sırasında bilgisayarınızdaki programların boşluklarını veya zayıf noktalarını hedef almıştır. Bilgi hırsızlığı yapmaksızın, sisteminize izinsiz girilmesi de bir hackingtir.

Günümüzde birçok örgüt, kendileri için bilgi çalacak yazılımları geliştirmeleri için hacker arayışı içindeler. Artık mafya, kiraladıkları büyük botnetleri spam ya da saldırı amacıyla kullanabildiği gibi tehdit aracı olarak kullanıp haraç toplayabilmektedir. Kişisel bilgilerin ve hesapların ele geçirilmesi ise mafya için güzel bir fırsattır.

Siber savaşlar yaşanıyor ve daha kapsamlı siber savaşların çok uzak olmadığını fark eden hükümetler için de hackerlar çok kıymetli.

IV. Hacker çeşitleri

Richard A. Clarke, uzaktan kumanda ile makinelerde kısa devre yaptırıp, ofiste yangın çıkartan bir hackerın siber suçlu olduğunu, ancak bunu Amerikan ordusu için yapıyorsa, siber suçlu değil, siber savaşçı olduğunu belirtmiştir. Hackerın sisteme sızarak yapmış olduğu illegal davranış, devlet adına yapıldığında legal olarak görülmektedir.

Hackerlar, eylemlerini kimin adına yaptıklarına ve eylemlerinin amaçlarına göre kendi aralarında çeşitlilik göstermektedir. Genellikle şapka renklerine göre niyetleri dile getirilen hackerlar, iyi niyetli veya kötü niyetli olarak nitelendirilmiştir. Beyazı masumiyet, siyahı kötülük ve gri rengi ise netlik kazanmamış niyetler olarak belirlenmiştir. Kırmızı şapkalılar ise kendilerini diğer hackerlardan daha farklı görmektedir.

A- Siyah Şapkalı Hacker

Tehlikeli olan hacker çeşididir. Amaçları, güvenlik açıklarından faydalanmak suretiyle gizli bilgileri ele geçirmek veya sistemi çalışmaz hale getirmektir.

Siyah şapkalı hacker olarak bilinen Jonathan James, daha 15 yaşındayken, ABD Savunma Bakanlığı, NASA, Bell South, Miami/Dade gibi kuruluşları hacklemiştir. Uluslararası Uzay İstasyonu'nun ne şekilde işlediğini bilmeye yetecek kadar veri toplayan James, NASA'dan değeri 1,7 milyon dolar olduğu hesaplanan bilgiye de ulaşmıştır. Hacking saldırılarına maruz kalan bazı büyük şirketlerin şikâyetçi olması ve bu suçlamaları kabul etmese de, suçlamalardan korkan ve hüküm giyeceğini düşünen Jonathan 2008 yılında intihar etmiştir[17]. (Dünyaca Ünlü "5 Siyah Şapkalı Hacker", 2012)

ShadowCrew adlı hacker grubunun lideri olarak toplu bir hareketin öncüsü olan Albert Gonzalez, grubuyla birlikte 2 senede 17 milyon kredi kartı ve ATM kartı numarasını ele geçirerek, ABD nüfusunun büyük bir kısmının bilgilerini ele geçirip, bu numaraları para karşılığı satmıştır. 2010 yılında yakalanan Albert Gonzalez 20 yıl hapis cezası almıştır.

Kevin Poulsen, yarışma düzenleyen radyo istasyonunun telefon hattını hackleyerek, kendisini 102. arayan kişi olarak gösterip Porche araba kazanmıştır. Federal sistemleri hackleyerek arananlar listesine giren bilgisayar korsanı daha sonra yakalanmış ve cezasını çekmiştir. Poulsen, hapisten çıktıktan sonra gazetecilik yapmaya başlamıştır.

Bir başka hacker Gary McKinnon, en büyük askeri bilgisayar saldırısı düzenleyen bilgisayar korsanıdır. ABD'nin silahlı kuvvetlerinin ve NASA'nın bilgisayarlarına erişmiştir. McKinnon, kendisi kabul etmese de ABD yetkililerince, sisteme sadece sızmakla kalmayıp, bazı önemli dosyaları sildiği, 300'den fazla bilgisayarı işleyemez duruma getirdiği ve 800.000 doları aşkın zarara sebep olduğu gerekçesiyle aranmaktadır. İngiltere'de yaşayan McKinnon, ABD'ye iade edilmemek için mücadele etmektedir[18]. (Profile:Gary McKinnon, 2012)

---

[17] Dünyaca Ünlü "5 Siyah Şapkalı Hacker"http://www.imajweb.com/dunyaca-unlu-5siyah-sapkali-hacker.html, 07/04/2013

[18] Profile: Gary McKinnon, http://www.bbc.co.uk/news/uk-19946902 Erişim, 07/04/2013

1957-1998 yıllarında faaliyet gösteren, Amerikan bilgisayar şirketi Digital Equipment Corporation'nın ağını hackledikten sonra hapis cezası alan Kevin Mitnick, ulusal savunma uyarı sistemini hackleyerek, sistemin bazı sırlarını elde etmiştir. En çok aranan bilgisayar korsanı olarak dünyaya adını duyuran Mitnick, cezasını çektikten sonra bilgisayar güvenliği danışmanı olarak şirketini kurmuştur. Mitnick, artık siyah şapkayı çıkarıp, beyaz şapkasını takmıştır. Hatta bilgisayar kullanıcılarını uyardığı ve bilinçlendirdiği iki kitap yayınlamıştır.

Siyah şapkalı hackerlar genellikle ulaşılmasında sakınca bulunan gizli bilgileri elde etmek suretiyle maddi zararlara sebep olmuşlardır. Maddi zararların yanı sıra sistem açıklarından sızarak, kritik bilgiler ele geçirilmiştir. Siyah şapkalı hackerlar, kritik bilgilerin ele geçirilebileceğini, kritik bilgilerden sorumlu kuruluşların yeterli korunamadığını göstermiştir.

B- Beyaz Şapkalı Hacker

Beyaz şapkalı hackerlar, donanımlarını, siyah hacker'lara karşı alternatif çözümler üreterek kullanmaktadır. Güvenlik kusurlarını bulan bu kişiler, şirketlere bu tarz durumlardan nasıl kurtulabilecekleri konusunda yardımcı olmaktadır. Beyaz hacker unvanı almış insanlar bilgilerini ve donanımlarını özel şirketlere ve istihbarat örgütlerine yardım etmek biçiminde sarf etmektedir[19].

World Wide Web (www) sistemini ve hiypertext olarak bilinen http sistemini hayatımıza kazandıran web'in babası Tim Berners-Lee beyaz şapkalı hackerdır. Beyaz şapkalı hackerlardan Linus Torvalds, Linux'un mucididir. FBI ile işbirliği yaparak, daha önce kendi sistemini kırmış olan Kevin Mitnick'i gün yüzüne çıkartan Tsutomu Shimomura, Kevin Mitnick'i yakalayan kişi olarak tanınmıştır.

[19] Beyaz Şapkalı Hackerlar, http://www.imajweb.com/beyaz-sapkali-hackerlar.html Erişim, 07/04/2013

C- Gri ve Kırmızı Şapkalı Hackerlar

Gri şapkalı hackerlar, duruma göre iyi veya kötü olabilen hackerlardır. Malumat pazarlayarak hayatını kazanan kimselerdir[20]. Bu nedenle dikkat edilmesi gereken hackerlardır. Menfaatler çerçevesinde değişiklik gösterebilmektedirler.

Günümüzde bir de kırmızı şapkalı hacker olduğunu savunanlar vardır. Ne beyaz şapkalı hacker özelliği, ne de siyah şapkalı hacker özelliği göstermediklerinden, belli bir hacker kültürü ve hactivizm inancı olmasından dolayı RedHack kendini kırmızı şapkalı hacker olarak tanımlamaktadır.

Script Kiddie ve Lamerler ise hacker değillerdir. Script Kiddie, hackerlığa özenen kişilerdir ve genellikle kişilerin e-posta veya anında mesajlaşma şifrelerini çalarlar. Lamer de, Script Kiddie benzeri kişilerdir, ne yaptıklarını bilmeyen, hackerlık için yeterince bilgisi olmayan kişilerdir[21].

§ 4. SİBER SALDIRILAR

I. İletişim ve Aktivizm

20. yüzyılın en önemli buluşu olan internet, elektronik haberleşmeyi sağlamıştır. İnternet kullanarak uzaktaki insanlara e-posta gönderilebilmekte veya anlık mesajlaşılabilmektedir. Aynı zamanda elektronik haberleşmenin gelişmesi, büyük önem kazanmıştır. Çünkü bu dönemde ses ve görüntünün elektronik yöntemlerle iletilmesinin, önceki teknik gelişmelerden daha büyük sosyo ekonomik, kültürel etki ve sonuçları olmuştur[22]. (ÖZDEMİR, 2009)

İletişim alanındaki gelişmeler, haberleşmenin alanını genişletmiştir. Dünyada olup bitenden insanlar kitleler halinde kolayca haberdar olabilmişlerdir. Bu sayede 20. yüzyılda artık kitle iletişimi söz konusu olmuştur.

---

[20] Beyaz Şapkalı Hackerlar, http://www.imajweb.com/beyaz-sapkali-hackerlar.html Erişim, 07/04/2013

[21] Hacker, https://tr.wikipedia.org/wiki/Hacker Erişim, 12/05/2013

[22] Dr. Hayrunnisa ÖZDEMİR, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Ankara, 2009, §.3 s.14, 15 ve orada dn. 43'te anılan Özkök, 4 vd; Alemdar, 94; Trachsel, 96,97.

İnternetin, toplumu bilgilendirme ve yönlendirme de etkisi büyüktür. Cep telefonlarının kullanılmaya başlanmasıyla iletişimde yeni bir devir başlamıştır. Kişisel kullanım aracı olarak kabul edilen cep telefonu, insan vücudunun parçasıymış gibi görülmektedir. Cep telefonlarının zaman içinde geliştirilmesi, internet ağına uyum sağlamış olması ve cep telefonlarında çeşitli uygulamaların kullanılabilir olması iletişime bağımlılığı artırmıştır.

IDC'nin (International Data Corporation) 3 aylık raporlarında, 2013 yılında akıllı telefon satışlarının cep telefonu satışlarını çok geride bırakacağı açıklanmıştır[23]. Artık tüketici tercihleri değişmiştir. Akıllı telefonlara uyumlu sosyal ağ uygulamaları telefonları daha cazip hale getirmiştir.

Sosyal ağlar, twitter, facebook, instagram gibi sosyal paylaşım siteleri aktivizmin oluşmasında temelleri atan ortamlar haline gelmiştir. Sosyal ağlarda zaman ve mekân sınırlaması yoktur. Sosyal ağlarda, paylaşım ve tartışma esastır. İnsanlar, sosyal medya platformunda iletişim ve paylaşımda bulunarak, hemfikir ve zıt fikirlerin ortaya çıktığı, aynı fikirlerin birbirini desteklediği grupları oluşturmaktadır.

İletişime olan bağımlılık, kitlesel tepkilerin ve düşüncenin anlık olarak paylaşılmasını sağlamıştır. Düşüncelerin ortaya konması, etki ve tepkinin karşılık bulması kolaylaşmıştır. Etki ve tepkilerin, taraf bulma ve olgunlaşma süreci kısalmıştır.

Aktivizm, toplumsal veya politik değişiklik meydana getirmek için yapılan eylemlerdir. Tarihte aktivist hareketler, zamana uygun olarak geliştirilen iletişim araçlarından faydalanılarak yapılmıştır. Matbaalarda basılan bildiriler, telgraflar, teksir makineleri, fotokopiler, birçok toplumsal hareketin önemli bir parçası olmuştur.

---

[23]Worldwide Quarterly Mobile Phone Forecast, http://www.idc.com/tracker/showproductinfo.jsp?prod_id=36#.UWlouErhFCk Erişim, 13/04/2013

Örgütlenmenin, temelinde iletişim yatmaktadır. Dijital aktivizm, internet ve aktivizm arasındaki ilişkilerin sadece bir boyutunu dile getirir. Günümüzde internet kullanılmadan yapılan bir aktivizm mümkün değildir. Aktivizm, dijital bir boyut kazanmıştır[24]. (UÇKAN)

II. Hacktivizm

Hacker ve activism kelimelerinin karışımı ile oluşturulmuş yeni bir terimdir. Hacktivist, amaçları için siber ortamı kullanmayı tercih eden, sanal protestoculardır.

Yaklaşık 7 milyar olan dünya nüfusunun, 3 milyara yakın internet kullanıcısı bulunmaktadır. Zararlı veya faydalı, birçok bilgiyi içinde barındıran internet, erişimdeki kolaylığı ve hızlılığı ile hizmet vermektedir. Genişleyen ağ ve hizmetler ile internet üzerinden örgütlenmenin daha kolay ve kısa sürede olabileceği bir gerçektir. Savaş stratejilerinden biri uçaklardan bildiri atmaktır. Artık bu stratejiye gerek kalmadan internet vasıtasıyla insanları eğitmek, örgütlemek ve akım oluşturmak basitleşmiştir. Öyle ki, Chiapas'ta ormanın derinliklerinde yaşayan Zapatistalar, medyayla ve dünyayla iletişimlerini internet aracılığıyla sağlamıştır. İnsanların birbirleriyle anlaşması ve bilgi paylaşımında bulunmaları için mesafe esastır. Ancak internet aracılığıyla iletişim mesafeyi önemsizleştirmiştir. Bilgi paylaşımını kolaylaştırmıştır, daha büyük kitlelerle daha kısa zamanda irtibat kurmayı sağlamıştır.

III. Hacktivist Hareketler

Son yıllarda bütün dünyayı ilgilendiren hactivist hareketler, bireysel veya gruplar halinde faaliyet göstermeye başlamıştır. Artık hackerlar şahsi menfaatlerinden ziyade kamunun menfaatini düşünerek hareket ettiklerini savunarak, hacker grupları oluşturmaktadır. Hacktivistler, düşüncelerini genellikle web sitelerini hackleyerek veya hacking sonucu elde ettikleri bilgileri paylaşıma

[24] Sokak+(Dijital) İletişim=Aktivizm, http://www.politus.org.tr/Detay2.aspx?id=105 Özgür Uçkan, Erişim 29/03/2013

açarak sergilemektedir. Hactivistler genel olarak internette sansüre karşı çıkmaktadır ve internetin özgür olması gerektiğini savunmaktadır.

Hacktivist gruplar, genellikle siyasi olaylara, tepkilerini siber ortamda göstermektedir. Sanal protestocuların eylemlerine kendi üyeleri haricinde destek vermek isteyenlerde katılmaktadır. Devletin bütünlüğünü ve güvenliğini tehlikeye düşüren tehdit unsuru olabilmektedir.

A- Wikileaks ve Bradley Mannig

Irak operasyonunda görev yapmış ABD kıdemli eri Bradley Manning, 1966-2010 tarihleri arasında ABD Dış İşleri Bakanlığınca yapılan gizli yazışmaları, ordu veri tabanından indirdiği doküman ve görüntüleri, 2010 yılı Kasım ayında Wikileaks sitesine sızdırmıştır. Yayınlanan görüntüler içerisinde, Cenevre Sözleşmesine göre sivil hedeflerin bombalanamayacağı kuralını ihlal eden görüntüler de yer almaktadır.

Pentagon'u rahatsız eden ve ABD'nin yönetimini sıkıntıya düşürecek bilgiler gözler önüne serilmiştir. ABD diplomatik yazışmaların kamuya sızdırılması uluslar arası arenada panik yaşatmıştır. Wikileaks sitesi ve kurucusu Julian Assange hakkında sansüre karar verilmesi üzerine, internetin özgür olması gerektiğini savunan hacker grubu Anonymous tepkisini sokaklardan duyurmaya çalıştı.

Bradley Manning, kendi ülkesinin gizli bilgi ve belgelerini dünyaya ifşa etmiştir. Bradley Mannig kendini "bilgi kamuya aittir, hakkı olanlara bedava sunulmalıdır" şeklinde savunmuştur[25]. (AYBASTI, 2013)

Wikileaks, tüm dünyaya açık, herkesin erişebileceği, kolaylıkla doküman gönderebileceği bir sistemle çalışmaktadır. Dolayısıyla büyük bir bilgi havuzu oluşturulmaktadır. Dokümanları gönderenlerin bilgileri, yani kaynaklar daima gizli kalmaktadır. Dokümanları gönderenler Wikileaks ile sesini duyurmaya ve bir

[25] http://www.bagimsizsinema.org/portfolio/red/ Red Belgeseli, Erişim 28/03/2013

şeyleri düzeltmeye çalışmaktadır. Hem Wikileaks çalışanları hem de doküman havuzuna katkıda bulunanlar için bu haksızlıklara karşı gelmektir.

B- Aaron H. Swartz

Aaron H. Swartz, 2009 yılında Amerikan federal mahkemelerine ait PACER veritabanında bulunan ve para karşılığı satılan yaklaşık 18 milyon belgeyi indirip, internette yayınlamıştır. 2011 yılında, MIT Üniversitesinin (Massachusetts Institute of Technology) bilgisayarlarını kullanarak, akademik dergileri arşivlemede kullanılan ve çevrimiçi bir sistem olan JSTOR (Journal Storage)'dan 4 milyona yakın makale, belge ve kitabı bilgisayarına indirip, internet üzerinden paylaşıma açmıştır[26]. (AYBASTI, 2013)

Bilgi korsanlığı ve yasadışı dosya indirme suçlarından yargılanan ve hakkında 35 yıl hapis cezasına çarptırılması beklenilen Aaron H. Swartz 10 Ocak 2013 tarihinde, kendini asarak hayatına son vermiştir[27].

Swartz, Reddit sosyal haber sitesinin kurucusudur. Telif hakkı ve mülkiyet hakkı konulu, internette telif hakkı ile korunun şeyleri yayınlatmama, telif haklarının ihlali durumunda hak sahiplerine siteler hakkında mahkeme karar çıkartmayı sağlayan, SOPA ve PİPA yasa tasarılarına karşı internet özgürlüğünü savunan Demand Progress hareketinin de kurucularındandır. İnternette özgürlüğü, bilginin özgürce paylaşılması gerektiğini savunan Swartz hactivist hareketin öncülerindendir.

C- Anonymous

2003 yılında bir grup bağımsız insanın internet üzerinden birleşmesiyle oluşmuş hactivist bir gruptur. Gülen adam maskesi grubun simgesidir. Sloganı ise "Biz anonimiz. Orduyuz. Affetmeyiz. Unutmayız. Bizi bekleyin." Şeklindedir. Birbirini tanımayan, dünyanın her yerinden üyesi bulunmaktadır. Herkes anonymousun bir üyesi olabilir ve eylemlere destekte bulunabilir. Bu nedenle net olarak üye sayısı bilinmemektedir. Anonymous, hiyerarşik bir düzene ya da

[26] 28/03/2013 http://www.bagimsizsinema.org/portfolio/red/ Red Belgeseli, Erişim 28/03/2013
[27] Aaron Swartz, http://tr.wikipedia.org/wiki/Aaron_Swartz Erişim, 01/04/2013

liderliğe karşıdır. Siyasi olaylara tepkilerini genellikle devlet teşkilatına ait sitelere saldırılarda bulunarak göstermektedir. Sabit politik bir hedefleri yoktur. Grup, internet özgürlüğünü savunmaktadır. Bu nedenle Wikileaks belgelerinin açıklanması üzerine verilen sansür kararına propagandasını sokaklarda yapmıştır. Seslerini sadece internet üzerinden değil, zaman zaman sokaklardan duyurmaya çalışmaktadır. Saldırılarında genellikle DDoS silahını kullanmaktadır.

Dünyanın dört bir yanında Anonymous bağlantılı gruplar mevcuttur. Dağınık bir yapılanmaları vardır, ancak onları bir araya getiren ve organize olmalarını sağlayan internettir. Bu dağınık yapılanma içinde bazen saldırı hedeflerine karşı ikiye bölünmeler olabilmektedir.

