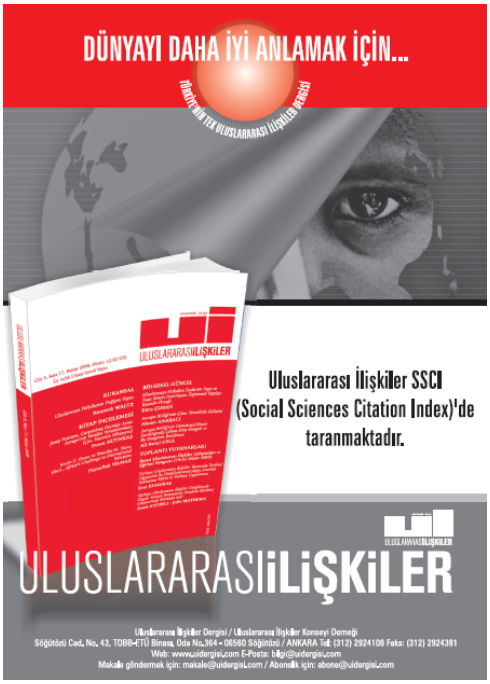
ULUSLARARASI İLİŞKİLER
Akademik Dergi

Yayın ilkeleri, izinler ve abonelik hakkında ayrıntılı bilgi:
E-mail: bilgi@uidergisi.com
Web: www.uidergisi.com



NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik

Salih BIÇAKCI*

* Doç. Dr., Kadir Has Üniversitesi, Uluslararası İlişkiler Bölümü

Bu makaleye atıf için: Bıçakcı, Salih, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler*, Cilt 10, Sayı 40 (Kış 2014), s. 101-130.

NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik

Salih BIÇAKCI*

ÖZET

Siber uzayın sivilleşmesiyle birlikte Vestfalya sisteminin getirdiği ulus devlet modeli derinden etkilenmiştir. Soğuk Savaş sonrasında ortaya çıkan bu yeni dönemde nükleer savaşın ve çekişmenin izlerini görmek mümkündür. Siber Uzayın günümüzde karşı karşıya kaldığı tehditler ve bunların henüz netleşmemiş sınırları örneklerde net olarak görülmektedir. NATO gibi uzun soluklu bir güvenlik ittifakına ve üyelerine bu yeni güvenlik ortamında yapılan siber saldırılar, gelecek adına önemli ipuçları vermektedir. Bu makalede NATO'nun bu yeni tehditlere karşı aldığı tedbirler ve belirlenen siber güvenlik stratejileri ortaya çıkaran süreç tartışılmıştır.

Anahtar Kelimeler: Siber Güvenlik, Hacker, Cracker, Stuxnet, NATO, Siber Strateji, Kosova, Estonya, Gürcistan, İran.

NATO's Emerging Threat Perception: Cyber Security in the 21st Century

ABSTRACT

Westphalian state system has been deeply affected from the civilianization of the cyber space. It is possible to see the traces of nuclear war and its competition in this new post-Cold War period. The contemporary threats against the cyber space and their vague boundaries could clearly be seen in the examples. Cyber attacks in this new security environment towards long lasting alliance NATO and its members are giving important clues for the future. In this article, one discussed defensive measures of NATO for these new threats and the process, which determined the cyber security strategies. Upon this cyber defense strategy, NATO tries to level the cyber capabilities of its members and takes the necessary steps to achieve this goal. The Lisbon summit endorsed the preparation of a new strategy that includes cyber defense and protection of the critical information infrastructure.

Keywords: Cyber Security, Hacker, Cracker, Stuxnet, NATO, Cyber Strategy, Kosovo, Estonia, Georgia, Iran, Cyber Espionage.

* Doç. Dr., Uluslararası İlişkiler Bölümü, İİSBF, Kadir Has Üniversitesi, İstanbul. E-posta: asbicakci@khas.edu.tr. Bu makale, yazarın İstanbul Bilgi Üniversitesi Yayınevi tarafından Mustafa Aydın'ın editörlüğünde hazırlanan Güvenlik Çalışmaları Serisi'nin yedinci kitabı olan *21. Yüzyılda Siber Güvenlik*, (İstanbul: Bilgi Üniversitesi Yayınları, No. 436, Ağustos 2013) başlıklı kitabı esas alınarak hazırlanmıştır.

