Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler

Significance of Cyber Security for National Security: A Study Concerning the Necessary Measures

Mehmet Nesip ÖĞÜN[*] ve Adem KAYA[**]

Öz

Teknoloji insanların günlük yaşamına her alanda daha fazla nüfuz etmektedir. İnternet, kolaylık sağlayan bir araç olmanın ötesine geçmiş ve birçok alanda kullanılması zorunlu bir vasıta halini almıştır. Yaşamımızın İnternet ile bu ölçüde bütünleşik hale gelmesi kişisel bilgilerimizi de aynı ölçüde tehlikeye sokmaktadır. Benzer şekilde kamu kurumlarındaki veri tabanları ve gizli bilgilerden, enerji santrallerine, su dağıtım şebekelerinden, iletişim ağlarına ve seyrüsefer sistemlerine kadar birçok kamu kuruluşu ve hizmeti de tehlike altına girmektedir. İnternet kullanımının ve teknolojik gelişmelerin akıl almaz bir hızla ilerlediği günümüzde her an kişisel bilgisayarlarda ve kurumlarda yer alan kişisel bilgilere, banka hesaplarına ve yaşanılan ülke için hayati öneme sahip olan kritik altyapılara karşı ciddi saldırı ve tehditler gündeme gelmektedir. İnternet ortamında, olayların saniyelerle ifade edebilecek zaman dilimleri içerisinde meydana geldiği de göz önünde bulundurulursa etkin ve güçlü savunma sistemlerinin inşa edilmesi, farkındalık ve bilinç oluşturulmasının önemli ortaya çıkacaktır. Göreceli olarak yeni bir alan olmasına rağmen, konu üzerinde yapılan çalışmalar sayı bakımından fazla ve içerik bakımından geniştir. Bu çalışmada siber güvenlik kavramı, milli

[*] Dr. Bnb., KKTC Güvenlik Kuvvetleri Komutanlığı, E-posta: nesip75@yahoo.com.
[**] J.Yzb., 23. Jandarma Sınır Tümen K.lığı, Şırnak, E-posta: adem200128@gmail.com.

güvenlik açısından önemi ve elde edilen bütün bulgulardan hareketle, kişisel, kurumsal ve ulusal düzeyde alınabilecek önlemlere dair öneriler ortaya konmuştur.

Anahtar Kelimeler: *Siber, Milli, Güvenlik, İnternet, Web.*

Abstract

Technology is constantly progressing and it has begun to impact our daily lives to an alarming extent. Internet passed beyond being a facility tool and began an important medium that is actually necessary. Thus, Internet and our daily lives integrated and imperil our personal information, of equal degree. From databases and private information that stored in governmental institutions, to power plants, waterworks, communications networks and navigation systems; many governmental institutions and services are in danger now. Superfluity of threats, dangers and consequences, all became a non-ignorable reality. Adding this reality the data transfer speed, it will come into light that building effective and strong defence systems, creating an awareness and consciousness on the matter are of great importance. Although it is a relatively new field, there are excess studies and wide range of content on the subject. Setting out all evidences, a final assessment that show the significance of cyber security for national security has been made in this study. Suggestions on the precautions have also been presented in all individual, institutional and national level.

Key Words: *Cyber, National, Security, Internet, Web.*

Giriş

Halen dünya üzerinde 2,3 milyar internet kullanıcısı bulunmaktadır.[1] Günümüzde İnternetten daha hızlı gelişen tek şey

[1] Internet World Stats İnternet Sayfası, **World Internet Users and Population Stats**, <http://www.internetworldstats.com/stats.htm>, 18.05.2013.

cep telefonu teknolojisidir.[2] Cep telefonu teknolojisi de bu hızlı gelişimini İnterneti kullanmasına borçludur.

İnternet kullanımında güvenlik, İnternetin tasarımından daha sonra ortaya çıkmış olan bir olgudur. İnternetin yapısı erişim odaklıdır; başka bir ifadeyle İnternet tasarlanırken kullanım kolaylığı, düşük maliyet ve evrensellik ilkeleri göz önünde bulundurulmuş, bu teknolojiyi kullananların bu yapıya zarar verecekleri düşünülmemiştir.[3]

İnternet kullanımı ve teknolojinin hızla geliştiği günümüzde daha etkin ve güçlü savunma sistemlerinin inşa edilmesi, acil durum hazırlığı ve bunların kullanım süreçlerinin oluşturulması çok önemlidir. Saldırıların, gerçekleştiği ilk anda tespit edilmesi, sanal ya da fiziksel bariyer inşa edilmesi, ulusal ve bölgesel siber güvenlik politikalarının geliştirilmesi siber güvenliğin sağlanması için zorunlu hale gelmiştir.[4]

Siber güvenlik göreceli olarak yeni bir alan olmasına rağmen konu üzerinde çok sayıda çalışma yapılmaktadır.[5] Yapılan çalışmaların sadece başlıklarına bile bakıldığında bunların büyük kısmının teknoloji temelli olduğu ve sistem ve ağ yöneticilerine hitap ettiği görülmektedir.

Siber güvenlik konusunun, daha çok kullanıcılara hitap eder

[2] Seymour E. Goodman, "Critical Information Infrastructure Protection", Terrorism (Ed.), ***Responses to Cyber Terrorism NATO Science for Piece and Security***, IOS Press (Cilt 34), Ankara, 2008, p. 25.
[3] Seymour E. Goodman, A.g.e., pp. 25-26.
[4] Seymour E. Goodman, A.g.e., pp. 27, 31.
[5] EBSCO Host İnternet Sitesi, **Library, Information Science & Technology Abstracts**, <http://web.ebscohost.com/ehost/results?sid=81216314-aa32-45bd-9479-d9e0a32310bb%40sessionmgr110&vid=9&hid=108&bquery=cyber+security&bdata=JmRiPWx4aCZ0eXBlPTAmc2l0ZT1laG9zdC1saXZl>, 11.07.2013; GOOGLE AKADEMİK İnternet Sitesi. **Cyber Security**, <http://scholar.google.com.tr/scholar?hl=tr&q=cyber+security&btnG=&lr=>, 11.07.2013; JSTOR İnternet Sitesi. **JSTOR: Search Results Cyber Security**, <http://www.jstor.org/action/doBasicSearch?Query=cyber+security&acc=off&wc=on&fc=off>, 11.07.2013.

şekilde işlendiği ya da farklı bir ifadeyle konunun farkındalık ve eğitim boyutuyla ele alındığı çalışma sayısı çok azdır. Bu nedenle siber güvenliğin bu boyutlarıyla ele alındığı çalışmalara olan ihtiyaç artmaktadır. Son derece donanımlı bir ağ yöneticisinin tüm uğraşlarını bilinçsiz bir kullanıcı bile bir seferde boşa çıkarabilir. Artık İnternet bağlantı hızının GB'lar (Gigabyte) ile ifade edildiği göz önünde bulundurulduğunda, büyük gayretler sonucu çaba ile sıkı şekilde örülen bir güvenlik ağında bilinçsiz bir kullanıcının yaratacağı anlık bir boşluk, tüm kurumsal bilgilerin istenmeyen ellere geçmesine ya da geçebilecek bir ortam oluşmasına fırsat verebilir. Bu noktadan hareketle bu konu üzerinde çalışma yapmanın ihtiyaç ve önemi ortaya çıkmaktadır. Son zamanlarda yeni ortaya çıkmaya başlayan "Siber Güvenlik Durumsal Farkındalık" (Cyber Security Situational Awareness) çalışmaları bu ihtiyaca hitap etmekte ve çalışmalarda artış olması beklenmektedir.[6]

Siber güvenlik, içerik itibarı ile bilgisayar sistemleri ve genel olarak teknoloji ile çok iç içe geçmiş olup, teknik boyutları birçok farklı çalışmanın konusunu teşkil ettiğinden siber güvenliğin teknik ayrıntıları ele alınmamış, özet bilgiler sunulmakla yetinilmiştir.

Konunun doğası gereği gizli kalan ve erişime açık olmayan bilgiler bulunduğundan sadece açık bilgi kaynaklarından faydalanılabilmiştir.

İnternetin ulusal sınırları aşan ve fiziksel olarak sınırlandırılamayan yapısı aynı zamanda uluslararası ilişkiler konusuna girmektedir. Bu da kendi içerisinde birçok alt dallara ayrılabilecek başka çalışmaların konusunu teşkil etmektedir. Çalışmada İnternetin uluslararası boyutu sadece siber güvenliğin sağlanmasına yönelik olarak ulusal ve uluslararası kuruluşların yürüttüğü işbirliği örneklerinin sunulması ile sınırlı olarak ele alınmaktadır.

[6] Sushil Jajodia and Peng Liu, et all. (Ed.), ***Cyber Situational Awareness***. New York, Springer, 2010, p. V.

İnternetin Tarihçesi

İnternet ortamında güvenlik ihtiyacı zamanla ortaya çıkmış ve gelişmelere paralel olarak yeni saldırı ve savunma teknikleri ile önemini artırmıştır. Güvenlik kavramının bu alandaki gelişimi hakkında fikir oluşturması bakımından İnternetin tarihine kısaca değinmekte fayda vardır.

Başlangıçtaki temel maksadı iletişimi sağlamak olan İnternetin tarihi, 1837 yılında telgrafın icadına kadar geri götürülebilmektedir.[7] Daha sonraları iletişim için Atlantik ötesi kablolar çekilmesi[8] iletişimde mesafe kavramını yavaş yavaş ortadan kaldırmaya başlamıştır. İlk zamanlarda kod çözme maksatlı olarak üretilen ve hacmi bir ofis büyüklüğünde olan bilgisayarların zaman içerisinde geliştirilmesiyle teknolojide yeni bir çığır açılmıştır.[9]

Rusya'nın aya uydu göndermesi sonucu geri kaldığını düşünen[10] ve araştırma birimi kuran ABD, nükleer bir saldırı durumunda tek bir merkeze bağlı kalmadan iletişimin kesintisiz bir şekilde yürütülmesini sağlayacak bir sistem üzerinde çalışmaya başlamıştır.[11] Bu çalışmalar bugünkü anlamda İnternetin oluşmaya başlamasını sağlamıştır. Devlet tekelinde olan bu iletişim biçiminin idaresi daha sonraları 1990'ların başında sivillere devredilmiştir.[12]

İnternetin ilk zamanlarında bir filtreleme veya yönetim sistemi olmaksızın ortaya çıkan bilgi paylaşımı büyük bilgi kaynağı

[7] Clare Cridland, "The History of the Internet: The Interwoven Domain of Enabling Technologies and Cultural Interaction", Terrorism (Ed.), ***Responses to Cyber Terrorism NATO Science for Piece and Security***, IOS Press (Cilt 34), Ankara, 2008, p. 1.
[8] Clare Criland, A.g.e., p. 1.
[9] Brian Randell, **"A History of Computing in The Twentieth Century-The Colossus"**, <http://www.cs.ncl.ac.uk/publications/books/papers/133.pdf>, 16.04.2012,
[10] Emre Bakır, "İnternet Güvenliğinin Tarihçesi", ***TUBİTAK Bilgem Dergisi***, Yıl 2011, Cilt 3, Sayı 5, Sayfa 6-17, s. 8
[11] Gabriel Weimann, ***Terror on The Internet: The New Arena The New Challenges***, Washington D.C., United States Institue of Peace, 2006, p. 5.
[12] Clare Cridland, A.g.e., p. 1.

artışı meydana getirmiş, bu durum medyanın bilgi kaynağı olma tekelini kırmıştır.[13] İnternet artık kişilerin İnternet erişiminin bulunduğu dünyanın her yerine yayın yapmalarına olanak tanımıştır. Ancak, medya filtrelemesinin olmaması komplo teorilerinin yaygınlaşmasına sebep olmuştur.[14] RSS (Really Simple Syndication) beslemeleri İnternet kullanıcılarının web sitelerini ziyaret etmeden, istenen bilgilerin güncel şekillerine erişmelerine olanak sağlamıştır. Bu da internette popüler olana erişimi kolaylaştırmıştır. Bu tespitler İnternetin gelecekteki mimarisini yasaların ve sansürün şekillendireceğini göstermektedir.[15]

Güvenlik Kaygılarının Ortaya Çıkışı

Oluşturulma maksadı iletişim olan İnternette temel felsefe bilgi paylaşımı olarak ortaya çıkmıştır.[16] Bu sistemden faydalananların sisteme zarar verebilecekleri ya da vermek isteyecekleri başlangıçta kimsenin aklına gelmemiş dolayısıyla bu ortamda güvenlik kaygıları olmamıştır.[17] Güvenlik kaygısı olmamasına bir etken de başlarda bu sistemi kullananların sayısının sınırlı olması ve bilgisayarların her eve girebilecek kadar yaygın olmayışıdır.