Anonymous adını ilk kez Sony operasyonu ile duyurmuştur. ABD ordusuna hizmet veren Lockheed Martin şirketinin enformasyon ağına saldırı düzenlemiştir. 2011'de İrlanda yerel seçimlerinde partinin web sitesini ele geçirerek, siteye mesaj bırakmıştır. Arap Baharı'na destek veren grup, Tunus'ta yaşanan devrim sırasında Tunus'lu hackerlarla birlikte devletin 8 web sitesini çökertmiştir. Wikileaks ve Bradley Manning olayından sonra hükümetin Wikileaks'ten belgeleri yayınlamayı durdurmasını istemiştir, ancak belgeler yayınlanmaya devam etmiştir. Anonymous Wikileaks ile çalışmak istemeyen Visa, MasterCard ve PayPal'a savaş açmıştır ve 8 Aralık 2010'da Visa ve MasterCard'ın siteleri Anonymous tarafından çökertilmiştir. Daha bir çok devlet ve özel şirket sitelerine saldıran grup, memnuniyetsizliklerini yaptıkları saldırılar ile göstermektedir. Öyle ki, beğenmedikleri ve tatsız buldukları Burger King'in ürettiği "Whopper" burgerin tatsız olmasını gerekçe göstererek Burger King'in Twitter hesabını ele geçirip, sayfanın tasarımını başka bir yiyecek şirketi olan McDonalds'ın logosu ve fotoğraflarıyla döşemiştir.

Anonymous, İsrail'in Gazze operasyonlarını protestosu 2012 yılında başlamıştır. "OpIsrael" adını verdiği siber saldırı operasyonuyla İsrail web sitelerini hedef almıştır. 7 Nisan 2013'te yine İsrail'e büyük bir siber saldırı düzenlemiştir.

D- RedHack

Kızıl kırıcılar olarak bilinen grup 1997 yılında, belirli bir tüzük ile yapılanmıştır. Şirinler isimli çizgi filmin, Şirin Baba, Doğrucu Şirin, Çalışkan Şirin, İsyankar Şirin, Şirine gibi iyi karakterli kahramanlarının isimlerini kod adı olarak kullanan grup üyeleri, sevimli ve zararsız oldukları imajını vermektedir.

Protestolarını, sosyal medya aracılığıyla yapmaktadır. Grubu, twitter hesabından, destekçileri takip etmektedir. Twitter hesapları aracılığıyla, yaptıkları eylemlerini ve saldırılarını destekçileri ile paylaşmaktadır.

İnterneti sadece bir araç olarak gören grup, 12 kişilik çekirdek kadrodan oluşmaktadır. 12 çekirdek kadro haricinde, sayısı 100'e ulaşan RedHack militanı bulunmaktadır. Kendilerini, sosyalizme inanan, bilişim alanındaki işçiler olarak nitelendiren grup üyeleri, çekirdek kadro haricinde birbirlerini tanımamaktadır ve belli güvenlik önlemleri çerçevesinde iletişim kurmaktadır. Eylemlerini belirlemede, halkın ihtiyaçlarının söz konusu olduğunu savunan RedHack, 2 grup çalışma sistemi geliştirmiştir. 1.grubun sistem açığı aradığını, açığını bulduğu sistemlere girip, sistemi hacklediğini, 2.grubun ise, eylemlerin belirli bir politik çizgide olduğundan gireceği sistemin açığını aramak şeklinde çalışma yürütmektedir. Türkiye'de yaşayan ve bu nedenle gündemi sıcak takip eden grup üyeleri, sokaklarda olduklarını, internet başında oturan asosyal kişiler olmadıklarını belirtmektedirler. Hacker kimliğiyle değil, devrimci olarak tanınmak isteyen grup, politik bir görüşleri olduğunu, açıklayacakları belgelerinde bu doğrultuya hizmet etmek zorunda olduğunu her fırsatta dile getirmektedir. Devletlerin, istihbarat örgütlerinin, sektörel anlamda kendi güvenliğini sağlamak isteyen veya Pazar yaratmak isteyen şirketler için siber istihbarat ve siber güvenlik, faydalanılması zorunlu bir alan haline gelmiştir. Bu bağlamda dış istihbarat servisleriyle faaliyet göstermediklerini, şirketler ve kişilerin tekliflerine cevap bile vermediklerini savunan grup, sosyalizm çıkarı olmayan, sosyalizmi hedeflemeyen hiçbir çalışmanın içinde olmayacaklarını ifade etmiştir. Tüzük çerçevesinde çalışan ve devrimci dayanışmanın ürünü olan grup, kendi içinde sosyalizmi hedef gösteren, bir şekilde sosyalist muhalefet içinde yer alan tüm

devrimci örgütlerin sonucu olduğunu, bunların ortak ürünü olarak, internet ortamında Redhack'in ortaya çıktığını belirtmiştir. Redhack'e karşı devletin oluşturmuş olduğu siber timlere karşı, kendilerine ve teknik bilgisine güvenen grup, yaptıkları saldırılar sırasında karşılarındaki saldırı ve savunma sisteminin yeteneklerini de ölçebildiklerini belirtmektedirler[28]. (RedHack, 2013)

"SEÇSİS", seçim sistemine müdahale yapmadıklarını, fakat sistemin bu tür bir şeye açık olduğunu, veri tabanında rahatlıkla oynamalar yapılabildiğini keşfeden RedHack, aslında hükümetlerin rahatlıkla kurulabileceği veya devrilebileceğinin sinyallerini vermektedir. Kendine ve teknik bilgisine güvenen grup, internet ortamında imkansız diye bir durumun olmadığının farkındadır.

Devlet kurumlarına karşı yapılan siber saldırılar, sadece uluslararası değildir. Devlet işleyişini eleştiren, iç tehditlere de maruz kalmaktadır. Haktivizm, önemini ve boyutunu yapılan faaliyetlerle göstermektedir.

RedHack grubu, Türkiye'yi ve dünyayı ilgilendiren bir çok faaliyette bulunarak, siber dünyada neler yapılabileceğini göstermiştir. 2005 yılında sisteme girerek İstanbul'daki bütün trafik cezalarını silmiştir. 2007 yılında MOBESE sistemine girerek deşifre etmiştir. 2008 yılının 2 Temmuz'unda Türkiye'deki bütün valiliklerin sitesine girerek, 2 Temmuz Sivas Katliamı ile ilgili yazılar yazmıştır. 2012'de Emniyetin %95'ini hackleyip, çok sayıda ihbar ve iç yazışmaları kamuoyu ile paylaşmıştır[29].

Nisan 2012'de İç İşleri Bakanlığının sitesini hackleyerek web sitesine mesaj bırakmıştır. 27 Nisan 2012 tarihinde TTNet internet servis sağlayıcısının 2 saat süreyle hizmetini aksatmıştır. Temmuz 2012'de Dış İşleri Bakanlığı'nın dosya paylaşım sitesinin hedef alınmıştır ve saldırı sonucunda Türkiye'de çalışan pek çok yabancı diplomatın kimlik bilgileri Dropbox adlı site üzerinden yayınlamıştır. 17 Temmuz 2012'de ÖSYM sitesini bir süreliğine çökertmiştir. 08 Ocak 2013

[28] Ulusal Kanal'ın Ezber Bozanlar isimli programında canlı yayına katılan redhack üyesinin açıklamaları, http://www.youtube.com/watch?v=WdIzEhpLJYE. Erişim 27/03/2013
[29] http://www.bagimsizsinema.org/portfolio/red/ Red Belgeseli, Erişim 28/03/2013

tarihinde YÖK'ün sitesini 2.kez hacklemiş ve ele geçirdiği yolsuzluk, haksızlık belgelerini yayınlamıştır. 23 Mart 2013 tarihinde İsrail gizli servisi MOSSAD'ın sitesini, başka bir hacker grubu olan Anonymous ile işbirliği halinde çökertme eylemi gerçekleştirmiştir[30]. Bazı saldırılarında Anonymous grubu ile birbirlerini desteklemiştir.

E- LulzSec

ABD'nin büyükelçiliklerince yapılan gizli yazışmalarının wikileaks sitesinde ifşa edilmesiyle, wikileaks sitesine DoS (servis dışı bırakma) saldırıları yapılmıştır. Wikileaks'e destek vermek isteyen Anonymous grubu ise Mastercard, Paypal, Visa ve çeşitli devlet kurumlarının sitelerine saldırı başlatmıştır. Anonymousun internette yaptığı protestoların hemen ardından LulzSec isimli hactivist grup ortaya çıkmıştır. LulzSec'te saldırılara desteğini, "Halk ya da tüketiciler aleyhine çalışmalar yaptığı" iddiasıyla şirketlerin ve ülkelerin önemli kurumlarının sitelerine saldırılar yaparak göstermiştir. 50 günlük faaliyetlerinin ardından kendilerini feshettiklerini duyurmuştur.

2011 yılında faaliyetlerini durduran grup, 2012 yılında LulzSec reborn olarak faaliyetlerine devam etmiştir. ABD ve İngiltere'de yüksek profilli hükümet ve özel sektör web sitelerini hedef almıştır. Genellikle saldırılarında DDoS siber silahını kullanmıştır.

Anonymous hactivist grubun bir dalı olarak bilinen LulzSec grubu Sony Pictures, MasterCard, PayPal, 20th Century Fox ve Nintendo gibi devlet ve özel sektör web sitelerine saldırıları ve özellikle Sony Playstation ağını hedef alan bu grup, 77 milyon kullanıcının bilgisini çaldığını duyurmasıyla tanınmaktadır. CIA'in web sitesine saldıran grup, siteyi kapatmıştır[31]. CIA'in web sitesini kapatma sorumluluğunu kabul eden grup lideri 24 yaşındaki Glen McEwen, Avutralya Federal Polisi tarafından 24 Nisan 2013 tarihinde yakalanarak tutuklanmıştır.

---

[30] RedHack, http://tr.wikipedia.org/wiki/RedHack Erişim, 25/04/2013

[31] http://www.reuters.com/article/2013/04/24/net-us-australia-lulzsec-arrest-idUSBRE93N02D20130424 Erişim, 24/04/2013

F- Suriye Elektronik Ordusu (SEA)

Suriye Elektronik Ordusu (SEA-Syrian Electronic Army) Mayıs 2011'de açtıkları web sitelerinde kendilerini, "Suriye'deki ayaklanmalar konusunda gerçeklerin çarptırılmasına sessiz kalamayan bir grup Suriyeli ateşli genç" olarak tanıtmıştır. Hactivist grup, sadece medya organlarını hedef almamıştır. Suriye'de yaşanan iç çatışmaları körükleyen, kasıtlı olarak insanlar arasında mezhep çatışması başlatarak nefreti yaymaya çalıştıklarını öne sürdüğü sosyal ağları da hedef almıştır.

SEA, Esad hükümeti yanlısı faaliyetlerde bulunmalarına rağmen, Esad hükümeti tarafından yönetilen resmi bir birlik değildir. Ancak bir televizyon konuşmasında Beşar Esad, "Sanal alemin gerçek ordusu" şeklindeki ifadesiyle, hactivist grubu desteklediğini ortaya koymuştur[32].

24 Nisan 2013 tarihinde Amerikan Associated Press haber ajansının twitter hesabından atılan "Beyaz Saray'da iki patlama oldu, Obama yaralandı." Tweeti ABD'de paniğe neden olmuştur. Çok kısa sürede 1.500 kişi tarafından paylaşılan tweet haberi Dow Jones Sanayi Endeksinin aniden 140 puan düşmesine neden olmuştur[33]. Haberin sahte olduğunun, Associated Press haber ajansının twitter hesabının hacklendiğinin anlaşılması üzerine Dow Jones Sanayi Endeksi yeniden yükselmiştir.

Associated Press haber ajansının hacklenmesi ve sahte haberin yayılması sanayi endeksinde maddi zarara neden olmuştur. Birkaç ay içinde Suriye karşıtı haber yapan BBC, NPR, CBS News gibi haber sitelerini, Columbia University ve İnsan Hakları İzleme Örgütünün web sitelerini hacklemiştir. Suriye Milli Takımının 2014 Dünya Kupası elemelerinden çıkarılmasına tepki olarak, FIFA

---

[32] Obama Yaralandı! http://www.iha.com.tr/obama-yaralandi-273797-haber Erişim, 24/04/2013

[33] Who is the Syrian Electronic Army? http://www.bbc.co.uk/news/world-middle-east-22287326 Erişim, 29/04/2013

Başkanı Sepp Blatter ile FIFA World Cup internet sitelerinin twitter hesaplarını hacklemiştir[34].

Hactivist grup, Suriye'de yaşanan insan hakları ihlalleriyle ilgili raporlarıyla dikkatleri üzerine çeken İnsan Hakları İzleme Örgütü (HRW-Human Rights Watch)'nün internet sitesi ve twitter hesabını hacklemiştir. HRW'nin internet sitesine "Syrian Electronic Army Was Here All Your reports are FALSE!! Stop Iying" şeklindeki tüm raporlarının yanlış olduğunu ve yalan söylemeyi bırakmalarını istedikleri mesajı bırakmıştır[35]. Mesaj tıklandığında ise Suriye Elektronik Ordusunun sitesine yönlendirilmektedir.

Suriye karşıtı haber ve eylemlere karşı tepkilerini haber sitelerini ve twitter hesaplarını hackleyerek ortaya koyan hactivist grup, Amerikan endeksinin düşüş ve yükselişi ile maddi zarara sebep olmuştur. 21 Mart 2013'te BBC'nin hava koşullarını bildiren haberlerini değiştirmiştir. BBC'nin 60.000 takipçisi sahte hava bildiriminden etkilenenler arasındadır.

G- Cyber-Warrior

Türk hactivist gruptur. Türk inanç ve ahlaki değerlerine saldıran web sitelerini hacklemesi ile tanınmıştır. Hacker grubu Gazze'ye yardım için çıkan ve İsrail'in uluslar arası sularda Mavi Marmara gemisine saldırısına tepki olarak İsrail'in birçok web sitesini çökertmiştir.

Grubun herhangi bir dernek, kurum, örgüt, parti, siyasal ya da ideolojik görüş ile bağı yoktur. Web siteleri bulunmaktadır. Gruba üye olmak isteyenlere, bilgi ve uzmanlık alanlarına göre organizasyonda görev verilir.

4 Temmuz 2003 tarihinde 11 Türk askerinin başına çuval geçirilmesi olayını protesto etmek için 1.500 Amerikan sitesini hacklemiştir. Hacklediği sitelere "BİR TÜRK AMERİCA'YA BEDELDİR 11 TÜRK İÇİN DÜNYAYI

---

[34] What is the Syrian Electronic Army? http://edition.cnn.com/2013/04/24/tech/syrian-electronic-army Erişim, 29/04/2013

[35] Suriye Elektronik Ordusu HRW'yu hack'ledi, http://www.hurriyet.com.tr/planet/22840596.asp Erişim, 29/04/2013

FETHEDERİZ" ve "Şimdilik 1.500 tane sitenizi topraklarımıza dahil ediyoruz İP/Cyber Warrior Team Akıncılar Grubu" şeklinde mesaj bırakmıştır[36]. (Cyber Warrior)

H- Ayyıldız Tim

Türkiye aleyhine yapılan saldırıları engellemeye çalışan ve Türkiye lehine saldırılar yapan hactivist gruptur. Türkiye'yi hedef alan ülke ve unsurları belirleyerek planlanan veya yapılacak olan herhangi bir saldırıya karşı cevap vermeyi görev edinmiştir.

Ülke kurumlarına, devlet adamlarına ve manevi değerlere yapılan saygısızlıkları, ülke bütünlüğüne yapılan bir saldırı olarak görüp, karşı saldırıya geçmektedir.

Diğer hactivist grupların aksine yönetiminde bulunan kişilerin kendisini ifşa etmesinden rahatsızlık duyulmamaktadır. Web siteleri bulunmaktadır. Web sitelerinde kendileri ve faaliyetleri hakkında bilgi vermekten çekinmeyen grup, yaptıkları eylemlerin yasa dışı olmadığını belirtmektedir. Anonymous'un, Telekomünikasyon İletişim Başkanlığı (TİB)'na yapmış olduğu saldırıya, karşı saldırı yaparak engellemiştir. Pentagon'un web sitesini 8 saat kapatmıştır. Bu saldırı DDoS saldırısı ile karşılaştırıldığında, daha fazla yetenek ve bilgi gerektiren bir eylemdir.[37] (Ayyıldız Tim, 2012)

I- Maddi Kazanç Saldırıları

Belirli bir düşünceye hizmet etmekten ziyade sistem açıklarından faydalanılarak maddi kazanç elde etmek için yapılan siber saldırılar da mevcuttur. Saldırılarda elde edilen verilerin kullanılması veya satılması ile internet mafyacılığı ortaya çıkmıştır. Bilinenden farklı olarak, iri gövdeli, eli silahlı kişiler yerine hackerlar da mafyaya çalışmaktadır. Şirketlerden ele geçirilen veriler tekrar şirketlere para karşılığında satılmaya çalışılmaktadır. Şirketler ve bankalar itibar

[36] http://www.cyber-warrior.org/Hacked/index.htm Erişim, 01/05/2013
[37] http://www.ayyildiz.org/portal/index_videolb/player.swf?url=video/ayyildiztim1d.flv&volume=100 Erişim, 01/05/2013

ve güven kaybetmemek adına saldırılara maruz kaldıklarını saklamaktadır. Kimi hackerlar ise büyük şirketlerin güvenlik açığını bulmanın ve güvenliği etkisiz hale getirmenin vermiş olduğu hazzın peşindedir. Güçlü olduğu düşünülen sistemleri alt etmekten duyulan heyecan, bu tür hackerlar için maddi kazanç sağlamaktan daha önemlidir.

Birçok büyük şirket siber saldırılara uğramaktadır. 100 milyon kullanıcıyı ilgilendiren Sony Playstation firmasının uğradığı saldırılar, müşterilerinin karşısında şirketi zor durumda bırakmıştır. Epsilon firmasına yapılan saldırıda milyonlarca müşterinin e-posta adresi çalınmıştır. Bu müşterilerin aynı zamanda Disney ve Dell gibi 100 kadar büyük şirketin müşterisi olması, saldırının çapını da büyütmüştür.

Hacker saldırılarında müşteri bilgileri çalınan büyük şirketlerin müşterileri zarara uğratılmıştır. Mayıs 2011'de Amerika'nın 3. Büyük bankası Citigroup, hacker saldırısına maruz kalmıştır. Müşterilerine ait 360.000 Amerika Citigroup kredi kartı bilgileri çalınmıştır. Citigroup günde ortalama 30 bin saldırı girişimi aldığını rapor etmiştir. Citigroup'un uğradığı saldırı nedeniyle çalınan kart bilgilerinin değerinin küresel karaborsada 5 milyar dolar olduğu düşünülmektedir[38]. (ASPAN & SOH, 2011)

Geçmiş zamanlarda olduğu gibi başına maske geçirip, bankaya giren ve silah doğrulttuğu veznedardan paraları torbaya koymasını isteyen hırsızlık olaylarına rastlanılmamaktadır. Artık siber ortama aktarılan bütün bilgiler de, siber ortam aracılığıyla hırsızlanmaktadır. Bankalardan çalınan müşteri kredi kartı bilgileri mafya tarafından alıcı bulmaktadır.

Bu tür siber saldırılar hackerlar için büyük bir kazanç kapısı olmuştur. Mafya için de bu tür kazanç kapıları cazip hale gelmiştir. Sony, Google, Lockheed Martin gibi daha birçok büyük şirket saldırılardan nasibini almıştır. 2010 yılında

[38]Citi says 360,000 accounts hacked in May cyber attack, http://www.reuters.com/article/2011/06/16/us-citigroup-hacking-idUSTRE75F17620110616 Maria ASPAN; Kelvin SOH, Erişim, 30/04/2013

İngiltere hükümeti günde ortalama 650 saldırıya uğramış, ABD ise 15.000 saldırıya uğramıştır[39]. (Bilimania)

Şirketleri hedef alan saldırılar ekonomik kayıplara sebep olmaktadır. Saldırıların arkasında bazen hevesli bir genç bazen daha koordineli çalışan hacker grupları, bazen de sanayi casusluğunu meslek edinen kişiler çıkmaktadır. Siber saldırılarda kullanılan teknikler zamanla geliştirilmiştir.