Giriş: İnternetin Ortaya Çıkışı ve Gelişimi

Bilgisayarın taşınabilir hale gelmesi ve internete erişimin yaygınlaşmasıyla birlikte 21. yüzyılda dünyaya bunların şekillendireceği belli olmuştu. Bireyler arasında coğrafi mesafeler azalır ve iletişim alışkanlıkları değişirken, yeni teknolojiler sağladıkları imkânların yanı sıra beklenmedik problemlere de sebep olabilmektedirler. İnternet bunun en güzel örneklerinden birisidir. İletişim, haberleşme ve paylaşma alanı olarak ortaya çıkan internet, aynı zamanda dünya üzerindeki mesafeleri kaldırarak aynı düşünceyi, hobiyi, inancı, merakı, ideali paylaşan insanları bir araya getirmiştir. Öte yandan internetin Çin'de yaşayan bir insanın Güney Afrika'daki insanların durumundan, ekonomik problemlerinden ve devlet ilişkilerinden haberdar olmasını sağlayarak dünya vatandaşlığı yönünde adım atılmasını sağladığını söylemek de abartı olmayacaktır. Üstelik bilgisayar teknolojisinin hızla gelişmesi internetin yayılmasını günden güne daha da arttırmaktadır.

İnternetin temel unsurları bilgisayar, kullanıcı ve ağdır. Bilgisayar teknolojisinin gelişmesi ve değişimi ağ teknolojisinin yeteneklerini de arttırmaktadır. Bilgisayar teknolojisinin ilk geliştiği yıllarda ana bilgisayara ancak tek bilgisayarın erişimi söz konusuydu. İki bilgisayarın aynı anda ana bilgisayara erişimi için gereken işlemci ve iletişim protokollerinin gelişmesiyle ağ kavramı ortaya çıktı. Zamanla dosya aktarım protokolü (*File Transfer Protocol* - FTP) ve aktarım denetim protokolünün (*Transmission Control Protocol* - TCP) gelişmesiyle birlikte çok sayıda kullanıcı, sunucu bilgisayara bağlanabilir hale geldi. Günümüzde telsiz iletişim (*wireless communication*) teknolojisinin gelişmesi ve akıllı telefon ve tabletler ile geniş kullanım alanları bulması ağ teknolojisinin önemini daha da arttırmıştır. Benzer şekilde sistemin esnekliği de politik ortamın elverdiği ölçüde büyüdü ve gelişti.[1] Soğuk Savaş yıllarında ABD ile müttefiki ülkeler arasında teknoloji ve bilgisayar kullanımı hızla artarken, AB'nin uyguladığı ithalat rejimi CoCoM (*Coordinating Committee for Multilateral Export Controls*) kuralları gereği Varşova Paktı ülkelerine nükleer silahların yönlendirilmesi ve hedef sistemleri için kullanılabileceği gerekçesiyle bilişim sistemlerinin satılmasını engelliyordu.[2] Soğuk Savaşın bitmesiyle birlikte o döneme ait yasaklar da uygulamadan kalkınca, sivilleşen ve genel kullanıma açılan internetin kullanıcı sayısı bir anda arttı. 2011'te yapılan ölçümlerde 2.267.233.742 kişinin internete girdiği tespit edildi.[3] Bu artışla birlikte dijital verilerin aktığı ve veri işleyen bütün cihazların bağlanabildiği bir sanal dünya oluştu. Foucault'un dediği gibi gücü oluşturabilecek bilgilerin aktığı bu alan kısa sürede güvenlik problemleriyle anılır hale geldi.[4] Siber uzayın oluşmasıyla ortaya çıkan güvenlik sorunlarının sadece bilgisayar mühendislerinin ya da ağ uzmanlarının çözebileceği teknik içerikli problemler olmadığı da kısa sürede anlaşıldı. Siber uzayın gelişmesiyle birlikte sosyal gerçekliğin en önemli iki katmanı olan mekân

1 Manuel Castells, *The Rise of the Network Society*, West Sussex, Wiley-Blackwell , 2010, s. 355-406.

2 Roland B. Schmitt, *The New Era in U.S. Export Controls. Report of a Workshop*, Washington D.C., National Academy Press, 1992, s. 14. James Andrew Lewis (der.), *Computer Exports and National Security: New Tools for a New Century*, The CSIS Press, Washington D.C., 2001, s. 10-12.

3 Http://www.internetworldstats.com/stats.htm (Erişim tarihi: 11 Mart 2012).

4 Michel Foucault, *Discipline and Punish: The Birth of the Prison*, New York, Vintage Books, 1979, s. 27.

ve zaman bağıntısı değişmeye başladı. Fiziksel uzaklıklar ve bilgi aktarımı için gereken zaman internetin oluşturduğu hızla kısaldı. Bu yeti kısa sürede ekonomik, politik ve askeri alanlarda kullanılmaya başlandı. Bankalar, borsalar ve her türlü ticari yapı, yeni teknolojiyi kullanarak daha geniş alanda hizmet vermeye başladı. Devletler de küçük ölçekte altyapı hizmetlerinin dağıtımında, makro ölçekte ise dış misyonlarıyla iletişimden diplomasiye, istihbaratî bilgi toplamada savunma teknolojilerine kadar geniş bir çerçevede bilgi teknolojisi ve siber uzayın imkânlarından yararlanmaya başladılar.