Bugün kullanıcı sayısının 2,3 milyara[18] yaklaştığı İnternette zamanla birtakım kaygılar belirmeye başlamıştır. İlk zamanlarda yaşanan endişeler İnternetin üzerinde var olduğu fiziksel altyapıya karşı gelebilecek tehditlerden ibaretken sonraları zararlı kodlar ve virüslerin üretilmesi ve yaygınlaşmasıyla beraber tehlikenin seviyesi de artmaya başlamıştır.[19]

Zamanla ekonomik sistemlerin, ticaretin ve bilgi sistemlerinin

---

[13] Clare Cridland, A.g.e., p. 3.
[14] Clare Cridland, A.g.e., p. 4.
[15] Clare Cridland, A.g.e., p. 3-6.
[16] University System of Georgia İnternet Sitesi, **A Brief History of the Internet**, <http://www.usg.edu/galileo/skills/unit07/internet07_02.phtml>.
[17] Seymour E. Goodman, A.g.e., p. 25.
[18] Internet World Stats İnternet Sayfası, A.g.y.
[19] Clare Cridland, A.g.e., p. 6.

İnternete entegre ve bağımlı hale gelmeleri ile ve de teknolojide yaşanan gelişmelerin sistemlere yetkisiz erişim, bilgi hırsızlığı ve hatta fiziksel zararlar vermeye olanak sağlamasıyla siber alanda güvenlik ciddi bir sorun olarak karşımıza çıkmıştır.

İnternet kullanımıyla ortaya çıkan bir problem de gerçeğin görüşlerden ayrılması sorunu olmuştur.[20] Herkesin yayıncı olarak yer alabildiği ortamda gerçeklerle görüşler öylesine iç içe geçmektedir ki, gerçeği görüşten ayırmak neredeyse imkânsız hale gelmektedir.

Siber güvenlik konusunda karşılaşılan en büyük problemlerden biri, özgürlük ile güvenliğin dengelenmesidir.[21] Siber ortamda güvenlik sağlanmaya çalışılırken, asıl maksadı bilginin özgürce paylaşımı ve iletişim olan İnterneti maksadının dışına çıkarmamak gerekmektedir. Güvenlik gerekçeleri ile hükümetlerin, kişilerin özel bilgilerine eriştiği ve telefon ve İnternet iletişimlerini takip ettiğini ortaya çıkaran gelişmelerden sonra İnternet kullanıcıları arasında ciddi kaygılar oluşmuştur.[22]

İnternet altyapısına gelebilecek fiziki zararlar kullanıcılara yönelik tehdit meydana getirmektedir. Aynı şekilde zararlı kodlar ve virüsler de İnternet kullanımını kısıtlamaktadır.[23] Siber suçların her yıl dünya ekonomisine verdiği zarar yaklaşık 1 trilyon dolar civarındadır.[24]

Siber Güvenliği Tehdit Eden Unsurlar

Siber güvenliği tehdit eden saldırı vasıtaları çok çeşitlidir. Bu, bazen bir virüs, solucan, Truva atı veya casus yazılım olabileceği

---

[20] Clare Cridland, A.g.e., pp. 3,4.
[21] Gabriel Weimann, A.g.e., p. 12.
[22] John Humprhrys, **State Cyber-Snooping: How worried should we be?**, <http://yougov.co.uk/news/2013/06/11/state-cyber-snooping-how-worried-should-we-be/>, 14.07.2013.
[23] Clare Cridland, A.g.e., p. 6.
[24] Robert K. Kane, ***Internet Governance in an Age of Cyber Insecurity,*** Council Special Report No. 56, 2010 <http://i.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf>, 28.02.2012, p. 5.

gibi, bazen de kendisini bir bankanın resmi sitesi olarak gösteren birebir kopya ve sahte bir İnternet sitesi olabilir. Ayrıca bireyleri de siber saldırıların hem vasıtası, hem de hedefi olarak görebiliriz. Bilinçsiz bir kullanıcının ilgi çekici bir bağlantıya tıklaması bilgisayarındaki verileri ve bilgisayarını bir korsanın eline teslim etmesi demek olabileceği gibi, aynı zamanda bilgisayarının çok ciddi bir suçta kullanılarak bu suça aracı ve ortak olması anlamına da gelebilmektedir.

Siber alanda ortaya çıkan tehditler sadece fiziksel varlıklara gelebilecek zararlar, bilgi hırsızlığı ve casusluk ile sınırlanamaz. İletişim vasıtası olarak kullanılan İnternetin bilgi çarpıtma ve propaganda maksatlı olarak kullanımı da dolaylı olarak zararlar meydana getirmektedir. Bunu da siber güvenliğin bir boyutu olarak ele almak gerekmektedir.

Siber güvenlik sadece bir saldırı ve bunun sonucunda verilecek bir zarar veya elde edilecek haksız bir kazanç demek değildir. İnternetin siber teröristler tarafından bir iletişim ve propaganda aracı olarak kullanılması da siber güvenlik konusu içerisine girmektedir.

Bu duruma benzer bir şekilde, istenmediği halde gönderilen elektronik postalar da bu mahiyette değerlendirilmektedir. Bunlar bazen sadece bir reklam, bir ürün pazarlama şekli ve bazen de propaganda aracı olabilmekte iken, bazen de posta eklerinde yer alan dosyalarda bireysel ve ülke varlıklarına çok ciddi zararlar verebilecek virüs, Truva atı ya da SCADA sistemlerini hedef almış yazılımlar bulunabilmektedir. Bu yolla zararlı yazılımlar kendilerini bilgisayardan bilgisayara, ülkeden ülkeye yayabilmektedirler.

Siber ortamda meydana gelen güvenlik açığı ve zafiyetlerin sıralandığı CVE (Common Vulnerabilities and Exposures) listesine her ay ortalama 100 yeni kayıt girilmektedir.[25] Bu da günümüzde bu

[25] Kenneth Geers, **"Cyberspace and the Changing Nature of Warfare"**, Centre of Excellence Tallinn, Estonya, <http://www.blackhat.com/presentations/bh-jp-

açıklıkları kullanacak olan aktörlerin ellerinde bulundurdukları veya oluşturmakta oldukları saldırı araçlarını kullanabilecekleri ortam ve güvenlik açıklarının ne kadar fazla olduğunu ve bunun yeni güvenlik güncelleme ve yazılımları ile tamamen ortadan kaldırılamayacağını, her yeniliğin beraberinde yeni açıklık ve istismarlar getireceğini göstermektedir.

Siber Güvenlik Tehdit Araç ve Yöntemleri

Siber ortamda karşılaşılabilecek ve teknik detayları başka çalışmaların konusu olabilecek başlıca saldırı araç ve yöntemleri arasında virüsler, Truva atları, kurtçuklar (worms), zombie ve botnetler, istem dışı elektronik postalar (spam), klavye işlemlerini kaydeden programlar (key loggers), casus yazılımlar (spyware), servis dışı bırakma (DoS), aldatma (IP spoofing), şebeke trafiğinin dinlenmesi (sniffers), yemlemeler (phishing) ve propaganda sayılabilir.[26]

Virüsler

Virüs, bilgisayar dünyasında on yıllardır karşılaşılan bir terimdir. Bu terim genellikle zararlı yazılımları ifade eden kapsayıcı genel bir ifade olarak kullanılmıştır, ancak bu kullanım yanlıştır. Her tür zararlı yazılım virüs olarak ifade edilemez. Virüs diğer dosyalara bulaşarak yayılan özel bir zararlı yazılım türünü ifade etmektedir.[27] Kayıtlara geçen ilk virüs 1986 yılında ortaya çıkan IBM-PC tabanlı "*Brain*" ismi verilen bir *boot sector* virüsüdür.[28]

08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf>, 28.02.2012.

[26] Kenneth, Geers, A.g.m.; Mustafa Ünver ve Cafer Canbay, "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", ***Elektrik Mühendisliği***, Yıl 2010, Sayı 438, Sayfa 94-103, <http://www.emo.org.tr/ekler/a9a502d6e646c25_ek.pdf?dergi=598 >, 11.04.2012; Sait Yılmaz ve Olcay Salcan. ***Siber Uzay'da Güvenlik ve Türkiye***, İstanbul, Milenyum Yayınları, 2008.

[27] James Graham and Richard Howard, et all, ***Cyber Security Essentials***, Boca Raton, Auerbach Publications, 2010, pp. 198, 199.

[28] James Graham and Richard Howard, et all, A.g.e., pp. 198, 199.

Truva Atları

Faydalı bir fonksiyonu varmış gibi görünen fakat aynı zamanda gizli ve güvenlik mekanizmalarını aşabilecek potansiyel zararlı fonksiyon içeren ve bazen bir sistem biriminin meşru olarak yetkilendirilmesini istismar eden bir bilgisayar programı olarak tanımlanmaktadır.[29] Genellikle ücretsiz olarak sunulan yazılımlarla birlikte sisteme bulaşmaktadırlar. Truva atlarından korunmanın en iyi yolu kaynağı bilinmeyen yazılımların sisteme yüklenmemesidir.