§ 5. SİBER SİLAHLAR

İlk çağlardan bu yana savaşmaktan vazgeçmeyen insanoğlu, teknolojik gelişmelerini de genellikle askeri alanda yapmış ve geliştirmiştir. Günümüzde siber ortama kayan savaş alanının silahları da değişmiştir. Siber ortama uygun silahlar üretilmektedir.

Siber ataklar sırasında karşı tarafı etkisiz bırakmak, zarar vermek ve veri çalmak için kullanılan siber ortam araçlarına siber silah denir[40].

Ülkelerin büyük bir bütçesi savunmaya ayrılmaktadır. Radarlara yakalanmayan bir bombardıman uçağının yaklaşık maliyeti 730 milyon dolar, avcı uçağının maliyeti 100 milyon dolar, Cruise füzesinin maliyeti 1 milyon dolar, bir hafif makineli tüfeğin en düşük fiyatı 1500 dolar ile ifade edilirken, siber ortamda kullanacağınız ürünler çok daha ucuzdur. Elde edilmesi daha kolaydır. İhtiyacınız olan bilgisayar ve yazılımdır. Bir bilgisayar ile tam teçhizatlı büyük bir ordunun verdiği zarardan daha fazla zarar verilebilir. Zarar verdiğiniz hedef sadece askeri sistemler değil, ülkenin her türlü alanıdır. Ülkelerin siber ortamla bütünleşmiş sistemleri, gelişmişliğin faydalarını sunmaktadır. Aynı zamanda siber ortamla bütünleşmek, siber tehditlere de açık olmaktır. Güçlü tarafınız, aslında en zayıf ve tehlikeye açık hale gelmektedir. Siber silahların tehdit ettiği alan ise ülkenin omurgasını oluşturmaktadır.

---

[39] Siber Saldırılar, İran, Elektrik Şebekeleri, http://www.bilimania.com/bilisim-teknolojileri/35-bilisim-teknolojileri/3117-siber-saldirilar-iran-elektrik-sebekeleri Erişim, 27/03/2013

[40] http://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-i.html Erişim, 24/05/2013

I- Siber Tehdit Unsurları

Ülkeler, şirketler korumak zorunda oldukları bilgilerini, sırlarını gizledikleri sürece güçlüdürler. Ancak bilgiler ve sırlar ortaya çıktığında savunma sistemi zayıflamış olacaktır. Zarar vermek daha kolay olacaktır.

A- Enformasyon ve İstihbarat

Bilgi hangi konuda ve ne sıklıkla kullanıldığı açısından toplumlar için önemlidir. Değişen dünya değerleri arasında bilgi ve bilginin korunmasının önemi kavranmıştır. Devletlerin birbirlerinin güçlü ve zayıf yönlerini bilmeleri bir üstünlüktür. Bunun için özelikle savunma ve saldırı sistemlerindeki sırlar, Ar-Ge birimlerinin uzun yılların çabası ve geniş bütçeli projelerle elde ettiği konw-how büyük önem taşımaktadır. Ulusal güvenliği tehlikeye sokacak tehditlerin tespiti ve yok edilmesi, saldırı güçleri hakkında bilgi toplanılması görevini istihbarat üstlenmektedir.

Devletler için bilgi, istihbaratın temel malzemesidir. Bilgi, korunduğu sürece değeri artmaktadır. Enformasyon, ham bilginin işlenmesi ve amaca uygun biçime getirilmesidir. Verilerin derlenmesi, analog ya da rakamsal sembollerin biçimlendirilmesi ve anlamlandırılmasıdır. Siber savaşta enformasyon, problem çözme veya karar verme amacı ile kullanılmaktadır.

Düşman devletler tarafından ülkenin güvenliğine ve çıkarlarına yönelik olarak düzenlenen her türlü gizli faaliyetler istihbarat kapsamında değerlendirilmektedir[41]. (ACAR & URHAL, 2007)

"Moğollar, aslında tarihin ilk enformasyon savaşçılarıydı…" bu yargıyı savunan ve "enformasyon savaşı" kavramını 1980'li yıllarda ilk ortaya atan, ABD askeri okullarında ders veren Jhon Arquilla'dır[42]. (HALICI, 2002)

Moğollar, düşmanı zayıf düşürmenin yolunun, düşmanı körleştirmekten geçtiğini keşfetmişlerdir. Düşmanı, istihbarattan yoksun bırakıp, adeta

[41] Ünal ACAR-Ömer URHAL, Devlet Güvenliği İstihbarat ve Terörizm, Ankara 2007, s.155
[42] Enformasyon Savaşı İçin Ağır Silahlanma, http://bianet.org/bianet/bianet/8406-enformasyon-savasi-icin-agir-silahlanma, Nihit HALICI, Erişim, 13/04/2013

körleştiriyorlardı. Tıpkı satranç oyunu gibi rakibin elindeki taşları görüyor fakat kendi taşlarını göstermiyorlardı.

Devletler ve şirketler arası rekabet büyüdükçe, istihbarat ihtiyacı arttı. Moğollar dönemindeki ulaklar artık yerlerini istihbari bilgi toplayan siber casuslara bıraktı.

Dünyanın farklı bölgelerinde artan terör olayları istihbaratın önemini ve güncel teknoloji ile güçlendirilmesi gerektiğini göstermiştir. İstihbarat faaliyetleri, hedef kişi veya grupların gözetim altında tutulmasını ve ülke çıkarları doğrultusunda ülkenin korunması görevini üstlenmiştir.

Dışarıdan gelebilecek dolaylı tehditler arasında yer alan casusluk, aynı zamanda, devlet güvenliğini tehdit eden eylem çeşitlerinden biridir. Devletlerin, diğer devletlere yönelik olarak, hedef alınan ülkenin siyasi, idari, askeri ve ekonomik alanlarda önemli değere sahip bilgilerini çalmaya yönelik çalışmalar yürüttükleri bilinmektedir[43]**.** (ACAR & URHAL, 2007)

B- Siber Casusluk Olayları

Siber saldırılar neticesinde ele geçirilen gizli bilgilerin ifşa edildiği siber casusluk olayları devletlerin ve şirketlerin siber güvenlik konusunda zayıf olduklarını ortaya koymuştur.

Casus yazılımlar gün geçtikçe artmaktadır. Farklı özellikleri geliştirilen casus yazılımlar, kendilerini saklayabilir, görünmez olabilirler. Bilgisayarlardan silindiği halde tekrar kopyalanabilir. Belirli bir süre var olup, daha sonra kendi kendini yok edebilir.

2003 yılında ABD'nin uğradığı titan rain saldırısında, NASA'dan, ABD askeri kurumlarından ve firmalarından bilgi çalınmıştır. Bu olay 1998 yılında yaşanan Ay Işı Labirenti operasyonunun benzeridir. Yapılan araştırmalar sonucunda titan rain saldırısının Çin kaynaklı olduğu anlaşılmıştır.

[43] Ünal ACAR-Ömer URHAL, Devlet Güvenliği İstihbarat ve Terörizm, Ankara 2007, s.155

Tibetlilerin bilgisayarlarında buldukları ve OpenNet Initiative (ONI) adlı kuruluşa başvurmalarıyla GhostNet isimli başka bir casus programa rastlanılmıştır. Kanada'nın Toronto üniversitesine bağlı Munc Centre for International Studies'te yapılan on aylık araştırma sonucunda programın, uluslararası bilgisayar casusluk programı olduğu ortaya çıkmıştır. 103 ülkede 1295 bilgisayarda faal olduğu anlaşılan casus programın Çin kaynaklı olduğu saptanmıştır.

McAfee güvenlik firmasının 2011 yılı içinde çıkardığı raporunda, Shady RAT operasyonu olarak tanımladığı, siber casusluk operasyonunda ülkelerin, uluslararası organizasyonların ve yıllardır uğraş veren ileri teknoloji firmalarının bilgilerine sızıp milyarlarca dolar değerindeki entelektüel mülkünün çalınmış olabileceği belirtilmiştir. McAfee'ye göre siber casusluk operasyonun arkasında bir devlet bulunmaktadır. McAfee göre, hackerlar, 2006 yılından beri geniş bir alanı kaplayan hedeflerden endüstri ile alakalı sırları içeren petabytelarca bilgi çalmıştır. Sınıflanmış devlet sırlarının, teknoloji firmalarından tasarım şemalarının, kaynak kodlarının ve doğal kaynaklarla enerji üreten firmalardan araştırma planlarının vs. çalındığı düşünülmektedir[44]. (ALPEROVİTCH, 2011)

Beş yıl süren saldırıların uzun kurban listesinde ABD, Tayvan, Hindistan, Güney Kore, Vietnam ve Kanada hükümetleri, Güneydoğu Asya Ülkeleri Birliği ASEAN, Uluslararası Olimpiyat Komitesi IOC, Dünya Anti-Doping Ajansı ile, savunmadan yüksek teknolojiye çok farklı sektörlerden çok sayıda şirket yer almaktadır.

McAfee'nin, Operation Aurora hakkında yaptığı saldırı açıklamasında başta Google ve en az 20 diğer şirketi giriş noktası olarak kullanıp, Operation Aurora adlı casus yazılım bu şirketlerden yararlanmıştır. Hedef kullanıcıların bilgisayar ağlarından uzaktaki sunucuya şirketlerin bilgileri çalınmıştır. Yine bir casusluk olayında kullanılan Night Dragon'da ise, ana petrol ve yakıt firmalarına ait entelektüel mülklerin yağmalanması hedeflenmiştir.

---

[44] http://www.mcafee.com/apps/search/default.aspx?q=Shady+RAT Erişim, 12/05/2013

C- Kritik Altyapılar

İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılardır[45]. Kritik altyapılar devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir[46].

Kritik alt yapılar için birçok tanım yapılmıştır. Dünyada yaşanan son virüs saldırılarında, bir ülkenin omurgası olan kritik alt yapılar hedeflenmiştir. Ülkelerin kritik altyapılarının hedef alınması ise daha büyük zararlara sebep olabilecek niteliktedir.

Kritik alt yapılar; savunma teknolojileri, kamu hizmetleri, sağlık servisleri, elektrik santralleri, telekomünikasyon alt yapıları, ulaşım, hava trafiği kontrol sistemleri, enerji üretim ve dağıtım sistemleri, finans servisleri, su üretim ve dağıtım şebekeleridir. Kritik alt yapılar ile internet arasındaki kontrol denetim bağı arttığından, internet üzerinden gelecek her türlü tehlike kritik alt yapıları etkileyecektir.

Bir çok siber savaş senaryolarında, kritik alt yapıların ele geçirilmesi, kilitlenmesi ve yönlendirilmesiyle ülkede oluşacak kaos gözler önüne getirilmeye çalışılmıştır. Şehrin elektrik şebekelerinin ele geçirilerek karanlığa bürünmesi, su şebekelerinin ele geçirilmesi, trafik ağının ele geçirilerek trafiğin felce uğratılması, telekomünikasyon ağının ele geçirilerek iletişimin durdurulması, telefonların çalışmaması, hastanelerde cihazların işlemez duruma getirilmesi, petrol boru hatlarının ele geçirilerek patlamalara sebep olunması, baraj kapaklarının açılması, karanlık gökyüzünde nereye gideceğini, nereye ineceğini

---

[45] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Ocak 2013

[46] http://www.bilgiguvenligi.gov.tr/siber-savunma/iki-kritik-kavram-kritik-altyapilar-ve-kritik-bilgi-altyapilari.html 24/04/2013

bilmeden uçan uçaklara sebep olunması gibi birçok tehlikenin aynı anda gerçekleştirilmesi bilim kurgu olmaktan çıkmıştır ve yapılması mümkündür.

D- SCADA ve APT

Denetleme Kontrol ve Veri Toplama (SCADA- Supervisory Control And Data Acquisition) sistemi geniş alana yayılmış üretim tesislerin bir merkezden bilgisayar aracılığı ile izlenmesi ve kontrol edilmesi olarak tanımlanmaktadır[47]. (EMRE, 2013)

Kritik altyapıların izlenmesi ve kontrol edilmesi de SCADA sistemleri tarafından yapılmaktadır. Bu sistemlerin büyük bir bölümü bilgi ve iletişim teknolojilerinden oluşmaktadır. SCADA sistemlerine saldırılması, felaketle sonuçlanabilir.

Siber ortama kayan savaşların, saldırı silahları da değişiklik göstermiştir. Belirli bir hedefe gizlice ilerleyen ve sistemi içten içe çökerten silahlar geliştirilmektedir. SCADA sistemlerini hedef alarak yazılmış olan Stuxnet, Duqu ve Flame yazılımlarının tespiti öncesinde, ne kadar zaman geçtiği bile tam olarak bilinmemektedir.

Gelişmiş Kalıcı Tehditler (APT-Advanced Persistent Threat), hedefi net olarak belirlenmiş, ileri seviyede ve uzun süreli tehditler içeren, siber savaşlarda kullanılmak üzere geliştirilmiş zararlı saldırı yazılımlarıdır. APT'ler genellikle devletlerin kritik altyapılarını hedeflemektedir.

APT'ler siber savunma sistemlerini kolaylıkla atlatabilir ve yayılabilir. Gelişmiş teknikler sayesinde hedef sisteme sızar ve bulaştığı sistemlerde uzun süre fark edilmeden çalışabilir. Sisteme kalıcı olarak yerleşir ve bilgi çalma, sistemi çökertme gibi hedeflerin yerine getirilmesini sağlar.

APT'lerin yayılması birçok şekilde olabilmektedir. Web siteleri, oltalama saldırıları, sıfırıncı gün saldırıları, Microsoft ofis ve Adobe PDF gibi ofis

[47] 5. Boyutta Savaş: Siber Savaşlar - II http://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html Bâkır EMRE, Erişim, 26/05/2013

programları ve USB, CD, DVD gibi donanım aygıtları aracılığıyla da yayılabilmektedir.

APT'lerin en temel özellikleri ise, ileri seviyede oldukları için, profesyonel kadro, kurumlar ve teknik imkânlar gerektirmesidir. Kalıcı ve yaşam sürelerinin uzun olabilmesi için de, geçerli sertifikalar ile imzalanma ve sıfırıncı gün açıklıkları ile yayılma gibi tespit edilmesini engelleyecek teknikler kullanılması gerekmektedir[48]. (HALTAŞ, 2011)

Uzun ömürlü yazılımlar, sıradan kişiler tarafından hazırlanamayacak kadar karmaşıktır. Farklı alanlarda uzmanlaşmış kişilerce kolektif bir çalışma gerektirmektedir, haliyle yazılımlar büyük bütçeler ayrılarak hazırlanmaktadır. Dolayısıyla devlet veya büyük şirketler tarafından desteklenmesi gerekmektedir.

E- Kritik Alt Yapıları Hedef Alan Siber Silahlar

2010 yılından itibaren tespit edilmeye başlanılan siber silahlar özellikle kritik alt yapıları hedef alarak geleneksel silahlardan daha çok zarar vermektedir. Ayrıca, siber silahların kimler tarafından yazılıp gönderildiği ise belirsizlik taşımaktadır. Bu durum ise düşmanınızı belirlemenizi olanaksız kılmaktadır.

1. Stuxnet

Özellikle SCADA sistemlerine saldırmak üzere yazılmış, bilinen ilk ve en karmaşık yazılımdır. 2010 yılının Haziran ayında Beyaz Rusya'daki küçük bir firma olan VirusBlokAda tarafından tespit edilmiştir. İncelemeler sonunda yazılımın karışık yapısı, basit bir solucan olmadığını göstermiştir. Farklı alanlarda uzmanların uzun zaman ve büyük bir bütçe harcayarak gerçekleştirilebileceği bir yazılım olduğu anlaşılmıştır.

Bu yazılımın en korkutucu tarafı ise Windows tabanlı bilgisayarlardan endüstriyel takım donanımlarının kontrolünde kullanılan özel bir sisteme atlamaya yönelik tasarlanmış olmasıdır. Hedefi kritik alt yapılardır.

---

[48] DUQU: Yeni Nesil Keşif Uçağı, http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/duqu-yeni-nesil-kesif-ucagi.html Fatih HALTAŞ, Erişim, 10/05/2013

2010 Kasım ayında İran'ın yüksek düzeyde güvenlikle korunan nükleer yakıt tesisinde tespit edilen virüs çok sayıda santrefüjün arızalanmasına sebep olmuştur. İran'ın uranyum zenginleştirme programına vurduğu darbe ile stuxnet asıl hedefinin ne olduğunu ortaya koymuştur.

İran nükleer tesisinden içeri girmeyi başaran stuxnet virüsü, yavaş ve emin adımlarla zarar vermeye başlamıştır. Santrefüjler uranyum zenginleştirmede kullanılan ve son derece hızlı dönen makinelerdir. Virüsün amacı, santrefüjlerin kontrolünde kullanılan Programlanabilir Mantık Denetleyicisi (PLC-Programmable Logic Controller) kontrol devrelerini hedef alarak kontrolü ele geçirmektir. Kontrolör yazılımı bozulmaya başlayınca hızla dönen makinelerin dönme hızı kontrolden çıkıp, makineler parçalanmaya başlamıştır. Sistemi ele geçirerek içten içe zarar veren virüsün korkunç tarafı ise merkez bilgisayarlarına her şeyi normal göstermesidir. Bu nedenle içten içe verilen zarar uzun zaman sonra anlaşılabilmiştir.

Parçalanan makinelerin yenilenmesi ve kalan makinelerin zararlı yazılımlardan temizlenmesi, yeniden yüklemelerinin yapılması, çalışmaları hayli aksatmıştır. Stuxnet virüsünün, İran'ın nükleer çalışmalarını 2 yıl geriye götürdüğü bilinmektedir. Dünya genelinde virüsün %60'ı aşan bir oranda İran'ı etkilemesi ise bu virüsün özellikle İran nükleer tesisini kontrol altına almak ve çökertmek için geliştirildiği düşüncesini arttırmıştır. Gerçek hedefi olan İran'daki Natanz uranyum zenginleştirme tesisine ulaşana kadar stuxnetin 100 binden fazla sisteme bulaştığı bilinmektedir.

Sistemi ele geçirme ve çökertme üzerine yazılmış virüsün, birçok kritik altyapıda kullanılan PLC devrelerini hedef olarak görmesi tüm dünyaya korku salmıştır.

2. Duqu

Stuxnetin tespitinden bir yıl sonra keşfedilen zararlı yazılımdır. Duqu virüsü, stuxnet virüsü ile büyük benzerlikler içermektedir. Stuxnet virüsünün yazarları tarafından yazılmış olabilir veya duqu virüsünü yazanlar, sutuxnet

virüsünün kaynak kodunu inceleme imkanı bulmuş olabilir[49]. Stuxnet ve duqu virüslerinin ortak özelliği, endüstriyel kontrol sistemlerini hedef almalarıdır. Ayrıca ikisi de geçerli sertifikalar kullanmaktadır, sıfırıncı gün açıklıkları ile yayılmaktadır ve İran'da görülmüştür[50].

İki virüs arasında farklar mevcuttur. Stuxnetin, hedefi sistemlere zarar vermektir, yıkıcı bir etkisi vardır. Dugu ise, SCADA sistemleri ile ilgili kritik bilgileri toplamak için tasarlanmıştır. Stuxnet saldırıları gibi, sisteme zarar verme saldırıları öncesinde istihbarat sağlamak amacıyla, saldırının daha etkin çalışması için tasarlanmıştır. Virüs, eriştiği sistemden 36 gün sonra kendisini silmektedir. Duqu, geleceğe yönelik büyük tehlikelerin sinyallerini vermektedir. SCADA sistemleri ile ilgili kritik bilgilerin tespiti, saldırı yapacağınız sistemin zayıf ve güçlü yönlerini ele geçirmektir. Bu da, stuxnet benzeri saldırı silahlarının oluşturulması demektir.

3. Flame

Virüs 2012 yılında keşfedilmiştir. Stuxnet virüsünden 20 kat daha karmaşık bir kodla yazılan ve özellikle Orta Doğu'yu hedef alan Flame virüsü veri sızdırma amacı taşımaktadır. Flame'de diğer virüsler gibi uzunca bir süre keşfedilememiştir. Etkilediği bilgisayarlardan yıllarca veri sızdırmış ve casusluk faaliyetlerini sürdürmüştür.