Bilişim teknolojisinin bu herkesi birbirine bağlayan ağ yapısı dikey kurumsal hiyerarşiyi de azalttı. Böylece yöneticilerin her düzeydeki personellerine erişebilmeleri kolaylaştı. Toplumsal düzeyden bakıldığında artık insanların bilgi alışverişinde bulunmalarının ağla bağlanmış bilişim sistemleri sayesinde daha kolay olduğunu görüyoruz. Toplumsal bağlılığı bu derece farklılaşmış toplulukları Sanayii Devrimi döneminde oluşmaya başlamış algılarla yönetmenin kolay olmayacağı aşikârdır. Uluslararası ilişkilerin temel aktörlerinden olan devletler de bu topluluğu daha kolay yönetebilmek için hızla bilişim teknolojilerini kullanmaya başladılar. Fakat devlet sisteminin yavaş hareket eden yapısını bu teknolojik değişime uygun olarak yeniden yapılandırmak beklenenden zor oldu. Teknoloji birçok sahada devlet yönetiminin vatandaşlarıyla etkileşimini etkinleştirdi, devletin bilgiye ulaşımını hızlandırdı ve vatandaşları eskisine göre daha rahat şekilde kontrol etmesini sağladı.

Fakat hızla genişleyen bu alan sistemlerin işlemez hale gelmesinden kayıtların silinmesine kadar birçok riski de beraberinde getirdi. Gelişmiş ülkelerde bütün sektörlerin hizmetlerini siber uzaya taşımasıyla birlikte kritik öneme sahip bilgiler telefon hatlarından, eşeksenel kablolarından, fiber optik kablolardan ve elektro-manyetik dalgalar üzerinden akmaya başladı. Kendine fayda sağlamak isteyen kişiler, gruplar ve organizasyonlar bu bilgilere erişerek ya da hizmeti durdurarak güçlerini arttırmak istediler. Yine de siber uzayda gerçekleşen güvenlik problemlerinde çoğunlukla internetin coğrafi mekândan nispeten bağımsız olma özelliği kullanılmaktadır. Bu yüzden siber güvenlik olayları sıklıkla ulus-devlet sınırlarının ötesine geçerek uluslararası işbirliğini zorunlu hale getirmektedir. Bir taraftan devletler ulusal ve uluslararası seviyede farklı tedbirler almanın güvenlikleri için gerekli olduğunu hissederken, diğer taraftan siber saldırıların savaşa dönüşebileceği endişesi ve çıkabilecek bir dünya savaşının siber uzayda yaşanması ihtimali uluslararası politikayı da şekillendirmektedir.[5] Öte yandan ulusal güvenliklerini sağlamak için siber uzaydaki gelişmelere odaklanan birçok devletin çıkaracağı kanunlar ile belirleyecekleri politik tavırlar[6] siber uzayın gelişiminin de yönünü belirleyecektir.[7]

5 Nazlı Choucri, "Introduction: Cyber Politics in International Relations", *International Political Science Review*, Cilt 21(3), 2000, s. 243.

6 Joseph S. Nye Jr., *Cyber Power*, Cambridge, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010; Tim Jordan, *Cyber Power: An Introduction to the Politics of Cyberspace*, Londra, Routledge, 1999, s. 208.

7 Robert O. Keohane ve Joseph S. Nye Jr., "Power and Interdependence in the Information Age", *Foreign Affairs*, Cilt 7 (5), Eylül-Ekim 1998, s. 81-94.

ARPANET ve İnternetin temeli

İnternet yakın zamanda dünyanın kullanımına açılmış ve hızlı yayılmış olsa bile temelleri Soğuk Savaş yıllarında atılmış bir ağ sistemidir. O tarihten bu yana işleyişten kullanım şekline kadar birçok konuda değişimler yaşandı. Bugün güvenlik rekabetinin parçası olarak gelişen siber uzay, devletlerin ve grupların güç yarışını sürdürdükleri bir alana dönüştü.[8]