Kurtçuklar (*Worms*)

Kurtçuklar da, tıpkı virüslerde olduğu gibi, kendini bir cihazdan başkasına kopyalamak üzere tasarlanmışlardır, ancak bunu kendi başlarına gerçekleştirmektedirler. Öncelikle bilgisayarda dosya veya veri transferi yapan fonksiyonların denetimini ellerine geçirip bir kez sisteme bulaştıktan sonra kendi kendine yollarına devam edebilirler. Kurtçukların en göze batan tehlikesi, büyük miktarlarda çoğalma yetenekleridir. Kullanıcıların veri ve dosya alışveriş yöntemlerini kullanarak kendilerini, irtibat halinde olunan tüm bilgisayarlara, tüm e-posta adreslerine gönderebilmektedirler. Bu da ağ trafiğinin önemli derecede yavaşlamasına neden olabilmektedir. Bir solucan yeni çıktığında, daha güvenlik yazılımları tarafından tanınmadığı için ilk etapta ağ trafiğini önemli oranda yavaşlatabilmektedir.[30]

Solucanlar genel olarak kullanıcı müdahalesi olmadan yayılmakta ve kendilerinin birebir kopyalarını ağdan ağa dağıtmaktadırlar. Kurtçuklar yayılmak için bir taşıyıcı programa veya dosyaya ihtiyaçları olmadığı için sistemde bir tünel de açabilmekte ve başkasının, bilgisayarınızın denetimini uzaktan eline

[29] Richard Kissel (Ed.), ***Glossary of Key Information Security Terms***, National Institute of Standards and Technology, 2011, <http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf>, 08.03.2012, p. 196.

[30] Microsoft İnternet Sitesi, **Virüsler**, <http://windows.microsoft.com/tr-TR/windows-vista/Viruses-frequently-asked-questions>, 17.04.2012.

geçirmesine olanak sağlayabilmektedir.[31]

Karıştırılan terimler oldukları için virüsleri, Truva atları ve kurtçuklardan ayıran özelliği burada vurgulamakta fayda bulunmaktadır: Truva atları zararsız birer yazılım gibi görünmekte ve bir sistemde istismar edeceği bir durum ortaya çıktığında (bilgisayarın İnternete bağlanması gibi) devreye girmekte, diğer zamanlarda sisteme herhangi bir müdahalede bulunmamaktadır. Kurtçuklar ise ağda kendilerini yayabilen kendi başlarına birer programdırlar. Bunların aksine virüs, bulaşmak için kendine yeten bir program değildir. Kendini başka dosyalara ilave ederek yayılır ve eğer virüslü dosya açılmazsa virüs başka ortamlara yayılamaz.

Zombi Ordular (*Botnetler*)

Zombi bilgisayarlar ya da *botnetler* bu tehdit grubunun en tehlikeli olanları olarak kabul edilebilir. Burada önemli olan nokta, bilgisayar kullanıcısının hiçbir haberi olmaksızın bilgisayarının çok ciddi suçlar işlenmesinde kullanılabilmesidir. Bu tür bilgisayarlar *robot* veya *bot* şeklinde de ifade edilmektedir.

Zombi ordunun bir parçası haline gelen bilgisayarlarda buna sebep olan nokta, genellikle bu tür bilgisayarların *firewall* denilen güvenlik duvarlarının olmamasıdır. Günümüzde bant genişliğinin artmasıyla beraber herhangi bir korunmaya sahip olmayan bir bilgisayar kolaylıkla bir *botnet*'in parçası haline gelebilir. Bir *botnet*, genellikle açık bırakılan bir kapıdan (*port)* bir bilgisayara, daha sonra aktif hale gelecek şekilde, Truva atı bırakılması sonucu oluşturulmaktadır. *Botnet*'in parçası haline gelen bilgisayarlar mesela bir web sitesine aynı anda yönlendirilerek bu siteyi hizmet veremez hale getirmek için kullanılabilmektedir.[32]

[31] Bilgiportal İnternet Sitesi, **Virüs, Solucan ve Truva Atı Nedir?**, <http://www.bilgiportal.com/v1/idx/19/2480/Gvenlik/makale/Virs-solucan-ve-Truva-at-nedir.html>, 17.04.2012.

[32] SearchSecurity İnternet Sitesi, **Botnet (Zombie Army)**, <http://searchsecurity.techtarget.com/definition/botnet>, 17.04.2012.

*Botnet'*in parçası olan bir bilgisayar suç unsuru olan dosya ve görüntülerin yayılmasında, istenmeyen elektronik posta olarak tanımlanan *spam* faaliyetlerinde, şahsi bilgilerinizin, internet ve banka hesaplarınıza ait bilgi ve şifrelerin ele geçirilmesinde kullanılabilmektedir. Ele geçirilen bu bilgiler de sizin adınız ve paranız kullanılarak çok ciddi suçların işlenmesine aracılık edebilir.[33]

İstem Dışı Elektronik Postalar (*Spam*)

İstem dışı elektronik postalar *(Spam)*, istenmediği halde gönderilen e-postalara verilen isimdir. Günümüzde istem dışı elektronik postalar hala büyük karmaşa yaratmaktadır. İnternet üzerinden gönderilen e-postaların yüzde sekseni istenmeyen e-posta kategorisine girmektedir.[34]

İstem dışı elektronik posta olarak gönderilen e-postaların çoğunluğu, reklam maksadıyla gönderilenler olmakla birlikte, bunların dışında bilgisayarlara zararlı yazılımlar bulaştırmak ve bir konuda propaganda yapmak gibi maksatlarla da gönderilmektedirler. İstem dışı elektronik posta olarak gelen e-postaları filtrelemek için filtre sistemleri olmakla birlikte e-postaların bu filtrelere takılmaması için değişik yöntemler kullanılmaktadır. Güvenliğimizi sağlamak ve zaman kaybını önlemek için kullandığımız elektronik posta filtreleri, zaman zaman, gelmesini beklediğimiz çok önemli bir postanın da elimize ulaşmasına engel olabilmektedir. Tüm bu sebeplerle istenmeyen elektronik postalar gelecekte de bizi rahatsız etmeye devam edecek gibi görünmektedir.[35]

[33] Alana Maurushat, **"Zombie Botnets"**, SCRIPTed, Cilt 7, Sayı 2, <http://www.law.ed.ac.uk/ahrc/script-ed/vol7-2/maurushat.asp>, 17.04.2012, p. 371.
[34] Michael O'Reirdan, **"Why Bother With Best Practices? Or Why Global Collaboration is Faster (and More Effective) Than a Speeding Bullet"**,***Cyber Security,*** New Europe (Special Edition), Sayı Mayıs-Haziran 2011, <http://www.scribd.com/doc/56702531/Cyber-Security-2011>, 20.03.2012,
[35] PERIMETEC İnternet Sitesi, **The Fututre of Spam**, <http://www.perimetec.com/all-about-spam/the-future-of-spam.php>, 15.07.2013.

Klavye İşlemlerini Kaydeden Programlar (*Keyloggers*)

Keylogger'lar kısaca klavye işlemlerini kaydeden programcıklardır. Bu programcıklar, farkına varılmadan klavyede dokunulan her tuşu kaydedip, fırsatını bulduklarında daha önce belirlenen adreslere bunları göndermektedirler. Özellikle bankacılık işlemlerinde klavyeden şifre girilmemesi, rakamlara tıklanarak veya rakamların üzerlerinde beklenerek şifreler girilmesi ve ayrıca cep telefonu ile SMS şifreleri yoluyla ilave güvenlik desteği sunulabilmesine rağmen İnternet üzerinden ticaret yapan birçok site, alıcıların kredi kartı bilgilerini girmesi için güvenlik seviyesi yüksek bu tür platformlar oluşturmamaktadır. Bu da klavyeden girilen bu bilgilerin nasıl kolayca başkalarının eline geçebileceğini göstermektedir. Bu durum, sadece alışveriş ve bankacılık işlemleriyle sınırlı değildir. Klavye işlemlerini kaydeden bu tür yazılımlar nedeniyle, e-posta ve sosyal paylaşım siteleri gibi kullanıcıların özel bilgilerinin yer aldığı web sitelerine ait kullanıcı adları ve şifrelerin ne kadar büyük tehlike altında olduğu anlaşılabilmektedir. Günümüzde sosyal medya ve çevrimiçi (*online*) oyunların ne kadar yaygın olduğu ve bunlar yüzünden meydana gelen cinayet ve intiharların ne kadar çok arttığı göz önünde bulundurulursa *keylogger*'ların meydana getirdiği asıl tehlike gerçek manasıyla anlaşılabilir.

Bu yazılımlar, aynı zamanda aldatan bir eşi takip etmede, işverenlerin çalışanlarını izlemesinde veya bir çocuğun bilgisayarda neler yaptığının gözlenmesinde kullanılabilmektedir. Bu programlar, maksatlı kişiler tarafından bilgisayarlara doğrudan fiziksel erişim sağlanarak veya İnternete bağlı olan bir bilgisayardaki açıklıklar kullanılarak sistemlerin içerisine kurulabilir.[36]

[36] Kishore Subramanyam and Charles E. Frank et all, **"Keyloggers: The Overlooked Threat to Computer Security"**, <http://www.keylogger.org/articles/kishore-subramanyam/keyloggers-the-overlooked-threat-to-computer-security-7.html#.T6GcbOs9XmQ>, 03.05.2012.

Keylogger'lar küçük programcıklardır ancak bunlar sadece yazılım olarak değil donanım olarak da var olabilmektedirler ve kullanıcılar ve sistemler bunların farkına varamamaktadırlar. Bu tür klavye hareketlerini kaydeden donanımlar fiziksel olarak klavye ile bilgisayar arasına monte edilmekte ve bilgisayar kasasının arka kısmına gizlenmektedir. Yapılan araştırmalarda ne kullanıcılar, ne de sistemler bu kaydedicileri fark etmiştir. Hazırlanmaları ve kurulumları çok basit olan bu tür cihaz ve yazılımların varlıklarına karşı dikkatli olunması gerekmektedir.[37]

Casus Yazılımlar (*Spyware*)

Casus yazılımlar klavye hareketlerini kaydedebilir, şifreleri, banka hesap bilgilerini ve özel dosyalarınızı çalabilirler.[38;39]

Casus yazılımlar genel olarak bedava deneme sürümlerinin içerisine enjekte edilmekte ve kullanıcılar tarafından bilgisayarlara kurulmaktadır. Bunlar genel olarak ebeveynler için çocuk izleme yazılımı, eş takip etme yazılımı gibi adlarla piyasaya sürülmektedir.[40] Eğer dikkatli okunursa bu tür yazılımların kurulmaları esnasında genellikle gerekli uyarılar yapılmakta, ancak uzun bir kullanıcı sözleşmesinin içerisindeki birçok hukuk teriminin arasında gözden kaçmaktadır. Genellikle kullanıcılar tarafından bu sözleşmeler okunmadan kabul edildiği için casusu yazılımlar kullanıcıların rızasıyla bilgisayarlara kurulmaktadır. Aynı şekilde bu tür yazılımlar kurulurken sunulan seçenekler hızlı ve gelişmiş seçenekler olarak ikiye ayrılmakta, kullanıcılar tarafından gelişmiş

[37] Kishore Subramanyam and Charles E. Frank et all, A.g.m.

[38] Robert McMillan. **Student Used Spyware to Steal Passwords, Change Grades**, <http://www.computerworld.com/s/article/9214898/Student_used_spyware_to_steal_passwords_change_grades>, 15.07.2013.

[39] John Wagley, **Court Shuts Site Selling Key Logging Spyware**, <http://www.securitymanagement.com/news/court-shuts-site-selling-key-logging-spyware-004868>, 17.07.2013.