Budapeşte CrySyS Lab (Kriptografi ve Sistem Güvenliği Laboratuvarı) tarafından yapılan ön rapora göre flame virüsü, bilginin sızdırılabilmesi için klavye, monitör, mikrofon, depolama cihazları, Wi-Fi, Bluetooth, USB gibi her türlü donanımı ve sistem işlemcilerini kapsamaktadır. Ayrıca, Flame virüsünün arkasında bulunan kişiler, virüsü yönlendirmek için komuta ve kontrolü çok sık değişen bir ağ kullanmaktadır, böylece dinleme cihazlarının mikrofonlarını aktif

[49] W32.Duqu: The Precursor to the Next Stuxnet, http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet Erişimi, 13/05/2013

[50] http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/duqu-yeni-nesil-kesif-ucagi.html Erişim, 13/05/2013

hale getirmek veya belli hedeflerden tüm belge ile şifreleri çalabilmektedir[51]. (Budapest University of Technology and Economics Department of Telecommunications, Laboratory of Cryptography and System Security, 2012)

Kaspersky Laboratuvarlarında yapılan incelemelerde İran, Flame'in tespit edildiği ülkeler içerisinde en çok etkilenen alan olarak görülmektedir. İran'dan sonra İsrail, Batı Şeria, Sudan, Suriye, Lübnan, Suudi Arabistan ve Mısır virüsten etkilenen bölgeler arasındadır. Flame'in etkilediği bilgisayar sayısı 1000'in üzerindedir.

4. Gauss

Ortadoğu virüslerin hedefi haline gelmiştir. Ortadoğu'yu hedef alan ve etkileyen başka bir virüste Haziran 2012'de keşfedilen Gauss virüsüdür. Kaspersky Laboratuvarlarında Flame virüsünün ayrıntılı analiz ve araştırmaları sonucunda keşfedilmiştir[52]. Kaspersky'nin araştırmaları sonucunda Flame ve Gauss virüsleri arasında önemli benzerlikler ve bağıntılar bulunmuştur. Çevrimiçi bankacılık hesaplarını izlemek üzere tasarlanmış siber tehdittir. Virüs etkilediği bilgisayarlardaki tarayıcı parolalarını, çevrimiçi bankacılık hesap kimlik bilgilerini ve hassas verileri çalmak için tasarlanmıştır.

Diğer yazılımlar gibi Ortadoğu'yu hedefleyen Gauss diğer yazılımlardan farklı olarak bankaları etkilemektedir. Virüs Lübnan, İsrail ve Filistin topraklarında 2500'den fazla bilgisayara bulaşmıştır.

5. Tinba

1 Haziran 2012'de Danimarka CSIS Güvenlik Laboratuvarı tarafından tespit edilmiştir. Trendmicro güvenlik firması tarafından 12 Eylül 2012 tarihinde tinba virüsünün analiz raporunu yayınlanmıştır[53].

---

[51] sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks, http://www.crysys.hu/skywiper/skywiper.pdf Erişim, 13/05/2013

[52] Gaus Nedir? http://www.kaspersky.com.tr/gauss Erişim, 13/05/2013

[53] http://www.trendmicro.com.tr/guvenlik-istihbarati/arastirma/index.html#aratrma-belgeleri Erişim, 13/05/2013

Rapora göre, özellikle Türkiye için özelleşmiş olan ve Türkiye üzerinde aktif olan zararlı bir yazılımdır. Türkiye'de Tinba virüsünden etkilenen 60.000'den fazla kullanıcı bulunmaktadır. Tinba veri çalmak için geliştirilmiştir. İnternet tarayıcılarından kanca atma yöntemiyle oturum açma bilgilerini toplayabilmektedir. Ayrıca ağ trafiğini dinleme özelliği de mevcuttur. Bunların yanı sıra araya girme saldırıları ve belli web sayfalarının görünümünü değiştirme yöntemleriyle iki aşamalı yetkilendirmeyi aşabilme yeteneğine sahiptir. (CSIS Security Group A/S and Trend Micro Incorporated , 2012)

Tinba konusunda TÜBİTAK-BİLGEM tarafından Türkiye'deki kullanıcılar uyarılmış ve zararlı yazılımdan kurtulmak için bilgi verilmiştir.

6. Shamoon Virüsü

Suudi Arabistan'ın ulusal petrol şirketi Aramco'ya 15 Ağustos 2012 tarihinde yapılan siber saldırıda birkaç saat içinde 30.000 bilgisayar hasar görmüş ve kullanılamaz hale getirilmiştir. Saldırıyı, kendilerini "Adaletin Keskin Kılıcı" olarak adlandıran hacker grubu üstlenmiştir[54]. (STEWART & COONEY, 2012)

Enerji sektörünü hedef alan virüs, bulaştığı sistemlere zarar vermek ve bilgisayarları kullanılamaz hale getirmeyi hedeflenmiştir.

Özellikle Suriye, Bahreyn, Yemen, Lübnan, Mısır gibi komşu ülkelerde işlenen suçlardan ve zulümden bıkmış olan anti-baskı hacker grubu olduklarını, bu felaketlerin en önemli destekçilerinden biri, Müslümanların petrol kaynaklarını kullanarak bu tür baskıcı önlemlere sponsor olduğunu düşündükleri Al-Saud rejimine karşı, uyarı niteliğinde olduğunu pastebin web sitesinde bildirmişlerdir[55]. (PASTEBIN, 2012)

[54]"Shamoon" virus most destructive yet for private sector, Panetta says, http://www.reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012 Erişim, 08/05/2013

[55] http://pastebin.com/HqAgaQRj Erişim, 09/05/2013

Anti-virüs şirketleri ve araştırmacılar virüsün hedefinde petrol endüstrisinin olabileceğini, saldırılara ve virüslere özenen çocuklar tarafından yapılan taklitçi bir saldırı olduğunu düşünmektedir[56].

Özenti bir hareket dahi olsa seslerini duyurmaya çalışan grup, yapmış oldukları saldırı ile petrol şirketine ekonomik zarar vermiştir.

7. DDoS Saldırıları

DDoS (Distrubuted Denial of Service), en basit saldırı tipi olduğundan yoğun olarak kullanılmaktadır. Saldırının amacı, sistemi durdurarak prestij ve maddi kayıp sağlamaktır. Hactivist grupların genellikle kullandıkları saldırı silahıdır. Siber savaşın silahları içinde en müthişi olmayabilir ancak rahatsız edici ve maddi zararlara yol açan bir unsurdur. Nitekim Rusya'nın Estonya ve Gürcistan'a yaptığı siber saldırının da temel silahıdır.

Kritik alt yapıları hedef alan bir saldırı tipi değildir. Fakat bankalara yapılan saldırılar sonucunda bankaların hizmet dışı kalması, bankamatiklerden para dahi çekilememesi hafife alınacak bir sorun değildir. Saldırının uzun süreli olması halinde ortaya çıkarmış olduğu sorunlar da büyük olmaktadır.

Dağınık servis engelleme ile ağlara saldırılarak çökmelerine veya trafik sıkışıklığına neden olunur. Dağınık olması saldırının yüz binlerce bilgisayar üzerinden yapılmasındandır. Saldırıda kullanılan yüz binlerce bilgisayara "botnet" adı verilmektedir. İnternet aracılığıyla botnetler üzerinden, hedefe saldırılar yönlendirilir. Botnet bir robot ağdır ve uzaktan kumanda ile çalıştırılan zombi bilgisayarlardan oluşur. Sahibinin haberi bile olmaksızın zombi bilgisayarlar gönderilen direktifleri takip eder. Bilgisayar sahipleri, bilgisayarlarının ne zaman zombi olduğunun veya DDoS saldırısı yaptığının farkında bile değildir. Ekranında hiçbir belirti görünmemektedir, her şey arka planda gerçekleşmektedir. Belki bilgisayar biraz daha yavaş çalışır veya bazı web sitelerine girişte yavaşlama fark edilebilir.

[56] http://www.infosecurity-magazine.com/view/27661/disttrackshamoon-a-new-targeted-and-destructive-virus/ Erişim, 08/05/2013

Herhangi bir web sitesini açmakla virüs bilgisayara gizlici yüklenebilir ve bilgisayar bir zombiye dönüşebilir. Bazen de virüsler e-posta aracılığıyla gelebilir, tanınan kişilerden gelen e-postalar dahi virüs taşıyabilir ve e-posta açıldığı anda virüs mevcut bilgisayara yüklenir. Bazen virüs durur ve emir bekler, bazen ise saldıracak başka bilgisayarlar arar. Bilgisayardan bilgisayara solucan gibi atlar. Böylece saatler içinde bulaşıcı virüs yüz binlerce hatta milyonlarca bilgisayarı etkisi altına alabilir. Böylece DDoS saldırıları için dev bir bilgisayar ordusu kurulmuş olacaktır. Bilgisayar sahipleri, bilgisayarının bir ordu neferi olduğunun farkına bile varmayacaktır.

En sık kullanılan DDoS saldırı çeşitleri; SYN Flood, UDP Flood, HTTP Flood, DNS Flood'dur. DDoS bir altyapı problemidir. Fiziksel altyapının güçlü olması, saldırılara karşı alınabilecek bir güvenlik önlemidir. Sürekli güncellenen anti virüs ve firewall yazılımları da zombi virüslerini bloke edebilir fakat hackerlar da sürekli yenilerini geliştirmektedir.

Firewall, DDoS saldırıları karşısında savunmasız kalmaktadır. Firewall'ın state tablosuna yazılan her oturum Firewall kurallarına göre ayrı değerlendirilir, saldırı yapan kişiler oturumları hiç kapatmayarak state tablosundan silinmeden istedikleri gibi geçebilmektedir.

Kanlı savaşların ardından, sessiz ve sinsice yaralayan siber silahlar daha masum gibi görünebilir. Ancak siber silahlar, dolaylı yoldan da olsa aynı etkiyi gösterecektir. Savaş daha sessiz bir hal almaktadır. Siber savaşların, insan hayatının devamını güçleştiren ve yaşamları tehlikeye atan etkileri bulunmaktadır.

§ 6. SİBER SAVAŞ

Siber savaşlar, 5.boyut savaşları olarak da tabir edilmektedir. İnsanoğlunun kara, hava, deniz ve uzaydan sonra 5. savaş alanı olarak belirlenmiştir. Siber savaş, düşmanı psikolojik olarak çökertmek için bilgisayar kontrolü altındaki sistemlerine izinsiz, gizli ve görünmez olarak internet üzerinden erişmektir[57]. Kontrolü ele geçirerek bilgileri çalmak, değiştirmek, çökertmek ya

[57] Kritik Alt Yapılara Siber Saldırı, http://ylt44.com/bilimsel/siber.html Cahit KARAKUŞ, İstanbul Kültür Üniversitesi, Erişim, 24/03/2013

da yanlış yönlendirmektir. Bir devletin başka bir devletin bilgisayar sistemlerine ve ağlarına sızarak hasar veya kesinti yaratmak üzere hareket etmesidir[58].

Siber savaş, kendi içinde birçok yöntem ve teknik barındırmaktadır. Siber savaş meydanında kullanılabilecek çalışma alanları vardır. Casusluk, manipülasyon, propaganda, iletişimin kontrol altına alınması, virüs ve Truva atlarıyla sistemlerin bozulması, siber bombalarla sabotaj, sistem kilitleme, dolandırıcılık, bilgi kirliliği gibi bir çok alan siber savaşın oluşumuna katkı sağlamaktadır.

I- Siber Ortamın Savaşlara Etkileri

İnternetin ortaya çıkması, bilişim sistemlerinin kullanılması, e- devlet ve e-ticaret gibi elektronik ortam hizmetlerinden faydalanılması birçok tehlikeyi de beraberinde getirerek, ülkeler arasındaki gerginliklerde saldırı malzemesi olmuştur.

A- Sibirya Doğalgaz Patlaması-1982

1982 yılında Sibirya'da yaşanan patlama, tarihte siber teknoloji kullanılarak gerçekleştirilen ilk siber saldırıdır. Saldırı sonucunda Sibirya doğal gaz boru hattında yaşanan patlama ise nükleer olmayan en büyük patlamadır.

Soğuk savaş sırasında Sovyetler Birliği ve ABD arasında casusluk faaliyetlerinin yürütüldüğü bilinmektedir. Ruslar 1982 yılında Kanada da bir şirketten doğal gaz boru hatlarını kontrol etmek için kullanılan bir yazılımı çalmaya başlamıştır. Rusların Kanada'dan gizlice çaldıkları, aslında CIA tuzağı ile çaldık zannettikleri virüslü bir yazılımdır[59]. ABD yazılımın içine Truva atı virüsü yüklemiştir[60].

---

[58] Richard A. Clarke, Robert K. Kanke, Siber Savaş (Cyber War), (çeviren:Murat Erduran) İstanbul Kültür Üniversitesi, Basım 2011, s.8

[59] Siber Saldırılar, İran, Elektrik Şebekeleri http://www.bilimania.com/bilisim-teknolojileri/35-bilisim-teknolojileri/3117-siber-saldirilar-iran-elektrik-sebekeleri Erişim, 27/03/2013

[60] Old Trick Threatens the Newest Weapons, http://www.nytimes.com/2009/10/27/science/27trojan.html?_r=2&ref=science&pagewanted=all& John Markoff, Erişim, 30/04/2013

ABD, Rusların yazılımı çalmaya başladıklarını fark etmiştir. Ancak operasyonu durdurmak yerine yazılımın içine virüs yerleştirmeyi tercih etmiştir. Rusların çaldığı yazılım bir süre sonra bozulmuş, boru hatlarındaki akışı anormal seviyelere çıkartmış ve borunun patlamasına sebep olmuştur[61]. (KARAKUŞ)

Casusluk faaliyetlerinin alan değiştirmesi gerektiğini gösteren ilk siber saldırı örneği can kaybına neden olmadan ancak birçok maddi zarara yol açarak boyutunu gözler önüne sermiştir.

B- Irak-1990

1990 yılında Körfez Savaşı için ABD siber savaşçıları ve özel operasyon komandoları bir araya gelerek, Irak'ın geniş hava savunma radar ve füze ağlarını nasıl imha edeceklerini incelemekle işe başlamıştır. General Norman Schwarzkopf, Bağdat'taki kurmay başkanlıkları ya da askeri birliklerin yerine hava savunma radar ve füze üssünün öncelikle imha edilmesi gerektiğini, böylece havadan gelecek tehlikeye karşı savunma sistemi kırılan Irak'ı, bombalamanın daha kolay olacağını düşünmüştür. Bu nedenle ilk saldırılar hava savunma radar ve füze üslerine karşı yapılmıştır.

Savaşa kadar dünyanın 5. büyük kara ordusuna sahip Irak, hava ve kara koordinasyonu konusunda zayıf kaldığından ve hava üstünlüğü ABD'de olduğundan ağır darbe almıştır.

ABD Ordu İstihbarat birimi telsiz frekansı tespit donanımlarıyla yüklü helikopterleri Irak sınırının güvenli kısmındaki stratejik noktalara göndermiştir. Irak ordusunun iletişim sistemleri üzerinde çalışarak, telsiz frekans sistemlerini tespit etmiştir. Operasyon başladığından itibaren Irak iletişim sistemi gizlici dinlenmiştir. Hatta dinlemek ile kalmayıp, bir müddet sonra iletişime geçilmiştir. Irak ordusu kendi birimlerine telsizle talimat veremeyeceğini anlayınca, yedek frekans listesi üzerinde değişiklik yapmaya başlamıştır. Ancak ABD Ordu helikopterleri içindeki donanımlar, yeni frekansları da tespit etmiştir. Irak ordusu

[61] Kritik Alt Yapılara Siber Saldırı, http://ylt44.com/bilimsel/siber.html Cahit KARAKUŞ, İstanbul Kültür Üniversitesi, Erişim, 24/03/2013

birlikleriyle telsiz iletişimi yapmaktan vazgeçerek, gömülü telefon hatlarına dönmüştür. Eski temel seri telefon hatlarından herhangi birine şifreli vericilerle girip tüm bilgileri ordu istihbaratına göndermeye çalışmıştır. Ancak ABD ordusu, telsiz iletişimini kesmekte kullandığı yöntemi yine kullanmıştır. Irak ordusu son çare olarak talimatları yazarak göndermeye çalışmıştır. En ufak bir talimatı bile arazideki komutanlara kamyonlarla gönderip cevapları kamyonlarla almaya çalışmışlardır. Birden fazla birime bu şekilde talimatların gidip gelmesi ve aynı anda hareket edilmesi zorlaşmıştır. Ayrıca ABD ordusu talimatları taşıyan kamyonları hedef almaya ve devre dışı bırakmaya başlayınca, Iraklı şoförler mesaj taşımayı reddetmeye başlamıştır. Arazi komutanları merkezden emir alsa bile dinlenildikleri için cevap verdikleri taktirde bulundukları yerin tespit edilebileceği düşüncesiyle cevap vermemeye başlamıştır. Hatta cihazları kapatmışlardır. İletişimin ele geçirilmesiyle Irak komuta kontrol sistemi tamamen yıkılmıştır[62]. (MİTNİCK & SIMON, 2013)

Irak Savaşı, savaşların geleneksel yöntemler yerine, siber ortam yetenekleri ile yürütülebileceğini, ordunun kalabalık olmasının önemli olmadığını, önemli olanın siber ortam güvenliğinin sağlanması gerektiğini, savaşta siber ortamın ele geçirilmesi durumunda, kimsenin burnunun kanamasına bile gerek kalmadan savaşa galip gelinebileceği ihtimalini gösteren, ilk büyük savaştır.

C- Ay Işığı Labirenti-1998

Moonlight moze operasyonu olarak bilinen ve Mart 1998'de başlayan operasyon ile ABD'nin Pentagon, NASA, ABD Enerji Bakanlığı ve üniversitelere ait araştırma ve geliştirme sırları, askeri tesislerin haritaları, askeri yapılandırmaları ve askeri donanım tasarımlarını içeren birçok gizli bilgi çalınmıştır.

Rus hackerlar tarafından bilgilerin çalındığı düşünülmektedir. Çalınan bilginin değeri açık artırmaya çıkarttığınızda yüz milyonlarca dolarla ifade

[62] Kevin D. Mitnick, William L. Simon, Sızma Sanatı, (çeviren:Emel Aslan), 1.baskı, Ankara 2013, s.288, s.289

edilebilecek büyüklüktedir. ABD'nin yapmış olduğu teknik takip sonucu bilgilerin Moskova'ya sevk edildiği tespit edilmiştir[63]. Ancak Rusya, konu ile bir ilgisinin olmadığını belirtmiştir.

İnternet üzerinden yapılan sızmalarla kritik alt yapı bilgileri devlet sırları bazen rotasını bilmeden hacking yapan ve ne bulursam kârdır düşüncesinde olan hackerlar için kazanç kapısı olabilmektedir.

D- NATO Kosova Krizi -1999

Dağılma sürecine giren Yugoslavya Federal Cumhuriyeti ordusunun, bağımsızlık isteyen Kosova Kurtuluş Ordusuna karşı sürdürdüğü operasyonlara NATO müdahale etmiştir. NATO, 30 Ocak 1999 tarihinde yaptığı basın açıklamasında Yugoslaya'daki hedeflere hava saldırı yapma yetkisinin Genel Sekreterde olduğunu belirtmiştir[64].

NATO Genel sekreterinin direktifi ile Sırp hedefler bombalanmaya başlanmıştır. Ancak bombalamaya karşılık NATO karargâhına ve üye ülke askeri haberleşme sistemlerine yönelik siber saldırılar başlanmıştır. NATO'ya yapılan saldırıda siber silah olarak DDoS ve binlerce zararlı bilgisayar virüsünü içeren e-postalar kullanılmıştır. Saldırılar incelendiğinde Sırpların yanı sıra Çinli ve Rus hackerlarında saldırılara destek verdikleri anlaşılmıştır[65]. NATO'nun resmi web sitesi sık sık kesintiye uğramış, NATO'nu e-posta hesabı günlerce kapalı kalmıştır.