4 Ekim 1957'de SSCB'nin dünya yörüngesine ilk yapay uyduyu yerleştirmesi ve ardından 3 Kasım'da bu sefer canlı bir köpekle birlikte Sputnik II'yi uzaya göndermesi, o güne kadar iki kutuplu dünyada yaşanan rekabette lider konumda olduğunu düşünen ABD'nin ilk defa nükleer tehdidi hissetmesine sebep oldu.[9]ABD Başkanı Eisenhower'ın Bilim Başdanışmanı James Killian'ın belirttiği gibi, Sputnik sonrasında "Amerikan bilimine, teknolojisine ve eğitimine itimadın aniden buharlaştığını"[10] gören yönetim Şubat 1958'de ABD'nin rekabet gücünü geliştirmeye katkı yapması için İleri Araştırma Projeleri Ajansı'nı (*Advanced Research Projects Agency* – ARPA) kurdu.[11] Ajansın en önemli görevi Sovyetler Birliği'nin ispatlanmış teknolojik üstünlüğünü alt etmekti. ABD'nin milli güvenliğini sağlamak için farklı branşlarda araştırmalar yapan bilim insanlarını şemsiyesi altına alan ARPA'daki projeler uzay araştırmalarının yanı sıra balistik füze savunması, dünya üzerinde nükleer test yapılan coğrafi noktaların saptanması gibi konuları da içeriyordu. ARPA'nın ilk bilgisayara yönelik çalışmaları ise teknolojinin gelişimiyle ilişkilidir. O dönemde bilgisayar işlemcilerinin çok sayıda kullanıcının bilgisayar sistemine girişini desteklememesi araştırmaların zaman almasına ve işlemlerin gereken hızda yürütülmesine engel oluyordu. Fakat işlemci teknolojisinin gelişmesiyle birlikte çoklu kullanıcının ana bilgisayara bağlanabilmesi konusu tartışılmaya başlandı. Böylece uzay çalışmalarına katkı yapabilecek bilim insanlarını tek bir ağda buluşturmanın teknik alt yapısı da hazırlandı. 1958'de kurulan NASA'nınihtiyaç duyduğu kritik araştırmacı kitlesini oluşturmak için 1962 'de oluşturulan İleri Araştırma Projeleri Ajansı Ağı (*Advanced Research Projects Agency Network* - ARPANET) ABD'nin ihtiyaç duyduğu gelişme ortamını sağladı.

Küba füze kriziyle birlikte bütün Kuzey Amerika'nın vurabilecek hale gelmesi ve SSCB'nin füze teknolojisini denizaltılara yerleştirecek kapasiteye ulaşmasıyla ABD güvenlik politikasında "Karşılıklı Kesin İmha" kavramı (*Mutually Assured Destruction* - MAD) yoğun şekilde gündeme geldi. MAD'in yanısıra tartışılan diğer bir konuda nükleer bir saldırı sonrasında iletişim hatlarının çalışmasını sağlamaktı. ARPANET'in saldırılardan etkilenmemesi için neler yapılması gerektiği tartışmalarında Rand'dan Paul Baran "fiziksel saldırı sonrasında kalan en büyük grupla elektrik bağlantısı sağlayarak" iletişimi sür-

8 Nye, *Cyber Power*; Jordan, *Cyber Power*, s. 208.

9 Cristina Carbone, "Staging the Kitchen Debate: How Splitnik Normalized in the United States", Ruth Oldenziel ve Karin Zachmann (der.), *Cold War Kitchen Americanization, Technology and European Users*, Cambridge, The MIT Press, 2009, s. 59-81; Ilina Kohonen, "The Space race and Soviet Utopian Thinking", *The Sociological Thinking*, Cilt 57 (1), Mayıs 2009, s. 114.

10 Columba Peoples, "Sputnik and 'skill thinking' revisited: technological determinism in American responses to the Soviet Missile Threat", *Cold War History*, Cilt 8(1), Şubat 2008, s.61.

11 National Research Council, *Innovation in Information Technology*, Washington D.C., The National Academies Press, 2003, s. 60.

dürebilecek bir ağ yapısını tartışmaya açtı.[12] Baran'ın önerdiği merkezi olmayan ve dağıtık çalışan ağlar kavramı üzerine yapılan tartışmalar sonrasında altyapı buna göre düzenlendi. 1970'lerde internetin temeli olan askeri nitelikli ARPANET, ABD'nin müttefiklerinde gelişmeye başlayan ağ sistemleriyle (İngiltere'deki Ulusal Fizik Laboratuvarındaki (*National Physical Laboratory*) ticari ağ ve Fransa'daki araştırma ağı olan *Cyclades*) birleştirildi. Böylece uluslararası bilgisayar ağlarının oluşumuyla internetin (*International Network of Computer Networks* - Bilgisayar Ağlarının Uluslararası ağı) nüvesi ortaya çıktı.[13]

Bilgisayar ağlarının hızla büyümesi yeni teknoloji merakını arttırırken, 1971'de ARPA'nin ileri teknolojiler sahasındaki ortaklarından birisi olan *BBN Technologies*'da çalışan Bob Thomas ilk kendini çoğaltan (*self-replicating*) programı yazdı. *Creeper* adını verdiği programı *TENEX* işletim sistemiyle çalışan *DEC PDP-10* bilgisayarlarına yükledi. *Creeper* kısa sürede ARPANET'te hızla yayılmaya başladı. Program bulaştığı bilgisayarlarda "I'm the creeper, catch me if you can!"[14] mesajını ekrana yazıyordu. Problem anlaşıldıktan sonra *Creeper*'ı silmek üzere *Reaper* adında bir program yazıldı. Böylece ARPANET sisteminde ortaya çıkan ilk "solucan" (*worm*) siber güvenliğe yönelik oluşacak gelecek tehditlerin ilk işaretçisi oldu.