[40] SpywareGuide İnternet Sitesi, **"Spyware"**, <http://www.spywareguide.com/term_show.php?id=12>, 03.05.2012.

seçeneklerin okunması ve ayarlanması bir zahmet ve zaman kaybı olarak algılandığından hızlı seçenekler tercih edilmektedir. Böylelikle kendi rızamızla özel bilgilerimiz başkaları tarafından ele geçirilmektedir. Aslında kullanıcılar tarafından gösterilecek özen ve dikkat birçok problemin oluşmasını engellemeye yetecektir.

Hizmet Dışı Bırakma (*DoS*)

Bu, basit bir şekilde tanımlamak gerekirse, bir sisteme kullanıcıların erişiminin engellenmesi, sistemin hizmet veremez hale getirilmesi anlamına gelmektedir. Temel mantığı, sahte istekler göndermek yoluyla, sistemi gerçek hizmet isteklerine cevap veremeyecek kadar meşgul kılmaktır. Hizmet dışı bırakmadan kastedilen bir diğer anlam ise saldırılar ile sisteme fiziksel olarak zarar verip sistemin hizmet sunamaz hale getirilmesidir.[41]

Aldatma (IP Spoofing)

Bilgisayarlar arasındaki bağlantı çeşitli protokoller aracılığıyla sağlanmaktadır. Bu protokoller aracılığıyla başka bir bilgisayara bağlanıldığında bağlanan bilgisayar kendi kimliğini karşı tarafa tanıtır. Bağlanılan bir bilgisayara gerçek IP adresinin gösterilmemesi yani asıl kimliğin gizlenmesine *IP spoofing* (Aldatma) denir. Sahte IP paketi alan bilgisayar, paketin gerçekten gönderilen adresten gelip gelmediğini bilemez. Bu genellikle başkasının IP adresinden mail gönderilmesi veya forumlara mesaj yazılması olarak karşımıza çıkmaktadır. Teoride bu durum mümkün olmakla birlikte pratikte karşıdaki sistem gerçekten ele geçirilmeden başkasının bilgisayarına farklı bir IP'den bağlanma gerçekleşemeyecektir. Günümüzde *IP spoofing* için kullanılan ticari ve ücretsiz yazılımlar bulunmaktadır. Aldatma genel olarak bir web sitesini işlemez hale getirmek için saldırı esnasında kaynağı gizleme maksadıyla kullanılmaktadır.[42]

[41] Lashan Clarke, **How Denial Of Service (DoS) Works?**, <http://www.brighthub.com/computing/smb-security/articles/30075.aspx>, 17.07.2013.
[42] BGA, **"Günümüz Internet Dünyasında IP Spoofing"**, <http://blog.bga.com.tr/network-security/gunumuz-internet-dunyasinda-ip-spoofing>, 03.05.2012.

Şebeke Trafiğinin Dinlenmesi (*Sniffing*)

Kelime anlamı koklamak olan *sniffing*, bir ağ üzerindeki bilgisayarlar arasındaki veri trafiğinin dinlenmesi anlamına gelmektedir. Bunu yapmak için internette bol miktarda yazılım bulunmaktadır. Şebeke trafiğinin dinlenmesinde mantık, yönlendiricilere gelen her paketin kabul edilmesi dolayısıyla iki bilgisayar arasındaki tüm verilerin yakalanarak saklanmasıdır. Bu, korsanların kullandığı en önemli yöntemlerden birisidir. Bu yöntemden korunmak için bilgisayarlar arasındaki bağlantıların şifreli olması gerekmektedir. Kriptolu paketler de elbette dinlenip ele geçecektir ancak içeriğinden bir şey anlaşılamayacaktır.[43]

Yemlemeler (*Phishing*)

Oltalama, oltaya düşürme ve yemleme gibi anlamlara gelen *phishing* bir web sitesinin sahtesinin yapılarak kullanıcılardan bilgilerini girmelerinin istenmesi yoluyla kişilere ait verilerin ele geçirilmesi şeklinde gerçekleşen bir dolandırıcılıktır.[44]

Yemlemede genellikle sahte siteye e-posta yoluyla kullanıcı çekilmektedir. Bilgilerini güncellemesi gerektiği ya da bir ödül kazandığı, ödülün gönderilebilmesi için kimlik ve adres bilgilerini girmesi gerektiği söylenen kullanıcı ilgili bağlantıya tıklayarak bilgilerini güncellemekte daha doğrusu güncellediğini zannetmektedir. Bu yolla elde edilen kullanıcı bilgileri ve şifreler yardımı ile çeşitli dolandırıcılık suçları işlenmektedir.

Bu tür tuzaklara düşmemek için öncelikle biraz daha dikkatli ve bilgili olmak, hiçbir bankanın e-posta yoluyla bilgi güncellenmesini istemeyeceğini bilmek ve web site adreslerinin güvenli bağlantı sunup sunmadıklarını kontrol etmek, bunlarla da

[43] İsmail Sarı, **"Sniffing Nedir?"**, Cyber-Security <http://www.cyber-security.org.tr/Madde/579/Sniffing-Nedir>, 03.05.2012.

[44] E-Siber İnternet Sitesi, **"Phishing Nedir ve Phishing Yapan Sitelerin Veritabanı"**, <http://www.e-siber.com/guvenlik/phishing-nedir-ve-phishing-yapan-sitelerin-veritabani>, 03.05.2012.

yetinmeyerek web sitelerinin lisanslarının geçerlilik durumlarını kontrol etmek gerekmektedir.

Propaganda

Ucuz ve etkili olmasından dolayı propaganda siber ortam üzerinde gerçekleştirilebilecek en kolay ve en güçlü siber saldırı yöntemidir. Doğru olsun ya da olmasın birkaç fare tıklaması ile metin veya görüntü formatındaki dijital bir bilgi dünya üzerinde herhangi bir yere saniyeler içinde gönderilebilmektedir.[45]

Propaganda faaliyetlerine verilebilecek örnekler arasında Çeçenistan Savaşı ve Irak Savaşı esnasında taraflarca internet üzerinden yayınlanan resim ve videolar sayılabilir. Gerek Çeçenistan Savaşında, gerekse Irak Savaşında propaganda maksatlı olarak elde edilen görüntüler, dünya kamuoyuna televizyon kanallarının yanı sıra internet medyası ve internet siteleri aracılığıyla gösterilmiştir.

Siber Güvenlik Tehdit Araç ve Yöntemlerin Genel Olarak Değerlendirilmesi

Yukarıda belirtilen araçların biri veya bir kısmı kullanılarak dünya üzerindeki birçok sistemden çok büyük miktarda veri ve ağ iletişimi kopyalanmaktadır. Bu da teorik olarak dünya üzerinde herhangi bir yerden, hassas politik ve askeri iletişimler üzerinde bilgi toplama operasyonlarının gerçekleştirilebileceğini göstermektedir.[46]

Günümüz teknolojisi ile bir saldırının ne zaman yapılabileceğini kestirmek olanaksızdır. II. Dünya Savaşı yıllarındaki gibi, bir füzenin fırlatılması için 20 dakika süre kullanma lüksü günümüzde artık yoktur. Siber saldırılar ışık hızında gerçekleşmektedir. Bu nedenle bu tür saldırılar anında karşılık vermeyi gerektirmektedir.[47]

[45] Kenneth Geers, A.g.m.
[46] Kenneth Geers, A.g.m.
[47] Katharina VonKnop, "Institutionslisation of a Web-focused, Multinstional Counter-Terrorism Campaign - Building a Collective Open Source Intelligent System", Terrorism (Ed.), ***Responses to Cyber Terrorism NATO Science for***

Ülkelerin milli güvenlikleri açısından önemli olan ve zarar görmesi durumunda hayati sonuçlar meydana gelebilecek kritik altyapılar arasında barajlar, su tutma ve sulama sistemleri, elektrik üretme ve dağıtım sistemleri, petrol tesisleri, gaz sistemleri ve fabrikalar sayılabilir. Bunlara ulusal enerji sistemleri, ulaşım sistemleri, e-devlet uygulamaları, telekomünikasyon sistemleri, ulusal finans sistemleri, ulusal savunma altyapıları, İnternet omurgası, stratejik sanayi tesislerinin işletim sistemleri, sanayi ve teknoloji sırlarını barındıran sistemler ve hatta bir hastanenin hastaların hayatı için çok önemli olan hidrojen ve oksijen dağıtımını kontrol eden sistemi bile eklenebilir.

Çoğu siber alan ile bütünleşik olan veya bir şekilde İnternet üzerinden erişebilen bu sistemlerin, gelebilecek müdahale ve saldırılardan korunması da hayati önem arz etmektedir. Bu duruma örnek olabilecek birçok vaka gerçekleşmiştir. Memnuniyetsiz bir çalışanın Avustralya'da nehir ve parklara saldığı atık sular, ABD'de 50 milyon kişiyi çaresiz bırakan ve 11 kişinin ölümüne neden olan, elektrik sistemi aksamasının sebebi olan yazılım, İran nükleer tesislerini hedef alan *Stuxnet* yazılımı ilk etapta akla gelebilen birkaç örnek arasında yer almaktadır.[48] Türkiye'de de Batman Hidroelektrik Santralinin faaliyetinin aksamasına sebebiyet veren milli olmayan yazılım,[49] Atatürk Havalimanında aksamalara sebep olan virüs,[50] 2011 yılında gümrük sistemlerinin çökmesi üzerine

***Piece and Security*,** IOS Press (Cilt 34), Ankara, 2008, p. 9.

[48] Ali Işıklı, ***Kritik Altyapı Güvenliğine Yönelik Özgün Çözümler: Sanal Hava Boşluğu Siber Güvenlik Çalıştayı***, Türkiye Noterler Birliği Konferans Salonu, Söğütözü, Ankara, Bilgi Güvenliği Derneği 2011 <http://www.iscturkey.org/calistay/1/images/stories/siberguvenlik.rar>, 06.05.2012,

[49] Milliyet İnternet Sitesi, **Batman Barajı Şifrelendi**, <http://www.milliyet.com.tr/2003/05/28/ekonomi/eko06.html>, 27.02.2012.

[50] Ajans Habertürk İnternet Sitesi, **Atatürk Havalimanı'nda Virüs Kabusu**, <http://www.haberturk.com/yasam/haber/125013-ataturk-havalimaninda-virus-kabusu>, 27.02.2012.

meydana gelen aksama ve uzun kuyruklar[51] ilk akla gelen örnekler arasındadır.