Saldırılar yakından incelendiğinde bazı sitelere hackerlar tarafından "Çok Yaşa Büyük Sırbistan" ve "Kara El (Black Hand) bu siteye el koydu" benzeri mesajlar bırakılmıştır[66].

---

[63] Testımony of James Adams Chıef Eexecutıve Officer Infrastructure Defense,INC. Commıttee On Governmental Affaırs Unıted States Senate March 2, 2000 http://www.fas.org/irp/congress/2000_hr/030200_adams.htm Erişim, 30/04/2013

[64] Statement by the North Atlantic Council on Kosovo, http://www.nato.int/docu/pr/1999/p99-012e.htm Erişim, 30/04/2013

[65] Salih BIÇAKCI, Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu, Uluslararası İlişkiler, Cilt 9, Sayı 34 (Yaz 2012), s. 210-211.

[66] Sci/Tech Net warfare over Kosovo, http://news.bbc.co.uk/2/hi/science/nature/200069.stm Erişim, 30/04/2013

NATO, saldırılara karşı koyabilmek için kullanmış olduğu Sun Microsystem'in SPARC-20 sunucularının yerine daha hızlı veri işleme gücü olan Ultra-SPARC'larla değiştirmiş, Pingler tarafından doldurulan bant genişliğinin de seviyesini yükseltmiştir[67]. (BIÇAKCI, 2012)

Uluslar arası platformda medet umulan NATO'nun kendisi bir saldırının esiri olmuştur. Aşağıda açıklanacağı gibi NATO, bu saldırı sonrasında bir dizi önlemler almıştır. NATO'ya yapılan saldırıda, web sitelerine bırakılan mesajlar saldırganların kim olduklarını ve olayın evveliyatına bakıldığında ise neden bu saldırıyı yaptıklarını açıkça göstermektedir.

E- Irak -2003

2003 yılında ABD, Irak'ı 2. Kez işgal etmeyi planlarken, Pentagon tarafından hazırlanan bir mesaj binlerce Irak subayına Irak Savunma Bakanlığı e-posta sistemi üzerinden iletildi. Aşağıda yer alan mesaj Irak birliklerinin hiç savaşa girmeden teslim olmaları için bir çağrıydı.

"Bu ABD Genelkurmayından size gönderilen bir mesajdır. Bildiğiniz üzere, yakın bir gelecekte Irak'ı işgal edeceğiz. Birkaç yıl önce yaptığımız gibi, sizi tamamen imha edecek bir güçle bunu gerçekleştireceğiz. Size veya askerlerinize zarar vermek istemiyoruz. Amacımız Saddam'ı ve iki oğlunu devirmek. Zarar görmek istemiyorsanız, tanklarınızı ve zırhlı araçlarınızı sıraya dizerek terk edin. Yürüyün, gidin, kendinizi kurtarın. Siz ve askerleriniz evlerinize dönün. Bağdat'ta gerekli rejim değişikliği yapıldıktan sonra siz ve başka Irak birlikleri yeniden göreve çağırılacaktır[68]."

Iraklı subaylara ABD Genelkurmayı CENTROM tarafından Irak ordusunun gizli ağı üzerinden gönderilen ve subayların hiç savaşa girmeden teslim olmalarını teşvik eden bu mesaj amacına ulaşmıştır. Birçok subay bu talimata itaat etmiştir. Bazı Iraklı komutanlar savaştan birkaç saat önce askerlerine

[67] Salih BIÇAKCI, Uluslararası İlişkiler, Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu, Cilt 9, Sayı 34 (Yaz 2012), s. 210-211.
[68] Richard A. Clarke, Robert K. Kanke, Siber Savaş (Cyber War), (çeviren:Murat Erduran) İstanbul Kültür Üniversitesi, Basım 2011, s.8

izin vermiş ve askerlerini evlerine göndermiştir. ABD, Irak'ı bombalamaya başladığında, karşı taarruza geçmiş bir ordu değil, karargah önlerine düzenli bir şekilde park edilmiş tanklarla karşılaşmıştır.

ABD, Irak ordusunu konvansiyonel saldırı öncesinde, hackerların Irak savunmasının gizli ağına girerek göndermiş olduğu mesajla subayları psikolojik olarak çökertmiştir. Eski usul kağıt broşür atma yöntemi yerini e-posta ve başka internet malzemelerine bırakmıştır. Siber savaşın yöntem ve etkisiyle propaganda göndererek düşmanın morali bozulmuştur.

F- Suriye-İsrail Gerginliği -2007

Suriye'nin Kuzey Kore işbirliğiyle yapmakta olduğu nükleer tesis 6 Eylül 2007 tarihinde İsrail tarafından bombalanmıştır. İnşaat halindeki tesis, Türkiye sınırından 75 km içeride yer almaktaydı. Suriye patlama sonrasında derin bir sessizliğe bürünmüştür. Dünya medyasının patlamayı yazan haberleri üzerine, Suriye Devlet Başkanı Hafız Esat patlamayı kabul etmiştir. Ancak bombalanan binanın boş olduğunu belirtmiştir.

Suriye'yi şaşkına çeviren ise, havadan gelen saldırının Suriye hava radar ekranlarında görünmemesidir. Gökyüzünde uçaklar bombalama yaparken, hava radar ekranında hiçbir değişiklik olmamıştır.

Bu konuda ihtimaler üzerinde durulmaktadır. Richard A. Clarke kitabında ihtimaller üzerinde durmuştur. İhtimaller, bilişim sistemlerinin ele geçirilmesi noktasında birleşmektedir. Birinci ihtimalde, İsrail, Suriye hava savunmasının üzerine insansız heron uçağı göndermiştir. Basit bir anlatımla, radarlardan gönderilen ışın gökyüzündeki nesneye çarpar, nesneden geri yansıyarak alıcı radar sistemine döner ve çarpılan nesnenin hangi irtifada uçmakta olduğunu, ne hızla hareket ettiğini ve büyüklüğünü belirlemektedir. Yansıyarak dönen radar elektronik ışını, açık bir bilgisayar kapısı bulunan radar sistemine gökyüzündeki nesneyi bildirir. Ancak arıza nedeniyle heron uçağını görmemiş olabilir veya gördüğü uçağın bilgisi açık kapıdan girerken değişmiştir. İkinci bir ihtimalde, Rus yapımı bilgisayar programı ile çalışan Suriye hava savunma ağının, bilgisayar

programı içine yerleştirilmiş olan truva atı virüsüdür. Heron uçağının gönderdiği sinyalle Suriye bilgisayar sisteminin ele geçirilmesi ve yetkinin elinden alınmış olmasıdır. Üçüncü ihtimal ise İsrail ajanlarının Suriye içine girip, fiber optik kabloları keserek kendi kablolarını yerleştirmesi ve sistem on-line olduktan sonra da tuzak kapısının açılmasıdır[69]. (CLARKE & KNAKE, 2011)

BM'nin Uluslararası Atom Enerjisi Kurumu (IAEA- International Atomic Energy Agency) olay yerinden aldığı toprak örneklerinde tesisin, büyük ihtimalle nükleer reaktör olduğu sonucuna varmıştır[70]. (BBC, 2011)

İsrail'in, Suriye nükleer tesis inşaatını patlatması 2010 yılında ifşa edilen wikileaks belgelerinde de yer almıştır. İsrail'deki basın sansürü dış kaynaklı yazılardan alıntı yapılmasını engellemedi, ancak İsrail gazetelerinin halen patlama ile ilgili haber yazması yasaktır. Patlama olayı konusunda sessizliğini bozmayan İsrail, patlamanın sorumlusu olduğunu da inkâr etmemiştir.

Suriye, gizlice nükleer tesis inşasına başlayarak Birleşmiş Milletlerin'in hedef ve ilkeleri uyarınca IAEA'nın denetim gerekliliğini ihlal etmiştir. Bu nedenle olay sonrasında sessizliğini koruyan Suriye, hava saldırısı sırasında hava radar ekranlarının hiçbir sinyal vermemesinin şaşkınlığı ile ilk iş olarak cihazları aldığı Rusya'yı aramıştır. İsrail, nükleer tesisin tespitinde nasıl bir istihbarat yürüttüğü ve saldırıyı nasıl yaptığı konusunda hiç açıklama yapmamıştır.

G- Estonya Siber Savaşı – 2007

2. Dünya Savaşından sonra Sovyetler Birliği, Estonya'yı Nazi işgalinden kurtarmıştır. Sovyetler Birliğinin 1989 yılında dağılması ile Estonya tekrar bağımsız bir devlet olmuştur. Estonyalıların çoğunluğunun, Sovyetler Birliğinin baskıcı 50 yılını hatırlatan bronz kızıl ordu askeri heykelini kaldırmak istemesi

---

[69] Richard A. Clarke, Robert K. Kanke, Siber Savaş (Cyber War), (çeviren:Murat Erduran) İstanbul Kültür Üniversitesi, Basım 2011, s.9, s.10

[70] Suriye'deki tesis muhtemelen nükleer reaktördü, http://www.bbc.co.uk/turkce/haberler/2011/05/110524_syria_nuclear.shtml Erişim, 27/04/2013

üzerine "Bronz Gecesi" denilen 26 Nisan 2007 tarihinde Estonyada yaşayan etnik Ruslar ve Estonyalılar arasında yaşanan gerginlik büyümüştür.

İnternete dayalı çalışma sistemi, Estonya'yı siber hedef haline getirmiştir. Bronz Gecesi'nden sonra en çok kullanılan internet siteleri çökmeye başlamıştır. Estonyaya yapılan saldırı DDoS saldırısıydı. On binlerce zombi bilgisayar tarafından Estonya siber saldırının esiri olmuştur.

Siber saldırıya maruz kalan Estonya'da 27-29 Nisan tarihleri arasında devletin internet sayfaları, gazetelerin web siteleri kullanılamaz hale gelmiştir[71]. 30 Nisan-18 Mayıs tarihleri arasında ise saldırılar hedefini daha organize hale getirmiştir. Ulusal bilgi sistemleri, internet hizmet sağlayıcıları büyük zararlar görmüştür. Ülkenin en büyük bankası Hansabank tamamen etkisiz hale getirilmiştir. İletişim ve ticaret durma noktasına gelmiştir. Uzman ekiplerin aldığı önlemler karşısında zombi bilgisayarlar ana bilgisayarlar tarafından yeniden programlanarak bu önlemlere adapte olmuştur. Ana bilgisayarların Rusya'da olduğu ve programın Kril afabesiyle yazıldığı tespit edilmiştir[72]. Ancak Rusya siber saldırıları inkar etmiştir.

Estonya'nın "e-devlet" gelişiminde öncü bir ülke olması nedeniyle web sitelerine düzenlenen saldırıda Estonya Meclisinin sitesine, tüm bakanlık sitelerine, siyasi parti sitelerine, altı büyük haber kuruluşunun sitelerine, en büyük bankaların ve iletişim konusunda uzmanlaşmış firmaların sitelerine ana hedef olarak saldırılmıştır[73].

NATO durumu araştırmak için siber-terörizm uzmanlarını Estonya'ya göndermiştir. Saldırılar, dünyanın her yerinden gelmiş olsa da, Rusya devlet

---

[71] Siber Savaşlar:5. Boyutta Savaş, http://www.siberguvenlik.org.tr/makaleler/siber-savaslar-5-boyutta-savas/ Bâkır Emre, Erişim, 27/04/2013

[72] Richard A. Clarke, Robert K. Kanke, Siber Savaş (Cyber War), (çeviren:Murat Erduran) İstanbul Kültür Üniversitesi, Basım 2011, s.15

[73] Russia accused of unleashing cyberwar, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia Ian Traynor, Erişim, 27/04/2013

sunucularının da bu saldırılara ev sahipliği yaptığı tespit edilse de, Rusya saldırıları kendisinin yaptığını kabul etmemiştir[74].

Bilişim sistemlerine bağımlı olmak, aynı zamanda siber saldırılar için son derece savunmasız olmaktır. Bankaların, finans kurumlarının, devlet dairelerinin, borsanın çalışamaz hale gelmesi Estonya'da hayatı durdurma noktasına getirmiştir. Bilişim sistemlerine yapılacak saldırı, topla, tüfekle yapılacak saldırı ile kıyaslanınca, bir devleti işgal etmeyi, esir etmeyi, yok etmeyi, daha da kolaylaştırmıştır.

H- Gürcistan Siber Savaşı – 2008

Sovyetler Birliğinin çöküşü ile bağımsızlığını ilan eden Gürcistan'da kendisini siber savaşın içinde bulmuştur. Gürcistan, internete Rusya ve Türkiye üzerinden bağlanmaktadır. 1991 yılında bağımsızlığını ilan eden Gürcistan, 1993 yılında Güney Osetya ve Abhazya'nın kontrolünü kaybetmiştir. Moskova'dan destek alan asiler, buralarda bulunan Gürcü ordusunu çıkartıp, söz konusu bölgelerde Rus koruması ve mali desteğiyle bağımsız hükümetler kurmuştur.

2008 yılında Güney Osetya asileri Gürcü köylerine füze saldırısı yapmıştır. Füze saldırısına karşılık veren Gürcistan, Güney Osetya'nın başkentini bombalamıştır ve 7 Ağustos 2008'de bölgeyi işgal etmiştir. 8 Ağustos 2008'de Rus ordusu işgalci güçleri Güney Osetya'dan çıkartmış, bununla da kalmayıp siber savaşçılarını devreye sokmuştur. Gürcistan'ın dış dünya ile bağlantılarını kesmek için Gürcü medyasına ve devletin web sitelerine saldırmıştır. Saldırı silahı olarak DDoS'u kullanmıştır. Gürcistan'ın CNN ve BBC web sayfalarına girişini engellemiştir. Rusya siber savaşçıları Gürcistan'a trafiği destekleyen tüm yönlendiricileri ele geçirmiştir. Dışarıdan haber almayan Gürcistan, dışarıya da e-posta bile gönderememiştir.

Zor durumda kalan Gürcistan, Rusya'dan gelen tüm trafiği bloke etmiştir. Fakat Rusya bu sefer tüm saldırı paketlerini Çin üzerinden göndermiştir. Siber

[74] Estonia hit by "Moscow cyber war", http://news.bbc.co.uk/2/hi/europe/6665145.stm Erişim, 27/04/2013

uzay alanını savunmaya çalışan Gürcistan'ın savunması böylece etkisiz hale gelmiştir. Sürekli kendisini savunma çabası içerisinde çareler aramıştır. Gürcü bankaları sistemlerini kapatmış ancak Rus korsanlar, tüm dünya bankalarına Gürcistan üzerinden saldırı düzenlemiştir, saldırıya maruz kalan bankalar Gürcistan ile bağlantılarını kopartmıştır. Gürcü bankaları işleyemez hale gelmiştir. Kredi kartları ve cep telefonları kullanılamamıştır. Gürcistan'a yapılan DDoS saldırısını desteklemek isteyenlere anti-Gürcistan web sitelerinde DDoS virüsünün bilgisayarlara yüklenip botnete katılmaları için teşvikler başlatılmıştır.

Rusya, Estonya ve Gürcistan'a karşı saldırılarını DDoS silahını kullanarak yapmıştır. Her iki saldırıyı da Rusya kabul etmemiştir. Ancak Rusya ile yaşanan gerginliğin peşi sıra her iki devletin de siber saldırılara maruz kalması, saldırı yapabilecek tek ülkenin Rusya olduğu ihtimalini kuvvetlendirmektedir.

Ayrıca Estonya gerginliğinde, saldırganların bulunması ve cezalandırılması yönündeki Estonya'nın diplomatik talebi, Rusya tarafından reddedilmiştir. Rusya saldırıyı inkar ettiği gibi bir de kabul etmek zorunda olduğu halde Estonya'nın diplomatik talebini reddetmiştir. Gürcistan saldırısında, saldırının Rus istihbarat servislerinin web sitelerinden yapıldığı tespit edilmesine rağmen kendi kontrolü dışında olduğunu iddia etmiştir.

I- Kırgızistan Olayları -2009

11 Eylül 2001 saldırılarından sonra ABD terörle mücadele amacıyla dünyanın birçok bölgesinde askeri üs açmıştır. Bu üslerden birisi de Kırgızistan'nın başkenti Bişkek yakınlarındaki ABD'ye ait Manas Üssüdür. Kırgızistan'da aynı zamanda Rusya'ya ait Kant askeri üssü bulunmaktadır. Dünya'da hem Rusya'nın hem de ABD'nin askeri üssü bulunan tek ülke Kırgızistan'dır. ABD, Kırgızistan'da üs açmayı talep ettiği sırada, Kırgızistan bu talebi değerlendirirken, Çin ve Rusya'nın da görüşünü almıştır. Üssün açılmasına razı olan Rusya, 2009 yılına gelindiğinde, ABD'nin bölgedeki politikalarından

rahatsızlık duymuş ve üssün kapatılması için Kırgızistan'a baskı uygulamıştır[75]. (DÜĞEN, 2012)

Manas askeri üssünün kapatılması ve 6 ay içinde boşaltılması konusunda parlamento kararı alan Kırgızistan, ABD ile müzakerelere açık olduğunun sinyallerini de vermiştir. Müzakerelerin hemen ardından Kırgızistan'ın dört internet servis sağlayıcısı siber saldırıya maruz kalmıştır. Saldırılar nedeniyle internet servis sağlayıcıları Batı Kırgızistan'ın %80'ine internet hizmeti verememiştir[76].

Kırgızistan'a yapılan saldırıların üssün devamına ilişkin müzakerelerin hemen ardından gelmesi, saldırı şüphesinin ABD askeri üssünün kapatılmasını isteyen Rusya üzerinde yoğunlaşmasına neden olmuştur. Rusya'nın uyguladığı siber saldırı baskısıyla müzakereler sonunda ABD Manas askeri üssünün statüsü değiştirilerek Transit Merkez Üs haline getirilmiş ve kira süresi 2014 yılına kadar uzatılmıştır.

İ- Mavi Marmara Saldırısı 2010

İsrail'in ambargo uyguladığı Gazze'ye yardım malzemesi götürmek için, değişik milletlere ve değişik dinlere mensup gönüllüleri ve insani yardım taşıyan gemiler uluslar arası sularda olmalarına rağmen 31 Mayıs 2010 tarihinde İsrail askerlerinin saldırısına uğramıştır. Gemideki yardım gönüllüleri ile yolculuk boyunca bağlantı kurulmuştur. Ancak saldırı öncesinde İsrail tarafından gemiden dünya medyasına yayın yapan uydu frekansı ve uydu telefonlarının iletişimi kesilmiştir. Gönüllülerden 9'u İsrail askerlerin silahlı saldırısı sonucu hayatını kaybetmiştir. Bu olay Türkiye'de ve Dünya'da büyük yankı yapmıştır.

İsrail'in, Gazze'ye yardım götüren gemilere saldırmasına tepki göstermek amacıyla değişik haktivist gruplar çok sayıda devlet, şirket ve banka web sitesine

---

[75] Dar Alanda Büyük Pazarlık: Kırgızistan'da ABD ile Rusya'nın Üs Mücadelesi, http://www.21yyte.org/arastirma/kirgizistan/2012/03/28/6545/dar-alanda-buyuk-pazarlik-kirgizistanda-abd-ile-rusyanin-us-mucadelesi Turgay Düğen, Erişim, 30/04/2013

[76] 5. Boyutta Savaş: Siber Savaşlar-II, https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html Erişim, 30/04/2013

saldırı yapmıştır. İsrail'in özür dilememek için direnmesine tepki olarak, değişik zamanlarda değişik haktivist gruplar tarafından İsrail web sitelerine saldırılar yinelenmiştir.

J- OpIsrael Operasyonu 2012-2013

Anonymous, İsrail'in Gazze'ye yaptığı askeri operasyonu *"*OpIsrael*"* adını verdikleri, İsrail'e yönelik saldırılarına Kasım 2012'de başlamıştır, zaman zaman saldırılarını sürdürmüştür. 7 Nisan 2013 tarihinde İsaril'e *"*OpIsrael*"* operasyonunun devamı niteliğinde büyük bir siber saldırı yapacağını, İsrail'i internetten sileceğini günler öncesinden duyurmuştur. Redhack grubu da *"*OpIsrael*"* operasyonunda Anonymous'a destek vermiştir. Eylemin Op_Israel adlı Twitter hesabı üzerinden yapılan açıklamada 100.000'den fazla internet sitesinin, 40.000 Facebook hesabının, 5.000 Twitter hesabının ve 30.000 civarında İsrail banka hesabının eylemden etkilendiği ve eylemin 3 milyar dolar civarında maddi zarara yol açtığı belirtilmiştir[77].