ARPANET dâhil olmak üzere birçok sunucunun birbirine bağlandığı sistemde kullanıcı sayısı hızla artmaktaydı. Kullanıcıların sunucular üzerinden dosya değişimi için gerekli olan dosya aktarım protokolünün (*File Transfer Protocol* - FTP) geliştirilmesiyle birlikte gizli ya da anonim dosyalar üzerinde ortak çalışabilme imkânı da arttı. Fakat kullanıcıların bilgisayarlarının birbiriyle haberleşebilmesi için geliştirilen paket değişim protokolü (*Packet Switching Protocol*) az sayıda bilgisayarda problem oluşturmazken, kullanıcı sayısı arttıkça iletişim de aksıyordu. Bu sorun, düğümler arasında dosyaları aktarırken önce paketlere bölen ve adrese ulaştığında parçaları birleştirilerek yeniden oluşturan gönderim kontrol protokolü (*Transmission Control Protocol-TCP*) sayesinde aşıldı ve iletişim daha da hızlandı.

Kısa bir süre sonra İngiltere Kraliçesi II. Elizabeth 26 Mart 1976'da Kraliyet Sinyal ve Radar Kurumu'ndan ilk elektronik postayı atarak, iletişimi yeni bir seviyeye taşıdı. Fakat internetin haberleşme ve dosya paylaşımındaki ayrıcalığından hala sınırlı sayıda kişi faydalanabiliyordu. Bu durumu değiştirecek olan kişisel bilgisayarların ilk prototipinin 1970'te elektronik parçaları kendin yap projesi (*DIY- Do it yourself*) olarak piyasaya çıktığında beklenenden fazla ilgi gördü. 1975'de "kişisel bilgisayar" terimi ilk defa kullanıldığında *Altair 8800* birçok evde yerini almıştı. Eylül 1975'de piyasaya çıkan *IBM 5100*'le birlikte kullanıcıların artmasıyla bilgisayar ve ağ kültürü daha da gelişti. Bilgisayar satışlarının artışını takiben bir bilgisayar firmasının tanıtacağı yeni ürün için davet mektubunu genel ağa göndermesiyle birlikte ilk *spam* mesajı da gönderilmiş oldu.

12 Paul Baran, "On Distributed Communications Networks", Rand Corporation, Eylül 1962, http://www.prgs.edu/content/dam/rand/pubs/papers/2005/P2626.pdf (Erişim tarihi: 07 Haziran 2012).

13 Laura K. Brendan, "Arpanet: An Efficient Machine as Social Discipline", *Science as Culture*, Cilt 10 (1), 2001, s. 76-77.

14 "Ben sürüngenim, yakala beni yakalayabilirsen!"

Soğuk Savaşın Sonu ve Siber Uzay

1980'lere geldiğimizde bilgisayarların artışıyla birlikte ağlara katılım da artmıştı. 27 Ekim 1980'de ARPANET, durum mesajlarına (*status message*) bulaşan virüs sebebiyle 72 saatliğine durdu.[15] ARPANET ve ağların kullanıcı kitlesinin artması gerçek dünyayı dolaylı da olsa etkileyebilecek dijital bir alan oluşmasını sağlamış, alan genişlerken güvenlik teorisinin temellerinden birisi olan risk kavramı da İnternet bağlantılı olarak tartışılmaya başlamıştı.[16] ARPANET eskiden kontrolün yüksek olduğu bir alan iken, büyüyüp genişledikçe, ağa yönelik tehditler ve riskler de artmaya başlamıştı.[17]Artık sistem kendi dinamikleri yanında kullanıcıların müdahalelerine de açık hale gelmişti.

1982'de bilim kurgu yazarı William Gibson, *Burning Chrome* başlıklı eserinde bu yeni gelişen siber alan için "siber uzay" kavramını kullandı. 1984'de yazdığı *Neuromancer* romanında kavramı daha da detaylandırarak, siber uzayı "milyarlarca meşru kullanıcı tarafından her gün tecrübe edilen uzlaşılmış bir halüsinasyon" ve "tasavvur edilemez karmaşa" şeklinde tanımladı.[18] Gibson'un ifadeleri geleceğe ait önemli işaretler taşıyordu. 1982'de ABD Savunma Bakanlığı ARPANET'teki tehditlerin artması üzerine, ABD askeri verilerini taşıyacak ayrı bir ağ oluşturmaya karar verdi. Böylece Aralık 1982'de ARPANET ve MILNET olarak iki ayrı ağ ortaya çıktı. ARPANET sivil araştırmalar için kullanılmaya devam ederken, MILNET sadece askeri amaçla kullanılır hale geldi. Böylece sivil siber uzayın temelleri atıldı.