Siber Güvenlik ve Milli Güvenlik

Siber güvenlik ilk olarak 1990'lı yıllarda bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için kullanılmıştır.[52] Fakat daha sonraları bu güvenlik sorunlarının yıkıcı sosyal sonuçlar doğurabileceğinin ortaya çıktığı gelişmeler meydana gelmiştir. Bunlar zamanla politikacılar, özel şirketler ve medya tarafından Batı dünyasına büyük bir tehdit olarak değerlendirilmiş ve "Elektronik Pearl Harbor"lar olarak dile getirilmiştir. 11 Eylül olayları, bilgi teknolojileri, bilgisayarlar ve güvenliğe odaklanılmasını sağlamış, özellikle de bilgi teknolojileri altyapılarının korunması, elektronik gözetleme, teröristlerin interneti iletişim vasıtası olarak kullanmasına dikkat çekmiştir.[53]

Teknolojik gelişmeler uluslararası güvenlik çalışmalarının şekillenmesinde özel bir öneme sahiptir. Özellikle de askeri dengelerin sağlanmaya çalışıldığı soğuk savaş döneminde belirleyici unsur teknolojik gelişmeler olmuştur. Günümüzde ise teknoloji tabanlı senaryoların içerisinde siber savaş, siber saldırı ve siber güvenlik kavramları yer almaktadır. Bu senaryolar teröristlerin veya kötü niyetli saldırganların fiziksel veya dijital yapılara saldırarak kritik altyapıları ve küresel iletişim ağlarını devre dışı bırakabileceği ve de yok edebileceği şeklindedir.[54] İnternetteki karşıt güçler ve ticarileşme,

[51] İşten Haber İnternet Sitesi, **Sistem Çöktü, Gümrük Kapılarında İşlemler Durdu**, <http://www.istenhaber.com/sistem-coktu-gumruk-kapilarinda-islemler-durdu/>, 17.05.2012.

[52] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School", ***International Studies Quarterly***, Yıl 2009, Cilt 53, Pages 1155-1175, <http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf>, 10.12.2011, p. 1155.

[53] Lene Hansen and Helen Nissenbaum, A.g.m., p. 1155.

[54] Barry Buzan and Lene Hansen, ***The Evolution of International Security Studies***, Cambridge, Cambridge University Press, 2009.

İnternetin gündelik hayatın üzerinde bir özerk bölge değil gündelik gerçekliğimizle iç içe geçmiş bir alan olduğunu göstermiştir.[55]

Uluslararası sistem aktörlerinin üzerinde uzlaştıkları ortak bir siber alan tanımı yapılmadığından siber alan üzerinden yapılan saldırılara uluslararası hukukun nasıl uygulanacağı konusu bir problem olarak ortaya çıkmaktadır.[56] Yine bu konuda ortaya çıkan bir başka problem siber saldırıların devlet eliyle mi yoksa suç unsurları tarafından mı gerçekleştirildiğinin anlaşılmasında ve tespitinde yaşanan sorunlardır. Bu sorun da devletlere siber saldırıların kaynağı konusunda şüphe ile yaklaşılmasına sebep olmaktadır.[57] İnternetin iz sürülebilme konusunda güçlükler içeren doğası gereği, siber saldırıların kaynağının net olarak tespit edilememesi gerçeği devam ettiği sürece bu durumun değişeceğini düşünmek yanlış olacaktır.

Siber güvenlik politik olarak kullanılmaya olanak sağlayan araçlar ihtiva etmesinin ötesinde ciddi bir ekonomik sektör meydana getirmiştir.[58] Siber güvenlik alanında devletler ve özel kuruluşlar tarafından büyük yatırımlar yapılmaktadır. Güvenlik açıklarının sonucunda ortaya çıkabilecek zararlar ve itibar kaybı göz önünde bulundurulduğunda devletler ve kurumların siber güvenlik yatırım maliyetlerinden kaçınmayacağı değerlendirilmektedir.

İnternet üzerinden gerçekleştirilen saldırıların milli güvenliğe ne derece zarar verebileceği konusu üzerinde durulacak olunursa, milli güvenliğe yönelen dört tür saldırıdan bahsedilebilmektedir: Bunlardan siber savaş ve ekonomik casusluk daha çok devletler ile

[55] Jos de Mul, ***Siberuzayda Macera Dolu Bir Yolculuk*** (Çev. ÖZDAMAR) 1. Baskı, Kitap Yayınevi, 2008, s. 9.
[56] Muharrem Gürkaynak ve Adem Ali İren, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", ***Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi***, Yıl 2011, Cilt 16, Sayfa 263-279, <http://iibf.sdu.edu.tr/dergi/files/2011-2-13.pdf>, 28.02.2012, ss. 265,266.
[57] Muharrem Gürkaynak ve Adem Ali İren, A.g.m.
[58] Gabriel Weimann, A.g.e., p. 150.

ilişkilendirilen tehditler iken, siber suç ve siber terörizm ise daha çok devlet dışı aktörler ile ilişkilendirilmektedir.[59]

Gerekli yasal düzenlemelerin yapıldığını varsaydığımız ideal bir durumda milli siber güvenlik yapılanmasının şu unsurları içermesi gerekmektedir:[60] Öncelikle teknik ve operasyonel işlemlerin gerçekleştirilebileceği uygun operasyonel bir merkez, strateji ve konseptlerin geliştirildiği ve koordine edildiği, yasal yaklaşımların oluşturulduğu, endüstri ve uluslararası organizasyonlar ile iletişimin gerçekleştirildiği bir koordinasyon merkezi, uygulamaya yönelik olarak stratejik kararların sunulduğu, tartışıldığı ve onaylandığı bir idari yapı.

Günümüzde İnternetin her alandaki kullanımı göz önünde bulundurulduğunda siber alanın milli güvenlik içerisindeki rolünün ne kadar arttığı ve gelecekte bu alanın milli güvenlikte ne kadar ön sıralarda yer alacağı görülmektedir.

Siber Güvenlikle İlgili Yapılanma ve Tedbirler

Siber güvenlik henüz olgunlaşmamış bir disiplindir. Bu konuda güvenlik güçlerinin yetenekleri ve yetişmiş personel sayısı azdır.[61] Buna internet ortamında meydana gelen vakalara karşı gereken müdahalenin yapılmasının gerektirdiği uluslararası karakter de eklenince siber güvenlik ve siber savunma konusunda oluşturulan yapılanmaların henüz yeterli olmadığı açıkça ortaya çıkmaktadır.

Siber alanda oluşan bütün bu tehditlere karşı devlet, kurum ve bireylerin bilinç seviyesi arttıkça uluslararası kuruluşlar ve devletler bazında tedbire yönelik birtakım girişimler oluşmaya başlamıştır.[62]

[59] Joseph S. Nye, **"Cyber Security and National Security"**, ***Cyber Security,*** New Europe (Special Edition), Sayı Mayıs-Haziran 2011, <http://www.scribd.com /doc/56702531/Cyber-Security-2011>, 20.03.2012,

[60] Süleyman Anıl, **"Defending Against Cyber Attacks"**, ***NATO CEP Perceptions,*** Sayı 8, <http://www.nato.int/issues/cep/cep_newsletter_08e.pdf>, 05.03.2012,

[61] Kenneth Geers, A.g.m.

[62] Chris Connolly and Alana Maurushat et all, **An Overview of International Cyber-Security Awareness Raising and Educational Initiatives**,

Siber alanın devlet aşan sınırları göz önünde bulundurulduğunda, siber güvenlik konusunda etkili tedbir ve çözümler oluşturulabilesi için uluslararası kuruluşların faaliyetlerinin ve devletlerarası işbirliğinin kıymeti ortaya çıkmaktadır.

Devletler açısından bakıldığında, İnternetten gelecek tehditler ve bunlara karşı yürütülecek tedbirlerle ilgili değişik algılama ve görüşler ortaya çıkmaktadır. Siber alanda kendilerine yönelik olarak meydana gelen saldırılara askeri karşılıklar verilmesi düşüncesine varan siber saldırıları savaş sebebi sayma yaklaşımının yanında; bu ortamdan gelen tehditlerin aynı ortamda karşılık bulması gerektiğini öngören düşünceler de bulunmaktadır. Bu yaklaşımlar saldırıların kaynağı, hedefi ve orantılı güç kullanımı tartışmalarını da beraberinde getirmektedir.[63]

ABD, Avusturya, Danimarka, Fransa, Almanya, Yunanistan, Finlandiya, İtalya, Türkiye, İsveç, İsviçre, Avustralya, Kanada, Hindistan, Japonya, İspanya, Portekiz, İngiltere, Malezya ve Singapur gibi ülkelerde siber güvenlikle ilgili sıkı yaptırımlar ve kısıtlamalar içeren düzenlemeler oluşturulmaya çalışılsa da; çoğu ülkede bu konuda yeterli düzenleme bulunmamaktadır.[64] Bu

<http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview _intnl_cybersecurity_awareness.pdf>, 20.07.2013.

[63] ESSARP Model United Nations 2013 Research Report, **Preventing and Prosecuting Cyber Warfare**, <http://www.essarp.org.ar/archivos/6/0/REPORT__Preventing_and_prosecuting_cyber_warfare.pdf>, 20.07.2013; Chunmei Kang and Qiang Zhao et all, **"Establishing Norm of Behavior in Cyberspace"**, <http://www.isodarco.it/courses/andalo12/paper/ISO12_Chunmei.pdf>, 20.07.2013; Marco Roscini, **"World Wide Warfare - *Jus ad bellum* and The Use of Cyber Force"**, <http://www.mpil.de/files/pdf3/03_roscini_14.pdf>, 20.07.2013, ss. 88-90; Harold Hongju Koh, **International Law in Cyberspace (Remarks)**, <http://www.state.gov/s/l/releases/remarks/197924.htm>, 20.07.2013; Catherine Lotrionte, "State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights", ***Emory International Law Review***, Cilt 26, pages 825-919, <http://www.law.emory.edu/fileadmin/journals/eilr/26/26.2/Lotrionte.pdf>, 20.07.2013, pp. 828-829.

[64] Manish Lunker, (20.07.2013). **Cyber Laws: A Global Perspective**,

aşamada İnternetin mekân olarak sınıra sahip olmadığı gerçeği göz önüne getirilirse devletlerin kendi iç sistemlerindeki düzenlemelerin yanında, değişik yaptırım ve bilgi paylaşımları içeren uluslararası işbirliği ve düzenleme yaklaşımı bir gereklilik halini almıştır. Ancak bu konuda gelinen aşama ve uygulamalara bakınca daha kat edilmesi gereken ne kadar uzun bir yol olduğu görülecektir.

Terörizme karşı görünüp bu konuda demeçler verirken değişik yollarla rakip ya da düşman olarak gördükleri devletlere karşı terörist faaliyetleri destekleyen birçok devlet olduğu gibi kimliklerin kolayca gizlenebildiği ve iz sürmenin son derece zor olduğu siber alanda da rakip devletlere zarar veren nitelikte olan siber saldırıları destekleyen devletler bulunmaktadır.

Türkiye'de de siber güvenlik bilincinin artması, son zamanlarda yoğun siber saldırılara maruz kalınması ve siber güvenlik tedbirleri ile ilgili girişimlerde bulunmanın ihtiyaç halini almasıyla birlikte değişik çalışmalar yapılmaktadır. Bu faaliyetler; Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Programı, Ulusal Bilgi Güvenliği Kapısı, Yasal Çalışmalar, Siber Güvenlik Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, Konferanslar ve Çalıştaylar ve de TSK bünyesinde icra edilen faaliyetler ve oluşumlar şeklinde sıralanabilir.[65]

<http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf>.