Anonymous grubu, "Çılgınca bir saldırı" olarak tanımladığı Gazze operasyonunu kınayan videolar ve basın açıklamalarını internette yayınlamıştır[78]. "OpIsrael" adıyla başlattığı siber saldırının hedefinde İsrail Savunma Gücü'nün (IDF-Israel Defense Forces) ve İsrail'in önemli kuruluşlarının siteleri vardır. Zaman zaman İsrail'in web sitelerine saldırıları devam etmiştir.

İsrail'in, Kasım 2012'de Gazze'de yürüttüğü operasyonlar neticesinde, İsrail yetkililerinin yaptığı açıklamalara göre İsrail'in web sitelerine karşı 44 milyon siber saldırı gerçekleşmiştir[79].

7 Nisan 2013 tarihinde, İsrail'i internetten sileceklerini duyuran Anonymous grubu "OpIsrael" operasyonu adı altında ikinci büyük siber saldırısını yapmıştır.

---

[77] https://twitter.com/Op_Israel Erişim, 12/05/2013

[78] İsrail Ordusu Siber Savaşı Kaybetti, http://www.aa.com.tr/tr/tag/102397--israil-ordusu-siber-savasi-kaybetti Erişim,03/05/2013

[79] Anonymous declares "cyberwar" on Israel, http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html Erişim,08/05/2013

İsrail devletinin uygulamış olduğu politikaya tepkiler internet aracılığıyla yapılmıştır. Siber saldırılar ile dünya kamuoyunun dikkati çekilmeye çalışılmıştır. İsrail devletinin, operasyonlarına son vermesi için kamuoyunun baskısı harekete geçirilmeye çalışılmaktadır.

§ 7. SİBER SAVUNMA VE GÜVENLİK

Banka müşterilerinin hesap bilgilerine ulaşan veya sosyal uygulama, e-posta gibi birçok kişisel hesapları hackleyen hackerlar, devlet kurumlarının web sitelerini hackleyerek sitelere mesaj bırakan hactivist gruplar, ulusal sırları veya şirket sırlarını ele geçirerek, bu bilgileri uluslar arası mecrada satışa çıkaran hackerlar ve daha farklı yollarla farklı şekillerde yapılan bütün hacking saldırıları ulusal ekonomiyi ve güvenliği sarsan siber tehditlerdir. Siber tehditler ekonomiyi ve ulusal güvenliği korumak için ülkeleri önlem almaya itmiştir. Saldırılara karşı stratejiler geliştirilmiştir. Ülkeler siber ordu kurduğunu açıklamaktan çekinmektedir. Savunma Bakanlığı içerisinde birimler oluşturulmaya başlanmıştır. Gerek araştırma geliştirme çalışmaları adı altında, gerek istihbarat çalışmaları adı altında siber savaşçılar yetiştirilmeye başlanmıştır.

ENISA, Dünya'da Ulusal Siber Güvenlik Stratejisini belirleyen ülkeleri Nisan 2013'te web sitesinde sıralamıştır. AB üyesi olan ve Ulusal Siber Güvenlik Stratejilerini belirleyen ülkeler;

Avusturya Ulusal BİT Güvenlik Stratejisi (2012),
Çek Cumhuriyeti Siber Güvenlik Stratejisi 2011-2015 Dönemi (2011),
Estonya Siber Güvenlik Stratejisi (2008),
Finlandiya Siber Güvenlik Stratejisi (2013),
Fransa Bilgi Sistemlerinin güvenliği ve savunma stratejisi (2011),
Almanya Siber Güvenlik Stratejisi (2011),
Litvanya Elektronik Bilgi Güvenliği (Siber Güvenlik) Gelişim Prgramı 2011-2019 (2011),
Lüksemburg Ulusal Siber Güvenlik Stratejisi (2011),
Hollanda Ulusal Siber Güvenlik Stratejisi (2011),

Polonya Siber Koruma Toplum Programı 2011-2016 Dönemi (2011)
Romanya Siber Güvenlik Stratejisi (2011)
Slovak Cumhuriyeti Bilgi Güvenliği için Ulusal Strateji (2008)
İngiltere Siber Güvenlik Stratejisi (2009)
AB üyesi olmayan ve Ulusal Siber Güvenlik Stratejilerini belirleyen ülkeler;
Avustralya Siber Güvenlik Stratejisi (2011),
Kanada Siber Güvenlik Stratejisi (2010),
Hindistan Ulusal Siber Güvenlik Stratejisi (2011),
Japonya Ulus Korumak için Bilgi Güvenliği Stratejisi (2010),
Yeni Zelanda Siber Güvenlik Stratejisi (2011),
Norveç Bilgi Güvenliği için Ulusal Strateji (2012),
Rusya Federasyonu Bilgi Güvenliği Doktrini (2000),
Güney Afrika Siber Güvenlik Politikası (2010),
İsviçre Siber Risklere Karşı İsviçre'nin Korunması için Ulusal Strateji (2012),
Amerika Birleşik Devletleri Siber Uzay Ulusal Stratejisi (2011)
Kenya ve Uganda'da 2013 yılında Siber Güvenlik Ulusal Stratejilerini belirleyen ülkeler arasındadır[80]. (National Cyber Security Strategies in the World, 2013)

Ulusal siber güvenlik stratejisini belirleyen ülkelere bakıldığında, Estonya ve Gürcistan'ın uğradığı saldırılarda, saldırının merkezi olarak düşünülen Rusya, 2000 yılında saldırıların çok öncesinde bilgi güvenliği doktrinini belirlemiştir. Estonya ise AB ülkeleri içinde siber güvenlik stratejisini belirleyerek savunmasını geliştirmeye çalışan ilk ülkedir.

I- Kritik Alt Yapı Güvenliğine Yaklaşım

Kritik alt yapıların ve korunmasının önemini fark eden ulusal ve uluslar arası örgütler önlem almaya başlamıştır. Hazırlanan stratejiler ve direktifler korunmaya ve savunmaya yöneliktir.

[80] National Cyber Security Strategies in the World, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world Erişim, 07/05/2013

A- ABD

Kritik alt yapıların korunmasına yönelik çalışmalarına AB'den önce başlayan ve yaşanan 11 Eylül 2011 saldırısıyla da tecrübesini arttıran ABD daha fazla ilerleme göstermiştir.

Kritik altyapıların önemini ve güvenliğinin sağlanması gerektiğini 1990'lı yılların ortalarında fark eden ABD, yasal ve kurumsal düzenleme sürecine girmiştir. ABD'de ilk defa 1996 yılında Başkan Bill Clinton'ın imzaladığı 13010 sayılı kanun hükmünde kararname ile kritik alt yapı terimine yer verilmiştir. Kararname ile Kritik Altyapının Korunmasından Sorumlu Komisyonu kurulmuş ve kritik alt yapı tanımı yapılmıştır. Kararnamede kritik altyapı terimi "Bir takım ulusal alt yapıların yetersiz hale gelmesi veya tahrip edilmesinin ABD'nin savunma ve ekonomi güvenliği üzerinde zayıflatıcı bir etkisi vardır ki bu yönüyle alt yapıların varlığı ülke açısından hayati öneme haizdir" şeklinde yer almıştır. Takip eden yıllarda ABD'de kritik altyapıların güvenliğinin sağlanmasına yönelik düzenlemelerde kritik altyapı tanımı da değişiklik göstermiştir[81]. (Uluslararası Stratefik Araştırmalar Kurumu, 2011)

11 Eylül 2001 saldırısının ardından Ulusal Güvenlik Dairesi ve Ulusal Güvenlik Konseyi kurulmuştur. Bu düzenlemenin hemen ardından da Kararname ile Başkan'ın Kritik Altyapıyı Koruma Kurulu (PCIPB- President's Critical Infrastructure Protection Board) kurulmuştur. Ulusal Güvenlik Dairesi kritik sektörlerde ortaklaşa kullanılacak bir Ulusal Altyapı Koruma Planı (NIPP-National Infrastructure Protection Plan) geliştirmiş ve bu planla bütün kritik altyapı tesis ve sistemleri ile kaynakların korunması görevinin tek bir çatı altında birleştirilmesi amaçlanmıştır.

12 Şubat 2013 tarihinde Başkan Obama, siber saldırılara karşı kritik alt yapıların siber güvenlik sisteminin geliştirilmesi için kritik alt yapı şirketleri ve endüstri ortakları ile ortaklaşa bir strateji geliştirilmesi ve uygulanmasını

[81] Uluslararası Stratejik Araştırmalar Kurumu, Kritik Enerji Alt Yapı Güvenliği Projesi Sonuç Raporu, 2011, USAK Derneği

talimatını vermiştir[82]. Geliştirilecek yeni stratejiye NIST'in öncülük etmesi, sanayi ile işbirliği yapması, teknik yenilikleri etkinleştirmesi ve rehberlik yapması beklenmektedir.

B- ENİSA

ENISA'nın 2010 yılından itibaren siber güvenliği sağlamada daha önemli rol oynayabilmesi için yetkileri artırılmıştır. ENISA ile ABD İç Güvenlik Bakanlığı bu alanda işbirliği yapmak adına 'Cyber Atlantic' adı altında bir etkinlik de düzenlemiştir. Etkinlik çeşitli siber saldırılar için senaryolar üretmek ve bunlara karşı koymak üzere yapılacak çalışmaları kapsamaktadır.

ENISA, Mayıs 2012'de yayımladığı Ulusal Siber Güvenlik Stratejileri raporunda devletlerin kritik bilgi alt yapı korumalarının (CIIP-Critical Information Infrastructure Protection) güvenlik düzeyinin yükseltilmesi gerektiğini vurgulamıştır.

C- Avrupa Birliği

AB kritik alt yapı unsurlarının korunmasına yönelik ilk adımını 2004 yılında atmıştır. AB Komisyonunun 20.10.2004 tarihli 2004/702 sayılı "Terörle Mücadelede Kritik Altyapıları Koruma" başlıklı tebliğinde kritik altyapıları "Kesilmesi veya hasar görmesi halinde vatandaşların güvenliğini, sağlığı ve ekonomik refahı üzerine veya üye hükümetlerin etkin ve verimli ekonomik refahı üzerine veya üye hükümetlerin etkin ve verimli işleyişi üzerine ciddi olumsuz etkiler oluşturacak fiziki ve bilgi teknolojileri tesisleri, hizmetler ve varlıklar" olarak tanımlamıştır[83]. (COMMISSION OF THE EUROPEAN COMMUNITIES, 2004)

---

[82] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0 Erişim, 09/05/2013

[83] Critical Infrastructure Protection in the fight against terrorism http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF, s.3 Erişim, 24/04/2013

Kritik alt yapıların korunması için başlatılan bu çalışmada kritik alt yapı tesis ve sistemleri ile ilgili sorunların tanımı yapılmış ve programın yürütülmesi için gerekli amaçlar, koruyucu tedbirler, araçlar ve prensipler belirlenmiştir.

AB kritik alt yapı olarak belirledikleri; enerji tesisleri ve ağlar, iletişim ve bilgi teknolojisi, finans (bankacılık, menkul kıymetler ve yatırım), sağlık, gıda, su (barajlar, depolama, arıtma ve ağlar), ulaşım (havaalanları, limanlar, intermodal tesisleri, demiryolu ve toplu taşıma ağları ve trafik kontrol sistemleri), üretim, depolama ve tehlikeli malların taşınması (örneğin kimyasal, biyolojik, radyolojik ve nükleer maddelerin) ve Hükümet (örneğin kritik hizmetler, tesisler, bilgi ağları, aktif ve önemli ulusal siteleri ve anıtlar) sistemleridir. İletişimde potansiyel kritik alt yapı belirlenmesi için üç kriter belirlemiştir. Bu kriterler coğrafi etkilenebilir alanı, büyüklüğü ve zamana göre etkilerinin kapsamı.

17 Kasım 2005 tarihinde, Komisyon kritik alt yapının korunması için Yeşil Kitap'ı yayınlamıştır. Kritik altyapının korunması için bir Eylem Planı (EPCIP Action Plan) oluşturulmuştur. Eylem Planı ile alt yapı unsurlarının korunması, tehditlerin tespiti, gerekli önlemlerin alınması, hasar ve saldırı olasılığının asgari düzeyde tutulması amaçlanmıştır. Kritik Altyapı Erken Uyarı Bilgi Ağı (Critical Infrastructure Warning Information Network) oluşturulmuştur[84]. (European Commission , 2010)

2008 yılında çıkarılan 2008/114/EC sayılı direktifte kritik altyapının korunmasında ulaşım ve enerji alanına öncelik verilmesi kabul edilmiş ve her bir üyenin kendi ülke sınırlarındaki kritik altyapı unsurlarını belirlemesinin gerekliliği vurgulanmıştır.

Komisyon ağ ve bilgi güvenliğini sağlamak, muhtemel tehditleri tespit etmek ve önlemek amacıyla 2010 yılında "Dijital Gündem"i uygulamaya koymuştur[85]. Dijital Gündemin temel amacı internet ve bilgi teknolojisine dayalı

[84]Critical infrastructure protection, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm Erişim, 11/05/2013

[85]Digital Agenda for Europe: key initiatives http://europa.eu/rapid/press-release_MEMO-10-200_en.htm Erişim, 11/05/2013

ortak pazarın sürdürülebilirliğini sağlamaktır. Komisyon enerji, ulaşım, bankacılık ve finans sektöründeki şirketlerin zorunlu olarak siber güvenlik tedbirleri almalarını talep etmiştir. Güvenlik açısından kritik altyapıların çoğunluğunun özel sektöre ait kurumlarca işletilmesi sebebiyle bu kurumların da siber güvenlik çalışmalarına dâhil edilmesi önem taşımaktadır.

AB ve NATO, 2010 yılında düzenlenen Lizbon zirvelerinin sonucu olarak siber güvenlik alanına daha fazla önem verilmesi ve siber güvenlik olaylarına müdahale için birer merkez oluşturulmasına karar vermiştir.[86] 11 Ocak 2013'te AB genelinde organize siber suçla mücadele konusunda koordinasyon sağlayacak Avrupa Siber suç Merkezi (EC3- European Cybercrime Centre) kurulmuştur. Haziran 2011'de AB kurumlarının güvenliğini sağlamak amacıyla AB'nin ilk Bilgisayar Acil Müdahale Ekibi (CERT-Computer Emergency Readiness Team) kurulmuştur.

Avrupa Komisyonu tarafından teklif edilen 07/02/2013 tarihli NIS Direktifi, genel stratejinin kilit unsurlarından biri olup tüm üye devletlerin, ana internet sağlayıcıların ve e-ticaret platformları ile sosyal ağ ve enerji, ulaştırma, bankacılık ve sağlık hizmetleri gibi kritik alt yapı operatörlerinin AB genelinde güvenli ve güvenilir dijital çevre yaratmalarını gerekli kılmaktadır. Teklif edilen direktif ile, üye ülkelerin NIS stratejisi geliştirmesi ve NIS risklerini ve olaylarını engelleyecek, ele alacak ve bunlara müdahale edecek yeterli mali ve insan kaynaklarına sahip bir yetkili ulusal NIS makamı tayin etmesini istemiştir. Riskler ve olaylarla ilgili üye devletler ve Komisyon arasında işbirliğinin mekanizmasının kurulmasını, finansal hizmetler, ulaşım, enerji, sağlık gibi sektörlerdeki kritik altyapı operatörleri ile bulut bilişim, arama motorları, e-ticaret, sosyal ağlar gibi bilgi toplumu hizmet sağlayıcıları ve kamu idarecilerinin risk yönetimi konusundaki uygulamaları ve temel hizmetlere yönelik ana güvenlik olaylarını bildirmeleri istenmiştir.

---

[86] http://www.bilgesam.org/tr/index.php?option=com_content&view=article&id=2178:suerekli-artan-oenemi-inda-siber-guevenlik&catid=122:analizler-guvenlik&Itemid=147 Erişim, 11/05/2013

II. NATO

NATO'nun 1999 yılında Kosova Kirizi sırasında uğradığı siber saldırılar sonucu NATO önlemler almaya başlamıştır. 2002 yılında NATO Güvenlik Ofisi'ne bağlı NATO Computer Incident Response Capability (Bilgisayar Olayları Karşılama Kapasitesi) kurulmuştur. 2007'de Estonya'da meydana gelen siber saldırılar ise siber güvenliği daha etkin bir şekilde ele alması gerektiğini ve siber saldırılara karşı önlemleri yeni bir düzeye taşıması gerektiğini anlatan olay olmuştur. Kooperatif Siber Savunma Mükemmeliyet Merkezi (NATO CCD COE) resmen NATO'nun siber savunma yeteneğini geliştirmek amacıyla 14 Mayıs 2008'de Estonya'da kurulmuştur[87]. Merkez, NATO tarafından 28 Ekim 2008 tarihinde uluslararası askeri örgüt haline getirilmiştir.

NATO'nun bilgi güvenliği ve telekomünikasyon projelerini yürüten ajansı NCIA (NATO Communications and Information Agency), siber savunma için ittifakı güçlendirmek, danışma, komuta, kontrol desteği ve istihbarat sağlamak, gözetleme ve keşif yeteneklerini artırmak amacıyla uygun maliyetli, birlikte çalışabilir iletişim ve bilgi sistemleri ve hizmetleri sunmaktadır[88]. (NCI Agency)

2012 yılı sonunda faaliyete geçmesi için sözleşme yapılan NATO'nun siber güvenlik merkezi projesi olan, Siber Olaylara Müdahale Merkezi (Cyber Incident Response Center, NCIRC)'nin, 7/24 çalışması ve NATO üyesi ülkelerdeki tüm siber suç vakalarına anında müdahale edebilecek altyapıya sahip olması beklenmektedir[89].

III. ABD

2011 saldırılarından sonra çok yönlü olarak güvenlik önlemleri arttırılmıştır. Ancak siber tehditlerin hedefi olan ABD'de dijital Pearl Harbour kaygısı giderek artmıştır. ABD'den sonra e-devlet uygulamalarının yaygın olduğu

---

[87] Cyber Defence, http://www.ccdcoe.org/2.html Erişim, 25/05/2013
[88] Connecting Forces, http://www.ncia.nato.int/About/Pages/default.aspx, Erişim, 25/05/2013
[89] NATO and cyber defence, http://www.nato.int/cps/en/natolive/topics_78170.htm Erişim, 11/05/2013

ikinci devlet konumundaki, Estonya'nın uğramış olduğu siber saldırı ülkede hayatı durma noktasına getirmiştir. E-devlet uygulamalarında lider olan ABD, Estonya'nın başına gelenlerden ders çıkarmıştır. Dünyaya sunduğu siber ortamın ve geliştirdiği 5.boyut silahın mucidi ABD, o silaha karşı kendini korumaya çalışmaktadır. Bu nedenle yeni güvenlik stratejileri geliştirmiştir. Siber güvenlik konusunda dünyaya örnek model olmaktadır.

Top, tank, tüfek gibi geleneksel yöntemlerle yapılan savaşların verdiği zarar, siber saldırılarılar ile verilen zarar eşit tutulmaktadır. Siber saldırılar ulusal güvenliğin ve toplum hayatının devamlılığını tehlikeye atan bir faktör olarak görülmektedir. ABD hükümeti, uğrayacağı siber saldırıları savaş sebebi olarak göreceklerini duyurmuştur[90]. Siber güvenliğe önem veren ABD Başkanı Obama, siber tehdidin ekonomik ve ulusal güvenliğin karşı karşıya kaldığı en ciddi zorluk olduğunu, 21. yüzyılda Amerika'nın ekonomik refahının siber güvenliğe bağlı olduğunu ilan etmektedir[91].