Siber uzayı ve dinamiklerini anlamak siber güvenlik konusundaki gelişmeleri daha net anlamamızı sağlayacaktır. Siber uzayı tanımlamak için yola çıkanlar için farklı teknolojik özelliklere odaklanmaktadır. Araştırmacılardan birçoğu sadece internet ortamına bu ismin verilmesinin uygun olduğunu düşünmektedir. Hâlbuki siber uzay bütün bilişim sistemlerini ve kullanıcıları içine alan bir evrendir. En genel anlamda, insanların birbirine bağlı bilişim sistemleriyle etkileştiği ve birbirine bağlı bilişim sistemlerinin birbirleri arasında ya da insanlarla iletişim içinde olduğu fiziksel olmayan alana *siber uzay* diyebiliriz. Bu alanı paylaşan aktörler ile ve unsurların çokluğu ve bütün katılımcıları tanımda

15 Arpanet'in için daha bütün düğümler (*node*) aralarında durumlarını gösteren (*status*) mesajlar göndermekteydi.Düğüm mesajı alır almaz çöp kutusuna atarak yok etmek üzere programlanmıştı.Fakat Los Angeles yakınlarındaki bir düğümün mesajları silememesi yüzünden durum diğerlerini de etkileyince sistem durdu. Detaylı bilgi için bkz.; Eric S. Rosen, "Vulnerabilities of network control protocols: an example", *Software Engineering Notes*, Cilt 6(1), Ocak 1981, s. 6-8.

16 Ulrich Beck, *Risk Society Towards A New Modernity*, Londra, Sage Publications, 1992, s. 29-30; Bill Durodie, "The Limitations of Risk Management", *Tidsskriftet Politik,* Cilt 8 (1), 2005, s. 14-21.

17 Wendy Hui Kyong Chun, *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*, Cambridge, The MIT Press, 2006, s. 247-297.

18 Orjinal tanım şöyledir: Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding." William Gibson, *Neuromancer,* New York, Ace Books, 1984, s. 69.

belirtme endişesi bütün tanımları biraz eksik bırakmaktadır. Fakat siber uzayı oluşturan katmanları açıklamak tanımların eksikliğini tamamlayacak ve alanın özelliklerini net bir şekilde ortaya koyacaktır.

Fiziksel Katman

Reel ve fiziksel dünyadaki donanım ile insanlar ve varlıklar siber uzayın oluşmasını sağlamaktadır. Siber uzayın değeri fiziksel dünya ile ne kadar etkileştiğine bağlı olarak değişmektedir. Fiziksel katmanın ana unsurunu kullanılan teknoloji oluşturmaktadır. Bilgisayarın ana kartı (*main board*), işlemcisi (*central processing unit*), hafızası (*random-access memory*), diski (*hard disk*) ve diğer ekipmanlarından oluşan bir ünitenin yanı sıra, diğer ağlarla bağlantısını sağlayan bir ethernet kartı ve kablolara ihtiyaç duyulmaktadır. Bir ağın diğer ağlarla iletişimini sağlayan yönlendirici (*router*) ve diğer ekipmanlara da ihtiyaç vardır. Fiziksel alandaki bu ekipmanların varlığı olmaksızın siber uzayın varlığı şimdilik söz konusu değildir.

Siber uzay'ın fiziksel varlığının sadece bilgisayar ekipmanlarından oluştuğunu düşünmek de yeterli olmayacaktır. Ayrıca akıllı telefonlar, oyun konsolları, televizyon sistemleri, uydu alıcıları gibi ağ ortamında iletişim kuran bütün elektronik aletler de bu ortamdadır. Öte yandan ülkelerin temel altyapılarının işleyişi için gerekli olan kritik alt yapı ile ülkelerin birbirleriyle bağlantı içinde olmasını sağlayan internet omurgası (*backbone*) da bu iletişimin devamlılığı için esastır. Herhangi kopma ya da kesilme iletişimi kesintiye uğratır ve o ülkenin internete erişimini genel olarak ortadan kaldırır. Bu tür durumlarda siber uzaya erişim ancak yedek hatlarla ya da uydu üzerinden sağlanabilir.