[65] BTK, **Bağlantılar**, <http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/baglantilar.php>, 15.04.2012; DPT, ***Bilgi Toplumu Stratejisi (2006-2010)***, Ankara, DPT 2006 <http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060700_BilgiToplumuStratejiBelgesi.pdf>, 15.04.2012; TUBİTAK BİLGEM, **Ulusal Bilgi Güvenliği Programı Hakkında**, <http://www.bilgiguvenligi.gov.tr/hakkimizda.html>, 15.04.2012; TBMM, ***Türk Ceza Kanunu***, Md. 243-245, 2004 <http://www.ceza-bb.adalet.gov.tr/mevzuat/5237.htm>, 15.04.2012; Adalet Bakanlığı, ***Kişisel Verilerin Korunması Kanun Tasarısı***, 2008 <http://www.kgm.adalet.gov.tr/tbmmkom/kisiselveriler.pdf>, 15.04.2012; Bilgi Güvenliği Derneği, **Siber Güvenlik Hukuku Çalıştayı Sonuç Bildirgesi**, <http://www.bilgiguvenligi.org.tr/files/bildirge2012.pdf>, 18.05.2012; TÜBİTAK BİLGEM, **Kripto Analiz Merkezi**, <http://www.uekae.tubitak.gov.tr/home.do?ot=1&sid=30>,

Bu çalışmalardan yasal çerçeve oluşturma süreci siber güvenlik tedbirleri konusunda önemli bir yer tutmaktadır. Mevcut yasaların yeterli olmadığı bu alanda yeni düzenlemeler yapılmaktadır. Bunlar arasında TCK'ya "Bilişim Alanında İşlenen Suçlar" başlığı altında eklenen 243. ve 244. Maddeler, kişisel verilerin korunması hakkında hazırlanan ve yasalaşma sürecinde olan tasarı, 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ve 5070 sayılı "Elektronik İmza Kanunu yer almaktadır.[66]

TSK bünyesinde de siber güvenlikle ilgili çalışmalar ve etkinlikler gerçekleştirilmekte olup diğer kamu kurum ve kuruluşları ile siber güvenlik alanında işbirliği yapılmaktadır.[67] TÜBİTAK UEKAE bünyesinde 2001 yılında kurulan "Bilişim Sistemleri Güvenliği Bölümü" bu alandaki faaliyetlerine ilk önce Türk Silahlı Kuvvetleri ile başlamıştır.[68] Bunun yanı sıra, 2012 yılında TSK bünyesinde diğer kamu kurum ve kuruluşları ile koordineli olarak faaliyet gösteren TSK Siber Savunma Merkezi Başkanlığı kurulmuştur.[69]

Siber güvenlik alanında planlanıp gerçekleştirilen çalıştay ve

19.05.2012; TUBİTAK UAKAE, (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) **Siber Güvenlik Tatbikatı**, <http://www.tubitak.gov.tr/sid/341/cid/21886/index.htm;jsessionid=EDCEA0BEC13F23C792676DDAF42EE248>, 15.05.2012; BTK ve TÜBİTAK, **"Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu"**, <http://www.tubitak.gov.tr/tubitak_content_files//basin/siber-tatbikat-rapor/siber-tatbikat-rapor.pdf>, 15.04.2012.

[66] TBMM, A.g.y.; Adalet Bakanlığı, A.g.e.; Bilgi Güvenliği Derneği, A.g.y.

[67] TSK TMMM (COEDAT), **Faaliyetler**, <http://www.tmmm.tsk.tr/anasayfa.htm>, 03.06.2012; TSK TMMM (COEDAT), **"Siber Terörizm (Siber Tehdit Farkındalık ve Bilinçlendirme Eğitimi" Kursu (COE-DAT 10)**, <http://www.tmmm.tsk.tr/kurs10.htm>, 30.05.2012.

[68] Teknolojide.com İnternet Sitesi, **Ulusal Siber Güvenlik Tatbikatı**, <http://www.teknolojide.com/ulusal-siber-guvenlik-tatbikati_5179.aspx>, 03.06.2012.

[69] TSK İnternet Sitesi, **Türk Silahlı Kuvvetleri Siber Savunma Faaliyetleri**, <http://www.tsk.tr/3_basin_yayin_faaliyetleri/3_4_tsk_haberler/2013/tsk_haberler_06.html>, 21.01.2013.

konferanslar bu alanda bilgi paylaşımı, bakış açısının geliştirilmesi, ortak bilinç oluşturulması ve iş birliği konusunda çok özel bir yere sahiptir. Siber güvenlik alanında gerçekleştirilen çalıştay ve konferanslar arasında şunları sayabiliriz: "17 Mayıs 2012 "Cloud, Virtualization and Security", 18 Nisan 2012 "E-crime Turkey 2012" 29 Mart 2012 "Mobile Security", 25 Şubat 2012 "Netsec Topluluk Buluşması/ Siber Savaş Aracı Olarak Kötücül Yazılımlar", 26-27 Ocak 2012 "Siber Güvenlik Hukuku Çalıştayı", 22 Aralık 2011 "Siber Güvenlik Konferansı", 29 Eylül 2011 "Siber Güvenlik Çalıştayı", 03-31 Temmuz 2011 "BGA Siber Güvenlik Yaz Kampı", 09 Temmuz 2011 "BGA-Kariyer.Net-Dataplus Ethical Hacking Workshop", 07 Temmuz 2011 "Siber Saldırı Aracı Olarak DDoS", 02 Temmuz 2011 "Siber Tehditler, Savunma Yöntemleri ve Hackerların Başarısı", 9-10 Haziran 2011 "Bilgi Teknolojileri Yönetişim ve Denetim Konferansı", 3-4 Haziran İstSec '11 "İstanbul Bilgi Güvenliği Konferansı", 21-22 Mayıs 2011 "Siber Tehditler ve Savunma Yöntemleri", 17 Mayıs 2011 "Uluslararası Hukuk Kulübü Bilişim Hukuku Panelleri", 16 Mayıs 2011 "SMi's Cyber Security 2011", 14-15 Mayıs 2011 "IBB Bilişim Güvenliği 2011 Zirvesi", 05 Mayıs 2011 "Bahçeşehir Üniversitesi Siber Güvenlik Etkinliği", 01 Mayıs 2011 "Hosting Zirvesi 2011", 30 Nisan 2011 "Web Uygulama Güvenliği Etkinliği", 14 Nisan 2011 "DDoS Saldırıları, Korunma Yolları ve BotNet Sorunu", 10-12 Mart 2011 "Uluslararası İstihbarat Ve Gözetim Teknolojileri Konferansı ", 15 Şubat 2011 "DDoS Saldırıları, Korunma Yolları ve BotNet Sorunu", 9 Şubat 2011 "Güvenli İnternet Günü (Safer Internet Day)" ve 30 Ocak 2011 "NetSec Topluluğu İstanbul Buluşması".[70]

Siber güvenlik tatbikatları teoride sağlam görünen sistemlerin açıklıklarının ortaya çıkması ve böylelikle gereken tedbirlerin alınmasının sağlanması açısından çok önemlidir. Ülkemizde yapılan tatbikatların diğer ülkelerde yapılanlardan ayrıldığı nokta gerçek

[70] BGA, **Bilgi Güvenliği Akademisi Etkinlikleri**, <http://www.bga.com.tr/etkinlikler-sayfasi/>, 25.05.2012.

saldırı ve savunma tekniklerinin kullanılmasıdır. Bu da siber güvenlik konusunu teoriden pratiğe taşıma ve gerçek durumu ortaya koyma anlamında çok fayda sağlamıştır.

Sonuç

Günümüzde meydana gelen siber güvenlik vakalarının tamamına yakını aşağıdaki yöntemlerden biri veya birkaçının birleşimi şeklinde gerçekleşmektedir: Genel erişime açık olan internet sitelerinin ana sayfalarını silmek veya değiştirmek, erişime açık olan bu sitelerdeki dosyalara erişim sağlayıp bilgi hırsızlığı gerçekleştirmek, ancak var olan dosyaları değiştirmemek, erişime açık olan siteleri saldırılar ile erişilemez hale getirmek, şahısların ve kurumların bilgisayarlarına virüs vb. zarar verici yazılımlar yüklemek, bu yazılımlar ile uzak sistemlere erişim sağlamak, bu yolla sistemlere fiziksel zararlar vermek, bu yolla bilgi hırsızlığı yapmak, bu yolla elde edilen bilgiler ile siber suçlar işlemek, bu yolla elde edilen bilgiler ile başka alanları ilgilendiren suçlar işlemek, siber ortamda yasal veya gayri yasal propaganda gerçekleştirmek, siber ortamı yasal olmayan faaliyetlerin organize ve koordine edildiği bir alan olarak kullanmak, değişik şekillerde ele geçirilip köle haline getirilen bilgisayarları zamanı geldiğinde saldırı için kullanmak, siber ortamda telif haklarını ihlal eder şekilde yayın yapmak, siber ortamı kişilik haklarını ihlal edici şekilde iftira, ifşa ve karalama alanı olarak kullanmak, siber ortamda çocuk istismarı yapmak, siber ortamda kontrolsüz bir şekilde erişilebilen yetişkin içeriği yayınlamak, siber ortamdaki ticaret platformlarını kullanarak yasal olmayan veya konusu suç teşkil eden pazarlama yapmak, siber ortam kullanılarak insanlara istemedikleri halde ve rahatsız edici şekilde reklam içeriği göndermek ve siber ortamda içerik hakkında yanlış anahtar kelimeler yayımlayarak kullanıcıları reklam ya da zararlı yazılım içeren sitelere yönlendirmek.

İnternetin hayatımızın bir parçası haline gelmesi ile birlikte bu alanda karşılaşılacak tehdit ve yöntemlerin de giderek arttığı görülmektedir. Elbette güvenlik yazılımları ve yöntemleri de buna paralel olarak gelişmektedir. Ancak ne yazık ki her güvenlik ihlali

ve saldırı beraberinde ek tedbirler ve kısıtlamalar meydana getirmektedir. Bu da, temelde bilgi paylaşımı ve bilgiye erişim maksatlı olarak geliştirilen siber ortamda her gün bilgiye erişimi biraz daha zor, biraz daha dolaylı hale getirmekte ve kısıtlamaktadır.

Her şeyden önce temeli bilgi paylaşımı ve bilgiye erişim olan İnternette güvenlik gerekçeleri ile özgürlükler dengesi iyi korunmalı ve İnternet işlevsiz hale getirilmemelidir.

İnternetin fiziksel altyapısı zarar gördüğünde veya tahrip edildiğinde yazılım bazında alınan tedbirlerin işe yaramayacağı bilinmeli ve öncelikle İnternetin fiziksel altyapısı sıkı bir şekilde korunmalıdır.

Çoğu saldırı siber ortamın sadece görünen yüzü olan web sitelerinin ana sayfalarına karşı gerçekleşmekte ve aslında ciddi zararlar oluşturmamaktadır. Bu nedenle korumasız ve şifresiz bir şekilde erişim sağlanan bu tür alanlarda özel ve gizli bilgiler bulundurulmamalıdır.

Saldırılar anında, verilen hizmetlerin aksamamasının sağlanması çok önemlidir: yoksa bir saldırıyı engellemek, bilgisayar ve sunucuların fişini çekmek ya da bağlantısını kesmek kadar basittir; ancak bu, amaca hizmet etmeyecektir.

Kullanıcılar *firewall* (güvenlik duvarı) kullanımı ve *port* (bağlantı noktası) yapılandırması konusunda eğitilmelidir. Ayrıca web uygulamaları son derece güvenli bir şekilde yapılandırılmalı ve ilgisiz kişilerin erişimini kısıtlamalıdır.