Cornell üniversitesi öğrencisi Robert Tappan Morris'in 1988 yılında internetin büyüklüğünü ve sistem açıklarını anlamak için yazdığı ve internete saldığı morris solucan yazılımı, internet ağına bağlı 60.000 bilgisayarın %10'unu çalışamaz hale getirmiştir. Bu olay internet güvenliği vakalarında koordinasyon eksikliğini fark ettirmiş ve ilk Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi (CERT/CC- Computer Emergency Readiness Team Coordination Center) kurulmasına vesile olmuştur. CERT/CC işbirliği ile İç Güvenlik Bakanlığı (DHS-Department of Homeland Security) organizasyonu içerisinde bulunan Ulusal Siber Güvenlik Birimi altında, ülkenin siber güvenlik duruşunu belirlemek, bilgi paylaşımını koordine etmek ve siber riskleri yönetmek amacıyla ulusal bir CERT organizasyonu (US-CERT) kurulmuştur[92]. US/CERT, ulusal siber bilinçlendirme çalışmaları yapmaktadır. Mevcut ve potansiyel güvenlik

---

[90] Cyber Combat: Act of War, **http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html** Siobhan GORMAN, Erişim, 23/05/2013

[91] Cybersecurity, http://www.whitehouse.gov/cybersecurity Erişim, 15/05/2013

[92] About Us, http://www.us-cert.gov/about-us/ Erişim, 21/05/2013

tehditleri ve güvenlik açıkları hakkında bildirimlerde bulunmaktadır. Ayrıca siber olayların ve yazılım güvenlik açıklarının ihbar edilmesi için 7/24 çalışmaktadır

Başkanlık direktifleri ile geliştirilen siber internet güvenliğinin sağlanması 2003 yılında yayınlanan "Ulusal Siber Uzay Güvenliğini Sağlama Stratejisi" belgesi ile resmiyete dökülmüştür[93]. Ocak 2008'de Başkan George W. Bush tarafından imzalanan "Kapsamlı Ulusal Siber Güvenlik Girişimi" (Comprehensive National Cybersecurity Initiative, CNCI) başlıklı direktif ile Amerika siber politikasını yenilemiştir. Bu belge bir takım büyük çaplı politika değişikliklerini içermektedir.

Siber güvenliğin arttırılması konusunda hassas olan Başkan Obama CNCI'yı desteklemiş ve girişimlere takviye hedefler belirlemiştir. Ağ güvenliğinin sağlanması, tehditlerin engellenmesi konusunda devlet, hükümet ve özel sektör ortaklarının, ortak bir durumsal farkındalık yaratması gerektiği ve tehditlere karşı acil savunma cephesi kurulması için mevcut güvenlik açıklarının azaltılması, izinsiz erişimin engellenmesi için hızlı hareket edilmesi gerektiği benimsenmiştir. Tehditlere karşı savunma yapabilmek için yeteneklerin arttırılması ve bilgi teknolojilerinin tedarik zincirinin güvenliği arttırılmaya çalışılmıştır. Ar-Ge çalışmalarına koordine ve yönlendirme yapılarak, siber eğitim çalışmalarının genişletilerek, siber güvenlik ortamı güçlendirilmeye çalışılmaktadır.[94] (The Comprehensive National Cybersecurity Initiative)

Günümüzde siber ordusunu kurduğu iddia edilen birçok ülke olmasına rağmen, ülkeler resmi kanallar aracılığıyla bu bilgileri doğrulamamaktadır. ABD ise siber ordusunu kurduğunu resmi olarak açıklamıştır. Diğer ülkelere göre daha şeffaftır. ABD Genelkurmay Başkanlığı'na bağlı ABD Siber Komutanlığı (Cyber Command) 2009 yılında kurulmuştur. Cyber Command'ın savunma ve saldırı

---

[93] National Strategy to Secure Cyberspace, http://www.dhs.gov/national-strategy-secure-cyberspace Erişim, 21/05/2013

[94] The Comprehensive National Cybersecurity Initiative http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative Erişim, 21/05/2013

görevleri vardır. Ulusal ağların güvenliğinden ve saldırı yeteneklerinin geliştirilmesinden sorumludur.

2013 yılında internet üzerinden gelen tehdit boyutunun artmasıyla ABD Siber Komutanlığı, siber savaşçılarının sayısını artırma yoluna gitmiştir ve ABD 5.000'e çıkardığı siber savaşçı kadrosuyla ordusunu oluşturmuştur. Küresel avantaj sağlamak için profesyonel bir ekip oluşturmayı hedefleyen ABD ordu ağını savunmak ve siber savaş mücadele etkisini artırmak için toplam 21.000 kişiyi aşmasını hedeflediği, asker ve sivillerden oluşan siber savaşçı ordusunu genişletme peşindedir. Başkan Obama, siber savunma sistemlerine verdiği önceliği, Pentagonun harcamalarının kısılması ve siber savunma bütçesinin 2014 yılında 800 milyon dolar daha artırılarak 4,7 milyara çıkarılmasını teklif etmesiyle bir kez daha yinelemiştir[95].

ABD Ticaret Bakanlığı kuruluşu olan NIST tarafından yapılan çalışmalar ABD'nin siber güvenlik konusunda gelişmesine yardımcı olmaktadır. ABD'nin ulusal ve ekonomik güvenliğin, kritik altyapıların güvenliği ile sağlanabileceğine dikkat çekilerek, ABD Başkanı 12 Şubat 2013 tarihli direktifi ile kritik altyapıların güvenliği ve esnekliğinin arttırılmasını istemiştir. Hazırlanacak standartlar ile devlet, kritik alt yapı sahipleri ve işletmeler arasında işbirliği ve siber bilgi paylaşımının geliştirilmesi sağlanılmaya çalışılmaktadır. Ulusal Standartlar ve Teknoloji Enstitüsü(NIST-National Institute of Standarts and Technology)'nün kritik alt yapılara dair siber riskleri azaltmak için siber çerçeveyi geliştirmeye öncülük etmesi beklenmektedir.

ABD, hazırlanan raporlar ve açıklamalarıyla Çin'i ve İran'ı siber tehdit olarak gördüğünü belirtmiştir. ABD Savunma Bakanlığı tarafından 6 Mayıs 2013 tarihinde yayınlanan, "2013 Military and Security Developments Involving the People's Republic of China" başlıklı yıllık Kongre Faaliyet Raporu, Çin Halk

---

[95] Obama budget makes cybersecurity growing U.S. priarity, http://www.reuters.com/article/2013/04/11/us-usa-fiscal-cybersecurity-idUSBRE93913S20130411 And, Sullivan, Erişim, 21/04/2013

Cumhuriyetinin askeri gücünü konu alan bir rapordur[96]. Raporda Çin Halk Cumhuriyetinin 2012 yılında başlattığı ilk uçak gemisi çalışmasından ve gelişmiş kısa ve orta menzilli konvansiyonel balistik füzelerinden, kara saldırısı ve anti-gemi cruise füzelerinden, askeri siber sistemlerine yapmakta olduğu yatırımlarından bahsedilmektedir. (The United States Department of Defense, 2013)

Aşağıda açıklanacağı üzere ABD'li güvenlik şirketi Mandiant'ın Şubat 2013'te yayınladığı raporuyla ABD'nin, Çin ordusunun siber gücüne olan endişesini attırmıştır. (bkz. V. ÇİN)

Siber tehdit olduğu düşünülen diğer bir ülke İran'dır. İran'ın uğradığı stuxnet saldırısının arkasında hangi devlet olduğu konusunda birçok ihtimal ortaya atılmıştır. Bu ihtimallerden birisi de ABD ve İsrail ortaklığıyla, stuxnet virüsünün geliştirildiğidir. Virüsün yazılım kodunun içinde yer alan 19790509 rakamlarının, İran'lı Yahudi iş adamı Habib Elghanian'in idam edildiği tarihi vurgulamasıdır. Ancak bu kadar açık bir şekilde ipucu bırakılamayacağı ve hedef şaşırtmak için başkaları tarafından böyle bir tarihe yer verilmiş olduğu da düşünülmüştür.

Bush yönetimi sırasında başlatılan ve "Olimpiyat Oyunları" olarak adlandırılan siber saldırılar ABD Başkanı Obama döneminde de devam etmiştir. Başkan Obama'nın, emriyle saldırı virüslerinin kullanımının devam etmesi ve hızlandırılması istenmiştir. Kontrolden çıkan stuxnet virüsü, hedefi olan İran'dan başka ülkelere de sıçramaya başlamış ve sanayi tesislerine saldırmıştır[97]. Ancak ABD tarafından bu saldırılar resmi olarak, ne kabul edilmiştir ne de reddedilmiştir. (SANGER, 2012)

---

[96] The United States Department of Defense, Military and Security Developments Involving the People's Republic of China 2013, Erişim, 24/05/2013

[97] Obama Order Sped Up Wave of Cyberattacks Against Iran, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 David E. SANGER, Erişim, 01/05/2013

Dünya'da lider güç konumunda olan ABD'nin, liderlik sandalyesinin sallanacağı yönündeki korkuları nedeniyle savunmasını geliştirmeye çabalamaktadır. Diğer ülkelerin savunma sistemleriyle yakından ilgilenen ABD, ülkelerin savunma ve saldırı teknolojilerini, bu yönde yapılan yatırımlarını tespit etmeye çalışmaktadır. Dış Siyaset Konseyi Başkan Yardımcısı Ilan Berman'ın İç Güvenlik Temsilciler Komitesinde, siber dünyada savunma ve saldırı teknolojilerini geliştirmek için var gücüyle çalışan, yatırımlar yapan İran'ı siber tehdit olarak görmektedir[98]. (BERMAN, 2013)

ABD, güvenlik konusunda kendisinden emin değildir. Özellikle stuxnet virüsünü ürettiğini kabul etmekten korkmaktadır. Kabul ettiği takdirde diğer ülkelerin daha güçlü siber silahlar üretebilmesi için onları yüreklendireceği ihtimali söz konusudur. Ayrıca SCADA sistemlerini hedef alan siber silah üretmesi ve bu silahla saldırıya geçmiş olması, ABD'nin pek de şeffaf olmadığını göstermektedir. Siber saldırıları savaş sebebi olarak göreceğini savunan ABD için bu durum iyi sonuçlar doğurmayacaktır.

IV. İsrail

Gazze'ye yaptığı saldırılardan dolayı sık sık siber saldırılarla mücadele etmek zorunda kalmıştır. İsrail, bu kadar siber saldırıya uğramış olmasına rağmen, siber güvenlik ve savunma stratejisine sahip bir ülkedir.

İsrail devletinin siber savunmadan sorumlu dört kuruluşu vardır. İsrail Savunma Kuvvetlerine bağlı, "Birim 8200" adı verilen, asker ve subaylardan oluşan personel üç alanda odaklanmaktadır. İstihbarat toplama, savunma ve saldırı, Birim 8200'ün siber savaşta belirlediği alanlardır[99]. (LEWIS & TIMLIN, 2011)

---

[98] The Iranian Cyber Threat, Revisited, Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies 20 May 2013, http://docs.house.gov/meetings/HM/HM08/20130320/100523/HHRG-113-HM08-Wstate-BermanI-20130320.pdf Ilan Berman, Erişim, 01/06/2013

[99] Cybersecurity and Cyberwarfare 2011,

İsrail'in siber güvenlik stratejisi içerisinde ülke içindeki bilgisayarların güvenliğini sağlamak, ulusal altyapı ve hükümet sistemlerinin savunmasını sağlamak ise iç istihbarat kurumu Shin Bet'in görevidir. Başlangıçta IDF'nin bir kolu olarak, İsrail'in bağımsızlık ilanı ile 1948 yılında kurulmuştur. Shin Bet faaliyet sorumluluğu daha sonra Başbakanlığa bağlanmıştır.

C4I **(**Command, Control, Commonications, Computers, Intelligence **-** Komuta, Kontrol, Haberleşme, Bilgisayar ve İstihbarat**)** sistemler bütünü, kolordu iletişim ve siber savunma faaliyetlerinden sorumludur. 2009 yılında askeri istihbarat ve C4I Müdürlüğü arasında işbirliğini geliştirmek için "Matzov" olarak bilinen üst düzey Şifreleme ve Bilgi Merkezi kuruldu. Merkez, teknolojik istihbarat sağlamak ile sorumludur. Hükümetin, askeriyenin ve büyük şirketlerin ağlarını korumakla sorumludur. Matzov ayrıca IDF, Shin Bet, MOSSAD ağları yanı sıra elektrik, su ve telefon gibi büyük şirketlere destek vermek, kod yazmak ve şifreleme yapmak için sorumludur.

18 Mayıs 2011 tarihinde yabancı ülkeler tarafından savunma sistemlerine zarar verebilecek siber terör saldırılarına karşı Ulusal Sibernetik Çalışma Grubu kurulmuştur. İsrail Ulusal Siber Bürosu (Israel National Cyber Bureau-INCB), 2012 yılının başlarında kurulmuştur. Bilgisayar sistemlerindeki saldırılara karşı ülkeyi savunmak için kurulan INCB, önem verdiği üç unsurun, güvenlik sisteminin, iş dünyasının ve akademi dünyasının işbirliğiyle savunma sistemini organize etmeyi amaçlamıştır[100]. Ülkenin uğradığı siber saldırılarda, ülkedeki çeşitli kurumlar arasında koruyucu önlemler alarak, siber savunma faaliyetlerini koordine etmiştir. Tel Aviv Üniversitesi Ulusal Güvenlik Çalışmaları Enstitüsü de çalışmalarını saldırı, savunma ve istihbarat aşamalarıyla yürütmektedir.

Yaptıkları saldırılarla ülkelerin güvenlik açıklarını da tatbik ve tespit etme fırsatı bulan RedHack grubu, İsrail'in en ufak bir sızmaya izin vermediğini, güvenliğinin güçlü olduğunu belirtmiştir.

---

http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf Erişim, 01/05/2013

[100] Cabinet Briefed on the Israel National Cyber Bureau http://www.pmo.gov.il/english/mediacenter/spokesman/pages/spokecyber111112.aspx 03/05/2013

İsrail'in avantaj sağladığı en önemli özelliği ise, kritik hükümet sistemlerinin siber tehditlerden etkilenmemesi için internetten bağımsız olarak, intranet aracılığıyla hassas ve gizli bilgilerini taşımasıdır. İnternet üzerinden gelebilecek siber tehditlere karşı kendini kapamış ve kritik ulusal sistemlerinin güvenliğini sağlamıştır[101]. (İstanbul Bilgi Üniversitesi, 2012)

V. Çin Halk Cumhuriyeti

Siber çalışmalarını gizlilik içerisinde yürütmektedir. Çin hükümeti, Çin kaynaklı olduğu tespit edilen siber casusluk olaylarını şimdiye kadar reddetmiştir. Her türlü siber saldırıya karşı olduğunu ve Çin hükümetinin siber saldırıları desteklemediğini defalarca ifade etmek durumunda kalmıştır.

Çin hükümetince 2004 yılında yayınlanan beyaz kitap, askeri bilişim sistemlerinin güçlendirilmesi ve siber savunmanın arttırılması için önemli bir faktördür[102]. Çin Ulusal Kalkınma Stratejisi 2006 yılında yayınlanan beyaz kitapta ise, kamu hizmetlerinde, ekonomide, eğitimde, Milli Savunma ve silahlı kuvvetlerin inşasında bilişim teknolojilerinden olabildiğince istifade edilmesini ve bilgi teknolojilerinin geliştirilmesini teşvik etmektedir[103]. Ülkede her alanda bilişim teknolojilerinin kullanımını ve geliştirilmesini teşvik ederken aynı zamanda temel bilgi ağlarının ve kritik bilgi sistemlerinin, güvenlik koruma sistem düzeyinin yükseltilmesini öngörmüştür. Ağ güvenliğinin sağlanması, şifreleme tekniklerinin geliştirilmesi ve kullanımının güçlendirilmesi, bilgi güvenliği risk değerlendirmesinin güçlendirilmesi bilgi teknolojileri stratejik eylem planı çerçevesindedir.

Çin siber güvenliği ve siber savunması Çin Halk Kurtuluş Ordusu'nun (Peoples Liberation Army – PLA) sorumluluğundadır. PLA'nın 3. ve 4. Bölümleri

---

[101] Siber Güvenlik Raporu, İstanbul Bilgi Üniversitesi, Bilişim ve Teknoloji Hukuku Enstitüsü, Mayıs 2012, İstanbul

[102] http://politics.people.com.cn/GB/1027/3081796.html Erişim, 19/05/2013

[103] http://www.gov.cn/gongbao/content/2006/content_315999.htm Erişim, 19/05/2013

ülkenin bilişim altyapısının korunmasından ve bilgi güvenliği ile ilgili ileri araştırma yapmaktan sorumludur.

ABD Siber Güvenlik Şirketi Mandiant, 18 Şubat 2013 tarihinde APT1 raporunu yayınlamıştır. Gelişmiş kalıcı tehditleri içeren raporda Çin'in 61398 nolu birliği konu alınmıştır. Birlik Şangay'ın Pudong bölgesinde yer alan 12 katlı bir binada 2006 yılından bu yana faaliyet göstermektedir. Bina, Çin Halk Kurtuluş Ordusu'nun bölgesine yakın bir yerde bulunmaktadır. Yüzlerce veya binlerce personeli olduğu düşünülmektedir. Personel, iyi derecede İngilizce bilmektedir ve bilgisayar ağ güvenliğinde uzman kişilerden oluşmaktadır. 20 sektörden 141 şirket siber casusluk yapılarak bilgileri sızdırılmıştır. Sızılan ağların içerisinde ortalama 356 gün kalınmıştır. En uzun 1.764 gün kalınmıştır. Şirketlerin yüzlerce terabaytlık mavi kopya, iş planı, fiyatlama belgesi, kullanıcı bilgisi, e-posta adresi ve iletişim listeleri ele geçirilmiştir. Casusluk yapılan sektörler, Çin'in 5 yıllık strateji planında yer alan sektörlerden oluşmaktadır. 61398 nolu birliğin, devlet destekli olduğu düşünülmektedir[104]. (MANDIANT, 2013)

Mandiant'ın yayınlamış olduğu raporu Çin reddetmiştir. Çinli filozof Sun Tzu'nun 2500 yıl önce yazdığı savaş sanatları, günümüzde Çin'e savaş stratejilerini belirlemede öncülük etmektedir. Sadece Çin'e değil, dünyada birçok şirkette Sun Tzu'nun öğretilerinden faydalanılmaktadır. Sun Tzu'nun, en önemli öğretisi ise taktik ve stratejiler ile savaşmadan düşmanı yenmenin mümkün olduğudur. Mandiant şirketinin raporu doğru ise yıllardır birçok önemli bilgiyi sızdıran Çin, "düşmanı ve kendinizi iyi biliyorsanız, yüzlerce savaşa bile girseniz sonuçtan emin olabilirsiniz" savaş sanatı öğretisini uyguluyor demektir. Rapor doğruları yansıtmıyor olsa bile sonuçta böyle bir rapor bütün dünyada yankı uyandırmış ve korku salmıştır, böyle bir durumda ise "Savaşmaktansa morallerini bozarak düşmanlarını alt et; kentlerini stratejiyle ele geçir." öğretisi başarıyla tamamlanmış demektir. Her iki durumda da Çin avantaj elde etmiştir.

[104] APT1, Exposing One of China's Cyber Espionage Unitshttp://intelreport.mandiant.com/ Erişim, 15/05/2013

Mandiant'ın yayınladığı rapordan 2 ay sonra 16 Nisan 2013 tarihinde Çin Halk Cumhuriyeti beyaz kitap yayınlamıştır[105]. Yayınlanan beyaz kitapta Çin Silahlı Kuvvetlerinin Kullanım Çeşitliliği başlığıyla ilk defa kara, hava ve deniz kuvvetlerinin asker sayıları açıklanmıştır. Çin, askeri alanda her zaman gizliliğini sürdürmüştür. Beyaz kitap ile bu sefer askeri şeffaflığının arttığını göstermeye çalışmıştır. Mandiant raporunun hemen ardından beyaz kitabın yayınlanması ve ordu hakkında bilgi verilmesi, Çin ordusunun zararsız olduğunu göstermeye çalışmasındandır. Ancak askeri yapılanmadaki asker sayısını veren Beyaz Kitap'ta siber savaşçılardan bahsedilmemiştir. Siber ve uluslar arası rekabette yüksek strateji zemini hazırlamak için ileri teknoloji ile askerin geliştirilmesinin önemi vurgulanmıştır.