Ülkelerin internet çıkışlarının kontrol altına alınması çabasıyla ilgili olarak üç farklı örnek vermek mümkündür. İlk örnek olarak, 2010'da ABD'de Senatör Joseph Lieberman ve Susan Collins tarafından hazırlanan ve Amerikan Başkanına herhangi bir tehlike anında interneti kapatma yetkisi tanıyan "Siber Uzayın Milli Değer Olarak Korunması Kanun Taslağı" verilebilir.[19] Bu tehlike anları "Milli Siber Acil Durumları" (*National Cyber Emergency*) olarak tanımlanmıştı. Bu konu tartışılırken siber saldırılara kinetik saldırıyla cevap verilebileceği de gündemi gelmişti.[20] Böyle bir bakış açısının yaratacağı problemleri tartışan OECD raporu siber güvenliğe askeri yaklaşımların hata olacağını belirterek, bölgesel internet kapatma sistemlerinin beklenmeyen sonuçlar doğurma ihtimali üzerinde durmuştur.[21]

19 Senato'daki İç Güvenlik Komitesinden geçen bu tasarı 2011 başında hala kanunlaşamamıştı. 706 sayılı İletişim Kanunu'na benzer hakları ABD Başkanı'na tanıdığından gündeme geldi. Kanun taslağının tam metni için bkz.; http://www.govtrack.us/congress/bills/111/s3480 (Erişim Tarihi:: 21 Haziran 2013).

20 Charles L. Glaser, "Deterrence of Cyber Attack and US National Security", *George Washington University Cyber Security Policy and Research Institute,* 1 Haziran 2011, http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-5%20Cyber%20Deterrence%20and%20Security%20Glaser.pdf (Erişim tarihi: 21 Ocak 2013).

21 Ian Brown ve Peter Sommer, *Reducing Systemic Cybersecurity Risk*, OECD/IFP Proje Raporu, 14 Ocak 2011.

İnternetin tehlike anında kapatılması fikrinin ABD'de tartışıldığı o günlerde Tunus'ta başlayan halk hareketi Mısır'a sıçramış, halk internet üzerinden sosyal medyayı kullanarak kitlesel organizasyonlar yapmaya başlamıştı. Dönemin Cumhurbaşkanı Hüsnü Mübarek halk hareketini önleyebilmek için Mısır'ın internete erişimini kesme yoluna gitti. 25 Ocak'ta *twitter*'ın sunucusuna erişimin engellenmesiyle başlayan hamle, 26 Ocak'ta *Facebook*'un ve 27 Ocak'ta da *Blackberry* servisinin engellenmesiyle devam etti. Her ne kadar engellemeler *twitter* kullanımını azaltmayı başardıysa da Mısırlı *twitter* kullanıcıları yurtdışındaki arkadaşları vasıtasıyla mesajlarını dünyaya iletmeye devam ettiler.[22]

Yine 2010 Haziran'da *VirusBlokAda* isimli virüs temizleme programı üreticisi *MS Windows* işletim sistemlerini ve *Siemens* endüstriyel yazılımlarını etkileyen bir bilgisayar solucanının (*Stuxnet*) bulunduğunu açıkladılar. Kimin tarafından yazıldığı hala bilinmeyen solucanın hedefi Siemens Programlanabilir Mantıksal Denetleyicileriydi. Saldırı sonrasında yapılan değerlendirmelerde en çok zararı İran'daki nükleer tesislerin aldığı belirlendi.[23] Birçok saldırı metodunun birleşimi ve açıklar kullanılarak hazırlanan bu solucan, İran nükleer tesislerinin üretim hedeflerini geciktirmişti. İran, nükleer tesislerine yapılan bu saldırı sonrasında kendine ait temiz bir intranet kurarak internet bağlantısını sınırlamayı planlamaya başladı.[24]

Görüldüğü gibi ülkelerin internet erişimini sağlayan altyapı zaman zaman politik kararlar tarafından şekillendirilebilmektedir. Tehdit ve güvenlik hissi ise internet kullanımını etkilemektedir.

Kodlar Katmanı ve Yazılım

Siber uzayın varlığını fiziksel alandan sanallığa yaklaştıran katmanlardan birisi de kodlar katmanıdır. Bütün fiziksel katman unsurları (anakartlar, işlemciler, RAM'ler, diskler) ancak kodlarla kullanılır hale gelmektedir. "Doğru – Yanlış" ya da "1 – 0" düzleminde oluşan programlama dilleri sayesinde işlemcinin nasıl çalışacağı belirlenmektedir.

Bütün donanım ekipmanlarının bütünlük içinde yürütülerek, verilen komutlara cevap vermesini sağlayan temel platform olan işletim sistemleri bilgisayar donanımlarının gelişmesine bağlı olarak gelişmiştir. 1960'lı yıllarda bir oda büyüklüğünde olan bilgisayar donanımlarına ancak sınırlı sayıda erişim sağlanırken, 1980'li yıllarda taşınabilir bilgisayarlar kullanılmaya başlanmıştır. Günümüzde ise akıllı telefonların, televizyonların ve çeşitli multimedya platformlarının çalıştırılması için gelişmiş işletim sistemleri

22 Mısır'da protestolar sırasında internet erişimin kapanması hakkındaki detaylı zaman şeridi için bkz., http://www.flickr.com/photos/ramyraoof/5814392791/sizes/l/in/photostream/ (Erişim tarihi 22 Nisan 2012).