Bilgisayar sistemi yöneticilerinin gerekli teknik eğitimi almaları sağlanmalıdır. Ayrıca sistem yöneticileri kendilerini siber güvenlik saldırı araç ve yöntemleri ve bunlara karşı alınacak tedbirler ve müdahaleler konusunda geliştirmelidir.

Yazılımlar daha tasarım aşamasında iken güvenlik ihlallerine karşı güçlü bir koruma içerecek şekilde yapılandırılmalı ve kaynak kodlarının gizliliği ihlal edilmemelidir.

Saldırıların meydana geldiği anda tespit edilmesi, bunlara karşı yeterli önlem ve müdahale imkânlarının bulunması kadar

önemli bir faktördür. Elde gerekli yöntem, araç ve kabiliyetler bulunsa da iş işten geçtikten sonra yapılan bir müdahale anlam taşımayacaktır.

Siber alanda meydana gelen tehditler ile mücadelede özel sektör ile kamu sektörü arasındaki işbirliği son derece büyük önem arz etmektedir. Kamu sektörü ve özel sektör, siber alanda milli güvenliğin sağlanması ve sürdürülmesi ve de bu alandan gelebilecek tehditlere karşı koyma hedeflerine yönelik olarak, tüm kaygılarını bir tarafa bırakıp ortak hareket etmelidirler.

Kablosuz ağlar konusunda kullanıcılar ve sistem yöneticileri bilgilendirilmeli ve gerekli tedbirlerin alınması sağlanmalıdır. Bunlardan en başta geleni paylaşımın şifreli ve kriptolu olarak gerçekleştirilmesi ve erişim noktalarının (AP) isimlerini (SSID) yayımlamayacak şekilde yapılandırılmasıdır.

Daha güvenli yazılım teknolojileri geliştirilmesi için TÜBİTAK gibi kurumlar ile işbirliğine gidilmeli, yazılım geliştirme ve test etme aşamalarında ülkenin genç yeteneklerinden faydalanılmalıdır.

Sistemlere erişim kontrol altında bulundurulmalı ilgisiz kullanıcıların bilgilere rastgele erişimi engellenmelidir.

Küresel olan siber tehditlerle yerel yaklaşımlar yoluyla mücadele etmek gerçekten zordur; bu nedenle konuya ulusal yaklaşımlar getirilmeli ve ilgili uluslararası kuruluşlar ile olan işbirliği güçlendirilmelidir.

Siber güvenlik konusunda meydana gelen gelişmeler o kadar hızlı gerçekleşmektedir ki, yasal düzenlemeler bunun gerisinde kalmaktadır. Bu nedenle ilgili yasal düzenlemeler bir an önce gerçekleştirilmeli ve ihtiyaçlar doğrultusunda sürekli güncellenmelidir. Bunun yanında, yasa koyucular, kanıtlanabilirlik ve geriye dönük iz takibi maksatlı olarak hizmet sağlayıcılara veri saklama ve erişim konusunda yükümlülükler getirmektedir; ancak özel sektör ve kamu, bu düzenlemelerle ilgili olarak maliyet ve gizlilik endişesi taşımaktadır. Bu nedenle bu konuda denge sağlanmalı, bilgi saklama konusunda ise verilerin güvenliği garanti altına alınmalıdır. Bunun

yanında kamu ile özel sektör arasında güven sorunu bulunmaktadır.[71] Bu sorun aşılıp gerekli adımlar atıldığında bireysel, kurumsal ve toplumsal faydaları hemen görülmeye başlanacaktır.

Siber tehditleri önlemenin veya en azından etkisini azaltmanın en etkin yollarından biri de eğitimdir. Gerek bireysel olarak kendimizi gerekse kurumsal olarak personeli siber güvenlik konusunda eğitmek ve son bilgilerle donatmak artık kaçınılmaz hale gelmiştir. Bununla paralel olarak kurumlardaki ve bireysel kullanımdaki bilgisayarlar en son teknoloji ve güvenlik yazılımları ile donatılmalıdır.

Kurumlarda mutlaka risk değerlendirmesi yapılmalı ve olası saldırı ve aksaklık durumunda uygulanacak hareket şekli belirlenmelidir. Yedek planlar oluşturulmalıdır.

Sistemlerin işleyişlerinin aksamadan devam ettirilmesi, gerek ekonomik gerekse sosyal anlamda çok önemlidir. Bu sebeple sistemler işler halde iken gerekli müdahalelerin yapılması son derece önemlidir. Bu tür durumlarda gereken müdahalelerin yapılması için oluşturulan koordinasyon büyük önem arz etmektedir.

Kritik yapıların korunması için gelişmiş devletlerde olduğu gibi yasal ve idari çalışmaların bir an önce tamamlanması gerekmektedir. Ayrıca kritik altyapılarda kullanılan yazılımların tamamen milli yazılımlardan oluşması, yabancı yazılımlara bağlılığı ortadan kaldıracak ve bu yazılımların, içerisine yerleştirildiği ve gerektiğinde kullanılabilecek olduğu konusunda şüpheler oluşan gizli kodlar veya arka kapılar konusundaki endişeler ortadan kalkacaktır.

Gerçekleştirilmekte olan siber güvenlik konferans ve çalıştayları ortaya çıkardığı faydalar açısından çok önemlidir. Bu tür faaliyetlere devlet ve özel sektör desteği artmalı, teşvikler

[71] EUROPE RAND İnternet Sitesi, ***Managing New Issues: Cyber Security in an Era of Technological Change***, The Hague Netherlands 2001 <http://www.rand.org/pubs/monograph_reports/MR1535.html>, 12.04.2012.

sağlanmalı ve katılım artırılmalıdır.

Ulusal düzeyde oluşturulanların yanında kurumlarda da siber güvenlikle ilgili birimler oluşturulmalı ve bunlar aracılığıyla gerekli tedbirler alınmalı, farkındalık meydana getirilmeli ve eğitim verilmelidir.

Siber güvenlik olayları ile ilgili saldırı şekilleri ve bunlara karşı korunma tedbirlerinin kaydedildiği ve gerektiğinde ilgililerce erişilebilecek bir veri tabanı oluşturulması benzer saldırılar meydana gelmesi durumunda iş gücü ve zaman kaybının azaltılmasını ve hatta ortadan kaldırılmasını sağlamak açısından son derece önemlidir.

Siber güvenlik alanında yaşanabilecek tehditler ve bu tehditlerin meydana getirebileceği zararlar göz önünde bulundurulduğunda, alınması gereken tedbirlerin çokluğu, çeşidi ve ihtiyaç duyulan koordinasyon ortaya çıkmaktadır. Sayılan tüm tedbirlerin yanında bilinçli bir kullanıcının yerini hiçbir teknolojinin alamayacağı değerlendirilmektedir.

SUMMARY

With over 2.3 billion worldwide users, Internet penetrated every scope of our lives. We use Internet to carry out our money transactions, address statements, shopping, talking and business operations.

While Internet provides us with so many facilities, it also puts our money, goods and secrecy in danger. Foundation philosophy of the Internet was not about its own security. It was about easing the way people communicate, sharing of information and providing a stable network, which is not dependent of a specific hardware. However, next stages of its development and spread came with a lot of vulnerabilities. These stages brought many security measures which at the same time restrict the access to information.

Despite being relatively new field, there are many studies on Internet and Cyber Security, many of which handle the technical

aspects of the matter. But also there are few studies on the awareness and education side of the Internet. Cyber Security Situational Awareness studies address this aspect of it and expected to increase by time.

It is possible to put the history of Internet back to the times when telegraph invented. With great advances in technology now it reached a phase that we cannot do without Internet.

There are so many threats and tools used to attack us via Internet. But every threat we face takes our security technology and knowledge, one step forward.

National and International Cooperation must be encouraged strongly to make the grade, because Internet's trans-boundary nature makes it a necessity rather than a choice.

National and International regulations must be formed to keep up with the changing nature of the use of Internet.

It is important to keep the systems active and online ,while fighting against cyber attackers, or else it may cost a lot –like keeping a human being alive while carrying out a surgery on his heart.

As an educational pace, National and International Cyber Security Conferences and exercises must be supported both by financial assistance and participating.

We must always remember that even the strictest measures cannot replace an educated user when it comes to security.

KAYNAKLAR

Kitaplar

BUZAN Barry and HANSEN Lene, ***The Evolution of International Security Studies***, Cambridge, Cambridge University Press, 2009.

CRIDLAND Clare, "The History of the Internet: The Interwoven Domain of Enabling Technologies and Cultural Interaction", Centre of Excellence Defence Against Terrorism (Ed.), ***Responses to Cyber Terrorism NATO Science for Piece and Security,*** IOS Press (Cilt 34), Ankara, 2008.

GOODMAN Seymour E, "Critical Information Infrastructure Protection", Centre of Excellence Defence Against Terrorism (Ed.), ***Responses to Cyber Terrorism NATO Science for Piece and Security*****,** IOS Press (Cilt 34), Ankara, 2008.

GRAHAM James and HOWARD Richard, et all, ***Cyber Security Essentials***, Boca Raton, Auerbach Publications, 2010.

IŞIKLI Ali, ***Kritik Altyapı Güvenliğine Yönelik Özgün Çözümler: Sanal Hava Boşluğu*****,** Siber Güvenlik Çalıştayı, Türkiye Noterler Birliği Konferans Salonu, Söğütözü, Ankara, <http://www.iscturkey.org/calistay/1/images/stories/siberguvenlik.rar>, 06.05.2012.

JAJODIA Sushil and LIU Peng et all, (Ed.). ***Cyber Situational Awareness***. New York, Springer, 2010.

KISSEL Richard (Ed.), ***Glossary of Key Information Security Terms***, National Institute of Standards and Technology, 2011, <http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf>, 08.03.2012.

MUL Jos de, ***Siberuzayda Macera Dolu Bir Yolculuk*** (Çev. Ali ÖZDAMAR) 1. Baskı, Kitap Yayınevi, 2008.

VON KNOP Katharina, "Institutionslisation of a Web-focused, Multinstional Counter-Terrorism Campaign - Building a Collective Open Source Intelligent System", Centre of Excellence Defence Against Terrorism (Ed.), ***Responses to Cyber Terrorism NATO Science for Piece and Security*****,** IOS Press (Cilt 34), Ankara, 2008.

WEIMANN Gabriel, ***Terror on The Internet: The New Arena The New Challenges***, Washington D.C., United States Institue of Peace, 2006.

YILMAZ Sait ve SALCAN Olcay, ***Siber Uzay'da Güvenlik ve Türkiye***, İstanbul, Milenyum Yayınları, 2008.

Makaleler

ANIL Süleyman, "Defending Against Cyber Attacks", ***NATO CEP Perceptions,*** Sayı 8, <http://www.nato.int/issues/cep/cep_newsletter_08e.pdf>, 05.03.2012.

BAKIR Emre, "İnternet Güvenliğinin Tarihçesi", ***TÜBİTAK Bilgem Dergisi***, Yıl 2011, Cilt 3, Sayı 5, Sayfa 6-17.