Çin'i siber tehdit olarak gören ve yayınlanmış olan beyaz kitaptan tatmin olmayan ABD, Mayıs 2013'te yayınladığı rapor ile endişe duyduğunu ispat etmiştir. (bkz. III. ABD)

Çin, filozof Sun Tzu'nun, "usta savaşçı saldırıda korku salan, karar vermede ise çabuk olandır" öğretisini de başarıyla gerçekleştirmiştir.

VI. İran

İran, yaptığı nükleer çalışmalar neticesinde stuxnet gibi güçlü bir siber saldırıya maruz kalmıştır. Saldırı neticesinde nükleer çalışmalarına darbe vurulmuştur. Siber güvenlik stratejisi konusunda geniş bilgi vermemektedir. Siber güç konusunda ABD, Rusya ve Çin'den sonra İran'ın dördüncü büyük güç olduğu düşünülmektedir.

Silahlı kuvvetler, savunma sanayisi ve üniversitelerden oluşan üçlü işbirliği ile güçlü bir mekanizma şekillenmiştir. Siber savunma ve gerektiğinde siber saldırı yeteneğini geliştirmiştir. İran Savunma Bakanı, ABD'nin siber terörün başında bulunduğunu, çeşitli suçlamalarla siber terörün arttırılması için ortam sağladığını belirtmiştir. İran gençlerinin dahi bilgisine güvenen İran

[105]中國武裝力量的多樣化運用（2013年4月）http://big5.gov.cn/gate/big5/www.gov.cn/jrzg/2013-04/16/content_2379013.htm Erişim, 26/05/203

Savunma Bakanı, İran'ın dahi bilgisinin siber alanda alt edilemeyeceğini belirtmiştir[106].

Siber savunma organizasyonu, ordu tarafından koordine edilmektedir. Askeri siber savunma takımları siber saldırıları önlemek amacıyla sürekli bilgisayar ağlarını kontrol ederek, saldırı söz konusu olduğunda anında savunmaya geçmektedir. Genellikle saldırılara maruz kalan İran'ın, siber saldırılarda, bilgisayarlardaki bilgilerinin hacklenmesi amaçlanmıştır. İran, stuxnet virüsünden sonra savunma sistemini geliştirmeye yönlenmiştir. İran, Velayet tatbikatları adı altında deniz ve hava kuvvetlerinin askeri gücünü tatbik etmektedir.

"Velayet-91" adı verilen uzmanlık saha tatbikatında ise siber saldırılara karşı tatbikat yapılmıştır. Tatbikatta düşman hackerlerin, savunma konumundaki bilgisayar sistemine siber saldırı eylemi teşebbüsünde bulunduğu, fakat bu saldırının deniz kuvvetlerinin siber savunma takımı tarafından zamanında fark edilerek, yerli bilgisayar programları ile yapılan misillemede gerçekleşen siber saldırılarının başarı ile etkisiz kılındığı belirtilmiştir[107]. (Velayet 91 uzmanlık saha tatbikatında siber saldırı başarı ile denendi, 2012)

2011 yılında İran Siber Polis Birimi kurulmuştur. Ulusal ve uluslar arası siber politikaların belirleneceği Siber Teknoloji Yüksek Kurulu'nu Nisan 2012'de kurmuştur. İran'da iletişimin denetlenmesi ve devlet tarafından internetin filtrelenmesi, medya erişiminde sınırlamalar söz konusudur.

VII. Rusya

Silahlı Kuvvetler Siber Komutanlığını kurmak için görüşmeleri devam eden Rusya, oluşturacağı komutanlık ile silahlı kuvvetler ve devlet altyapısının

---

[106] **İran savunma bakanı:Amerika hükümeti siber terörün başıdır** http://www.islamidavet.com/2012/10/29/iran-savunma-bakaniamerika-hukumeti-siber-terorun-basidir/ Erişim, 02/06/2013

[107] Velayet 91 uzmanlık saha tatbikatında siber saldırı başarı ile denendi, http://www.islamidavet.com/2012/12/30/velayet-91-uzmanlik-saha-tatbikatinda-siber-saldiri-basari-ile-denendi/ Erişim 01/06/2013

bilgi güvenliğini sağlanmayı hedeflemektedir. Devlet, sanayi ortakları ile işbirliği halinde çalışmaktadır. Siber yeteneklerin ortaya çıkışına, üniversiteler araştırma ve geliştirme çalışmalarıyla destek vermektedir.

Rusya Devlet Başkanı Vladimir Putin, önceliği devlet bilgi alt yapılarına yapmıştır. Federal Güvenlik Servisi tarafından, muhtemel ağ saldırılarına karşı Rus devlet sitelerinin bilgi alt yapılarını korumasını emretmiştir.

Ay Işığı Labirenti isimli siber casusluk olayının, Estonya, Gürcistan ve Kırgızistan'a yapılan siber saldırıların faili, Rusya olarak tahmin edilmektedir. Rusya'nın bu üç ülke ile yaşadığı gerginlik sonrasında ülkelerin siber saldırıya maruz kalması, saldırıları Rusya'nın yaptığı ihtimalini güçlendirmektedir. Ancak Rusya, saldırıların arkasındaki isim olmasına ve siber saldırıların ülkeleri baskı altına alabileceğinin farkında olmasına rağmen siber savunma konusunda faaliyette bulunmadığı, izlenimi vermektedir. Savunma Bakanlığı tarafından kurulacak olan Siber Komutanlığı için ağır davranılmaktadır. Bunun nedeni Rusya'nın siber savunma personelinin veya savunma faaliyetlerinin mevcut olmadığından değil, resmi olarak bunu kabul etmeyişidir.

VIII. Türkiye

Siber saldırılardan nasibini alan Türkiye'de siber güvenlik olaylarına karşı mücadelesine devam etmektedir. Symantec'in yayınladığı İnternet Güvenliği Tehdit Raporu dünya genelinde kötü niyetli saldırıların yüzde 81 oranında arttığını ve Türkiye'nin de bu artıştan payını alan ülkeler arasında yer aldığını ortaya koymaktadır[108]. Türkiye EMEA (Avrupa, Orta Doğu ve Afrika) bölgesinde kötü amaçlı yazılım saldırılarına en çok maruz kalan 10 ülke arasında 4. sıradadır. Rapora göre 2011'in sonu itibarıyla siber saldırılar gün bazında 77 saldırıdan 82 saldırıya kadar yükselmiş durumdadır. Türkiye'de internet kullanımında yoğun bir

[108] Symantec'in yayınladığı İnternet Güvenliği Tehdit Raporu kötü niyetli saldırıların yüzde 81 oranında arttığını ortaya koyuyor http://www.symantec.com/tr/tr/about/news/release/article.jsp?prid=20120514_01 Erişim, 11/05/2013

artış vardır. AB direktifleri doğrultusunda çalışmalarını sürdüren Türkiye, yaptığı çalışmalar ile diğer ülkelerden geride kalmayacak konumdadır.

A- Siber Güvenlik Koordinasyon Kurulu

20 Ekim 2012 tarihinde Resmi Gazetede yayınlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile Siber Güvenlik Koordinasyon Kurulu kurulmuştur. Kararın 4. Maddesinde "siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan program, rapor usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla" kurulu oluşturacak yetkililer belirlenmektedir. Kurulu, Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında, belirlenen bakanlık, kamu kurum ve kurul yetkilileri haricinde Ulaştırma Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticileri oluşturmaktadır.

Kamu kurum ve kuruluşlarında işbirliğini öngören karar ile Ulusal Siber Güvenliğin sağlanması amacıyla Bakanlık tarafından yayımlanan plan, program, usul ve standartlara, bütün kamu kurum ve kuruluşlarının uyması esastır. Yapılacak çalışmalar sürecinde mümkün olduğu ölçüde milli çözümler üretilmesi ve milli kaynaklar kullanılması ise ulusal güvenliğin sağlanmasında önemli bir husustur. Maddi kaynak planlaması ve kaynak tahsisinde önceliğin Ulusal Siber Güvenlik alanında yapılacak çalışmalara verilmesi ise kararın, çalışmaların önünü açacak ve gelişmesini sağlayacak bir ilkesidir.

B- TÜBİTAK- SGE

1997 yılında kurulan ve Bilgi Sistemleri Güvenliği (BSG) birimi adı ile Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) altında çalışmalarına başlamıştır. 2012 yılından bu yana ise TÜBİTAK'ın Bilişim ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi (BİLGEM) bünyesinde Siber Güvenlik Enstitüsü (SGE) faaliyetlerini sürdürmektedir. SGE; askeri kurumlara, kamu kurum ve kuruluşlarına ve özel sektöre bilgi güvenliği danışmanlığı yapar ve bilgi

güvenliği ile ilgili teknolojik çözümler sunar ve bu alanda araştırma ve geliştirme faaliyetleri yürütür[109].

SGE birçok hizmeti ile siber güvenlik alanında bilgi birikiminin oluşmasını sağlamıştır. SGE, kamu kurum/kuruluşları ve özel sektör şirketlerine sızma testleri ve güvenlik denetlemeleri yapmaktadır. Bilgi sistemlerinin, güvenli tasarımı, kurulumu ve konfigürasyonu konusunda çalışmaları ile eksik güvenlik önlemlerinin tespit edilmesini ve güvenlik önlemlerinin tasarlanmasını sağlayarak bilgi sistemlerinin güvenliğini sağlamaktadır. Bilgi Güvenliği Yönetim Sistemleri konusunda kurum ve kuruluşlara danışmanlık hizmeti vermektedir. Kamu kurum/kuruluş ve özel sektöre güvenli yazılım hazırlanması konusunda vermiş olduğu eğitimlerle destek sağlamaktadır. BT Ürün Güvenliği Laboratuvarlarında akıllı kart yongaları ve işletim sistemleri, kriptolu bellekler, akıllı kart okuyucuları, donanım güvenlik modülleri, ağ güvenliği ürünleri, güvenlik uygulama yazılımları ve güvenilir ortam modülleri için risk analizi ve sızma testi çalışmaları yürütmektedir. Zararlı yazılımların analizi yapılmaktadır. Dijital Adli Analiz Laboratuvarında adli olayların aydınlatılabilmesi için adli bilişim teknik ve araçları kullanılarak gerekli incelemeler yapılmakta, siber saldırılarda saldırının kaynağı, sisteme nasıl sızıldığı ve sistemde neler yapıldığı tespit edilmekte ve detaylı incelemeler yapılmaktadır. Ulusal geniş ölçekli ağ altyapılarında çalışacak siber tehdit gözetleme, tespit ve önleme sistemleri/teknolojileri geliştirme konusunda faaliyetlerini yürüten SGE'nin, geliştirdiği bu sistemlerin milli bilişim altyapı ve hizmetlerinin korunmasına ciddi katkı yapması beklenmektedir. TÜBİTAK BİLGEM SGE bünyesinde 2006-2010 Türkiye Bilgi Toplumu Stratejisi Eylem Planı kapsamında, bilgisayar güvenlik olaylarını ulusal ve uluslararası boyutta ele alan Bilgisayar Olaylarına Müdahale Ekibi (BOME) kurulmuştur. SGE aynı zamanda Ar-Ge, Danışmanlık ve BOME çalışmalarında

[109] Ulusal Bilgi Güvenliği Kapısı, http://www.bilgiguvenligi.gov.tr/hakkimizda.html Erişim, 30/05/2013

kazandığı deneyimi talepler doğrultusunda verdiği eğitimler aracılığı ile kurumlara aktararak bilinçlenmeye katkıda bulunmaktadır[110].

TÜBİTAK BİLGEM ve Bilgi Teknolojileri ve İletişim Kurumu koordinasyonunda, 25-28 Ocak 2011 tarihleri arasında bilgi teknolojileri ve iletişim, finans, eğitim, savunma, sağlık sektörlerinden; adli birimler, kolluk kuvvetleri ve çeşitli bakanlıklardan, özel sektör ve sivil toplum kuruluşlarından oluşan 41 kurum ve kuruluşun temsilcilerinin katılımıyla 1. Ulusal Siber Güvenlik Tatbikatını gerçekleştirmiştir. Tatbikatla, Türkiye'de siber güvenlik konusunda idari, teknik ve hukuki kapasitenin geliştirilmesi, kurumlar arasında bilgi ve tecrübe paylaşımına ve başta yönetim seviyesinde olmak üzere tüm kademelerde farkındalık oluşumuna önemli katkılar sağlanması ve kurumların bilgisayar olaylarına müdahale yeteneğinin tespit edilmesi amaçlanmıştır[111]. (TÜBİTAK-BİLGEM, 2011)

Ulaştırma Denizcilik ve Haberleşme Bakanlığı Koordinesinde, TÜBİTAK ve BTK tarafından 25 Aralık 2012-11 Ocak 2013 tarihleri arasında 2. Ulusal Siber Güvenlik Tatbikatı 61 kurum ve kuruluşun katılımıyla gerçekleşmiştir[112]. 8 aşamadan oluşan tatbikatın, İlk 6 aşamasında kurum ve kuruluşlara gerçek siber saldırılar düzenlenmiştir. Her kurum kendi sistemini savunurken, olası açıklar tespit edilmeye çalışılmıştır. Tatbikatın son 2 aşaması ise, tüm kurum ve kuruluşların katılımıyla Ankara'da yapılmıştır. Bu aşamada gerçek saldırılarla denenme imkanı olmayan saldırılar yazılı senaryolarla test edilmiştir.

Tatbikatlar sonucunda hazırlanan raporlarla siber güvenlik konusundaki eksiklikler ve bilişim sistemindeki açıklar tespit edilmiştir. Tatbikatlar sayesinde siber saldırılara karşı önlemlerin alınmasına ve kurumların bilişim sistemlerinin güçlendirilmesine, kurumlar arası koordinasyonun arttırılmasına fayda sağlamıştır.

---

[110] http://www.uekae.tubitak.gov.tr/sid/107/index.htm Erişim, 11/05/2013

[111] Ulusal Siber Güvenlik Tatbikatı 2011 Sonuç Raporu, http://www.bilgiguvenligi.gov.tr/raporlar-kategorisi/ulusal-siber-guvenlik-tatbikati-2011-sonuc-raporu.html Erişim, 12/05/2013

[112] 2. Ulusal Siber Güvenlik Tatbikatı Başarıyla Tamamlandı, http://www.tubitak.gov.tr/tr/haber/2-ulusal-siber-guvenlik-tatbikati-basariyla-tamamlandi Erişim, 12/05/2013

TÜBİTAK ile NATO'nun NCIA ajansı arasında Ar-Ge alanında işbirliği anlaşması imzalanmıştır[113]. Bu anlaşma ile iki kurum arasında bilimsel bilgi değişimi, ortak Ar-Ge çalışmaları ve danışmanlık, komuta, kontrol, iletişim, haber alma, gözetleme, keşif alanında ve teknoloji geliştirme konularında çalışmalar gerçekleştirmek amaçlanmıştır.

§ 8. SONUÇ

Nükleer silahların icadından sonra stratejinin oluşturulması ve geliştirilmesi 15 yıl sürmüştür. Bu süre içerisinde nükleer savaşlar çıktı çıkıyor derken nükleer silah stratejisi ile durum kontrol altına alınabilmiştir. Şu anda aynı sorun, siber ortam stratejilerinin belirlenmesinde yaşanmaktadır. Stratejilerin geliştirilmesi ve olgunlaştırılması uzun bir süre alabilir ancak siber tehlikeler kontrol ve denetim altına alınabilir.

Ulusal savunma önlemleri siber tehlikelerin zararını hafifletecektir. Öncelikle ülkelerin kritik alt yapılarının internetten bağımsız ağ ile çalışması sağlanabilir. İntranet sistemi internetten gelebilecek saldırıların önüne geçmek için uygulanabilir. Ulusal güvenlik politikaları belirlenerek yerli yazılımlara ağırlık verilmelidir. Yabancı ülkenin üretmiş olduğu yazılım güvenli olmayabilir. Kritik alt yapı sistemlerinde ve yazılımlarında, ulusal ürünler kullanılarak casusluk ihtimali zayıflatılabilir. Güvenlik açıklarını ve tehlikeleri belirlemek için saldırı tehdit algılama mekanizmaları kullanılmalı ve güçlendirilmelidir. Ulusal siber tatbikat çalışmalarının önemi vurgulanarak, genel katılım sağlanılabilir. Siber savunma stratejilerinde üniversitelerin ve özel kurumların desteği arttırılabilir.

Ulusal güvenliği tehdidi yanı sıra ticari sırları ele geçirmeye yönelik siber saldırılar ülkelerin ekonomisini sarsan unsurlardan biri olmuştur. Finans sektörü, bankalar, finansal işlemler siber ağ alt yapısı ile devamlığını yürütmektedir ve siber güvenliği sarsan tehlikelerden etkilenmektedir. SCADA sistemlerine

---

[113] TÜBİTAK ile NATO Arasında İşbirliği Anlaşması İmzalandı. http://www.tubitak.gov.tr/tr/haber/tubitak-ile-nato-arasinda-isbirligi-anlasmasi-imzalandi Erişim, 25/05/2013

yapılacak saldırılar, insan yaşamının devamlılığını sağlayan suyun bile elde edilememesi gibi tehlikelere yol açabilir. Her bireyi ilgilendirebilecek, neticelerle sonuçlanan saldırılar mümkündür.

Ülkelere maliyeti yüksek zararlar veren ve ulusal güvenliği tehlikeye atan saldırılar için uluslar arası işbirliği şarttır. Saldırı merkezleri yanıltıcı olabilmektedir. Siber saldırılarda, saldırıyı yapan ve saldırının kaynağı olan ülke farklı olabilmektedir. Bu nedenle hiçbir sorununuz olmayan bir ülkeden gelen saldırılar, aslında saldırının kaynağını şaşırtmak için yapılmış ya da ülkelerin birbirine düşmesini sağlamak amacıyla üçüncü bir taraf aracılığıyla yapılmış olabilir. Bu durum ülkeler arasında kısa zamanda büyük krizlere neden olabilir. Siber saldırılarda kaynağı belirlemek zordur ancak imkânsız değildir. Bu nedenle uluslar arası işbirliğine ve örgütlenmeye ihtiyaç vardır. Bu örgütlenme çerçevesinde kurulacak laboratuar ve araştırma merkezleri sayesinde uluslar arası soruşturmalar ve cezalandırmalar düşünülebilir.

Siber ortam çalışmalarında, öncelikle ulusların şeffaflık ilkesi ile hareket etmesi gerekmektedir. Ülkeler, siber savunmalarını ordu içinde yapılandırmaya başlamıştır. Ancak genellikle ülkeler yapılandırmış oldukları sistemleri gizlilik içinde yürütmektedir. Ülkelerin, birbirinden gizledikleri yapılanmaları, birbirlerine karşı korku ve şüphelerin artmasına neden olmaktadır. Korku ve şüphenin sonucu olarak, güçlü ve tehlikeli siber silahlar geliştirilmektedir.

Uluslar arası koordinasyon sağlanmalı ve ülkeler aynı görüş etrafında toplanmalıdır. Oluşturulacak kurallar çerçevesinde, saldırılara meydan verilmemelidir. Ulusların savunma sistem yapılanmasında, ordu içinde kurulacak birimler konusunda şeffaf olunmalıdır. Ülkeler, SCADA sistemlerine yönelik saldırılardan men edilmelidir. Siber ortam sorunları, uluslar arası şeffaflık sağlanarak ve belirlenecek kurallar çerçevesinde kontrol altına alınmalıdır.

Özgeçmiş

1979 yılında Aksaray'da doğdum. İlk, orta ve lise eğitimimi doğduğum şehirde tamamladım. Cumhuriyet Üniversitesi Meslek Yüksek Okulu Sigortacılık Programından 2000 yılında mezun oldum. Anadolu Üniversitesi İşletme Bölümünden 2008 yılında mezun oldum. Bir süre ortaokul ve lisede öğretmenlik yaptım. 2005 yılından bu yana Adalet Bakanlığı taşra teşkilatında görev yapmaktayım.