BGA, "Günümüz Internet Dünyasında IP Spoofing", <http://blog.bga.com.tr/network-security/gunumuz-internet-dunyasinda-ip-spoofing>, 03.05.2012.
BTK ve TÜBİTAK, "Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu", <http://www.tubitak.gov.tr/tubitak_content_files//basin/siber-tatbikat-rapor/siber-tatbikat-rapor.pdf>, 15.04.2012.
E-Siber İnternet Sitesi, "Phishing Nedir ve Phishing Yapan Sitelerin Veritabanı", <http://www.e-siber.com/guvenlik/phishing-nedir-ve-phishing-yapan-sitelerin-veritabani>, 03.05.2012.
GEERS Kenneth, "Cyberspace and the Changing Nature of Warfare", ***Centre of Excellence Tallinn,*** Estonya, <http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf>, 28.02.2012.
GÜRKAYNAK, Muharrem ve Adem Ali İREN. "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", ***Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi***, Yıl 2011, Cilt 16, Sayfa 263-279, <http://iibf.sdu.edu.tr/dergi/files/2011-2-13.pdf>, 28.02.2012.
HANSEN Lene and NISSENBAUM Helen, "Digital Disaster, Cyber Security, and the Copenhagen School", ***International Studies Quarterly***, Yıl 2009, Cilt 53, Sayfa 1155-1175, <http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf>, 10.12.2011.
KANG Chunmei and ZHAO Qiang, et all, "Establishing Norm of Behavior in Cyberspace", <http://www.isodarco.it/courses/andalo12/paper/ISO12_Chunmei.pdf>, 20.07.2013.
LOTRIONTE Catherine, "State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights", ***Emory International Law Review***, Cilt 26, Sayfa 825-919, <http://www.law.emory.edu/fileadmin/journals/eilr/26/26.2/Lotrionte.pdf>, 20.07.2013.
MAURUSHAT Alana, "Zombie Botnets", SCRIPTed, Cilt 7, Sayı 2, <http://www.law.ed.ac.uk/ahrc/script-ed/vol7-2/maurushat.asp>, 17.04.2012.

NYE Joseph S., "Cyber Security and National Security",Cyber Security, ***New Europe*** (Special Edition), Sayı Mayıs-Haziran 2011, <http://www.scribd.com/doc/56702531/Cyber-Security-2011>, 20.03.2012.

O'REIRDAN Michael, "Why Bother With Best Practices? Or Why Global Collaboration is Faster (and More Effective) Than a Speeding Bullet", ***Cyber Security,*** New Europe (Special Edition), Sayı Mayıs-Haziran 2011, <http://www.scribd.com/doc/56702531/Cyber-Security-2011>, 20.03.2012.

RANDELL Brian, "A History of Computing in The Twentieth Century - The Colossus", <http://www.cs.ncl.ac.uk/publications/books/papers/133.pdf>, 16.04.2012.

ROSCINI Marco, "World Wide Warfare - *Jus ad bellum* and The Use of Cyber Force", <http://www.mpil.de/files/pdf3/03_roscini_14.pdf>, 20.07.2013.

ÜNVER Mustafa ve CANBAY Cafer, "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", ***Elektrik Mühendisliği***, Yıl 2010, Sayı 438, Sayfa 94-103, <http://www.emo.org.tr/ekler/a9a502d6e646c25_ek.pdf?dergi=598 >, 11.04.2012.

İnternet

SARI İsmail, ***"Sniffing Nedir?"***, Cyber-Security <http://www.cyber-security.org.tr/Madde/579/Sniffing-Nedir>, 03.05.2012.

SpywareGuide İnternet Sitesi, "Spyware", <http://www.spywareguide.com/term_show.php?id=12>, 03.05.2012.

SUBRAMANYAM Kishoreve and FRANK Charles E., et all, ***"Keyloggers: The Overlooked Threat to Computer Security"***, <http://www.keylogger.org/articles/kishore-subramanyam/keyloggers-the-overlooked-threat-to-computer-security-7.html#.T6GcbOs9XmQ>, 03.05.2012.

Adalet Bakanlığı, ***Kişisel Verilerin Korunması Kanun Tasarısı***, 2008 <http://www.kgm.adalet.gov.tr/tbmmkom/kisiselveriler.pdf>, 15.04.2012.

DPT, ***Bilgi Toplumu Stratejisi (2006-2010)***, Ankara, DPT 2006 <http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060700_BilgiToplumuStratejiBelgesi.pdf>, 15.04.2012.

KANE Robert K., ***Internet Governance in an Age of Cyber Insecurity***, Council Special Report No. 56, 2010 <http://i.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf>, 28.02.2012.
TBMM, Türk Ceza Kanunu, Md. 243-245, 2004 <http://www.ceza-bb.adalet.gov.tr/mevzuat/5237.htm>, 15.04.2012.
EUROPE RAND İnternet Sitesi, ***Managing New Issues: Cyber Security in an Era of Technological Change***, The Hague, Netherlands 2001 <http://www.rand.org/pubs/monograph_reports/MR1535.html>, 12.04.2012.
Ajans Habertürk İnternet Sitesi, ***Atatürk Havalimanı'nda Virüs Kabusu***, <http://www.haberturk.com/yasam/haber/125013-ataturk-havalimaninda-virus-kabusu>, 27.02.2012.
BGA, ***Bilgi Güvenliği Akademisi Etkinlikleri***, <http://www.bga.com.tr/etkinlikler-sayfasi/>, 25.05.2012.
Bilgi Güvenliği Derneği, ***Siber Güvenlik Hukuku Çalıştayı Sonuç Bildirgesi***, <http://www.bilgiguvenligi.org.tr/files/bildirge2012.pdf>, 18.05.2012.
Bilgiportal İnternet Sitesi, ***Virüs, Solucan ve Truva Atı Nedir?***, <http://www.bilgiportal.com/v1/idx/19/2480/Gvenlik/makale/Virs-solucan-ve-Truva-at-nedir.html>, 17.04.2012.
BTK, ***Bağlantılar***, <http://www.tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/baglantilar.php>, 15.04.2012.
CLARKE Lashan, ***How Denial Of Service (DoS) Works?*** <http://www.brighthub.com/computing/smb-security/articles/30075.aspx>, 17.07.2013.
CONNOLLY, Chris and MAURUSHAT Alana, et all, ***An Overview of International Cyber-Security Awareness Raising and Educational Initiatives***, <http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf>, 20.07.2013.
EBSCO Host İnternet Sitesi, ***Library, Information Science & Technology Abstracts***, <http://web.ebscohost.com/ehost/results?sid=81216314-aa32-45bd-9479-d9e0a32310bb%40sessionmgr110&vid=9&hid=108&bquery=cyber+security&

bdata=JmRiPWx4aCZ0eXBlPTAmc2l0ZT1laG9zdC1saXZl>, 11.07.2013.
ESSARP Model United Nations 2013 Research Report, ***Preventing and Prosecuting Cyber Warfare***, <http://www.essarp.org.ar/archivos/6/0/REPORT__Preventing_and_prosecuting_cyber_warfare.pdf>, 20.07.2013.
GOOGLE AKADEMİK İnternet Sitesi, ***Cyber Security***, <http://scholar.google.com.tr/scholar?hl=tr&q=cyber+security&btnG=&lr=>, 11.07.2013.
HUMPHRYS John, ***State Cyber-Snooping: How worried should we be?***, <http://yougov.co.uk/news/2013/06/11/state-cyber-snooping-how-worried-should-we-be/>, 14.07.2013.
Internet World Stats İnternet Sayfası, ***World Internet Users and Population Stats***, <http://www.internetworldstats.com/stats.htm>, 18.05.2013.
İşten Haber İnternet Sitesi, ***Sistem Çöktü, Gümrük Kapılarında İşlemler Durdu***, <http://www.istenhaber.com/sistem-coktu-gumruk-kapilarinda-islemler-durdu/>, 17.05.2012.
JSTOR İnternet Sitesi, ***JSTOR: Search Results Cyber Security***, <http://www.jstor.org/action/doBasicSearch?Query=cyber+security&acc=off&wc=on&fc=off>, 11.07.2013.
KOH, Harold Hongju, ***International Law in Cyberspace (Remarks)***, <http://www.state.gov/s/l/releases/remarks/197924.htm>, 20.07.2013.
LUNKER Manish, (20.07.2013). ***Cyber Laws: A Global Perspective***, <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf>.
MCMILLAN Robert, ***Student Used Spyware to Steal Passwords, Change Grades,*** <http://www.computerworld.com/s/article/9214898/Student_used_spyware_to_steal_passwords_change_grades>, 15.07.2013.
Microsoft İnternet Sitesi, ***Virüsler***, <http://windows.microsoft.com/tr-TR/windows-vista/Viruses-frequently-asked-questions>, 17.04.2012.
Milliyet İnternet Sitesi, ***Batman Barajı Şifrelendi***, <http://www.milliyet.com.tr/2003/05/28/ekonomi/eko06.html>, 27.02.2012.

PERIMETEC İnternet Sitesi, ***The Fututre of Spam***, <http://www.perimetec.com/all-about-spam/the-future-of-spam.php>, 15.07.2013.
SearchSecurity İnternet Sitesi, ***Botnet (Zombie Army),*** <http://searchsecurity.techtarget.com/definition/botnet>, 17.04.2012.
Teknolojide.com İnternet Sitesi, ***Ulusal Siber Güvenlik Tatbikatı***, <http://www.teknolojide.com/ulusal-siber-guvenlik-tatbikati _5179.aspx>, 03.06.2012.
TSK İnternet Sitesi, ***Türk Silahlı Kuvvetleri Siber Savunma Faaliyetleri***, <http://www.tsk.tr/3_basin_yayin_faaliyetleri/ 3_4_tsk_ haberler/2013/tsk_haberler_06.html>, 21.01.2013.
TSK TMMM (COEDAT), ***Faaliyetler***, <http://www.tmmm.tsk.tr/ anasayfa.htm>, 03.06.2012.
TSK TMMM (COEDAT), ***"Siber Terörizm (Siber Tehdit Farkındalık ve Bilinçlendirme Eğitimi" Kursu (COE-DAT 10),*** <http://www.tmmm.tsk.tr/kurs10.htm>, 30.05.2012.
TUBİTAK BİLGEM, ***Ulusal Bilgi Güvenliği Programı Hakkında***, <http://www.bilgiguvenligi.gov.tr/hakkimizda.html>, 15.04.2012.
TUBİTAK UAKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü), ***Siber Güvenlik Tatbikatı***, <http://www.tubitak.gov.tr/ sid/341/cid/21886/index.htm;jsessionid=EDCEA0BEC13F23C792676 DDAF42EE248>, 15.05.2012.
TÜBİTAK BİLGEM, ***Kripto Analiz Merkezi***, <http://www.uekae. tubitak.gov.tr/home.do?ot=1&sid=30>, 19.05.2012.
University System of Georgia İnternet Sitesi, ***A Brief History of the Internet,*** <http://www.usg.edu/galileo/skills/unit07/ internet07_02.phtml>.
WAGLEY John, ***Court Shuts Site Selling Key Logging Spyware***, <http://www.securitymanagement.com/news/court-shuts-site-selling-key-logging-spyware-004868>, 17.07.2013.