23 Http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99 (Erişim tarihi: 22 Nisan 2012).

24 Ryan Paul, "Iran moving ahead with plans for national intranet", http://arstechnica.com/tech-policy/news/2012/04/iran-plans-to-unplug-the-internet-launch-its-own-clean-alternative.ars (Erişim tarihi: 22 Nisan 2012).

kullanılmaktadır. 1975'de kurulan *Microsoft*'un *Windows* işletim sistemi dünya üzerinde %50'nin üzerindeki pazar payıyla bilgisayarlarda en çok kullanılan işletim sistemidir.[25] Bu rakamı *Linux* işletim sistemleri[26] ve *Unix* tabanlı *Mac OS X* işletim sistemi takip etmektedir.

İşletim sistemlerinin ardından internetteki içeriğe erişmemizi sağlayan kodlar gelmektedir. İnternetin temel taşını oluşturan web sayfaları da kodlar sayesinde hazırlanmaktadır. Günümüzde kullanıcılar daha fazla etkileşim kurabilmek için web içeriğinin programlanmasında *Phyton, Ruby, Perl, PHP, ASP.NET, Java* gibi diller kullanmaktadırlar. Kodlama içeriğinin yoğun olduğu bu tür platformlarda, internet üzerinden başkaları tarafından yazılmış kodları kopyalayarak kullanan programcılar için sitelerinin kısa sürede bilgisayar korsanları tarafından ele geçirilme riski vardır. Ayrıca programlama dillerini yorumlayan platformların güncellenmemesiyle oluşan güvenlik zafiyetlerine de sıkça rastlanılmaktadır. Görüldüğü gibi birçok bileşenin kontrol edilmesiyle oluşan siber güvenlik, en başta insan unsuru olmak üzere en küçük hatalardan etkilenmektedir.

İçerik Katmanı

İçerik katmanı öncesinde belirtilen bütün katmanlar aslında bir çerçeve katman oluşturmaktadır. Fiziksel ve kodlar katmanı olmadan içeriğin internet üzerinde sunulabilmesi mümkün değildir. Fakat içerik ve onun içerdiği mesaj olmadan da interneti oluşturan diğer katmanların anlamı zayıflayacaktır. İçerik katmanıyla internet paylaşılan, taraf olunan ve eleştirilen bir ortaklık oluşturmaktadır. İçerik katmanı sadece mesaj ileten bir medya olmanın ötesinde finansal işlemlere ait verilerin tutulduğu, ülkelerin stratejik bilgilerinin depolandığı, hastanelerdeki hastaların tıbbi bilgilerinin tutulduğu bir ortamdır. Fakat içeriklerin çeşitliliği ve benzerliği hiyerarşik bir düzenleme yapılması gerekliliğini değiştirmemektedir. Farklı kurumlarda yönetimler çalışanlarına özgürce kurumun ağına bağlanabilme izni verirken, yine aynı çalışanların ağdaki bütün verilere erişmelerine müsaade etmez. Bilgi güvenliğini sağlamak isteyen kurumlar kendi çalışanları için hiyerarşiler oluşturmak zorundadırlar. Her kullanıcının ağ üzerindeki bütün belgelere istediği şekilde erişmesi kritik bilgileri tehdit eder. Veri hiyerarşisi mantığı günümüzde kullanılan birçok işletim sisteminde uygulanmaktadır. Böylece sistem ve güvenliği hakkında bilgi sahibi olmayan kullanıcıların sistemin tamamını tehlikeye atmasının önüne geçilmeye çalışılmaktadır. Öte yandan pratik, gündelik ve geçici sebeplerle veri erişimi hiyerarşisinin

25 Daha detaylı bilgi için bkz.,http://www.osnews.com/story/25485 (Erişim tarihi: 23 Nisan 2012) Öte yandan *Microsoft*'un geliştirme aşamasında Amerikan Milli Güvenlik Ajansı'ndan (*National Security Agency* - NSA) yardım aldığı farklı kaynaklarda yazılmıştır. Bundan daha korkutucu olan NSA'in bu yardımlara karşılık işletim sistemine arka kapı (*backdoor*) eklediği iddiasıdır. Bkz., http://www.tomshardware.com/news/microsoft-windows-7-nsa-backdoor,9130.html (Erişim tarihi: 23 Nisan 2012).

26 Linux işletim sistemini oluşturan en temel öğe linux kernelidir. Bu kernel farklı derleme tercihleriyle her biri ayrı işletim sistemleri oluşturabilir. Başlıca tercih edilen linux sistemleri: Ubuntu, Linux Mint, Arch Linux, Fedora, Debian'dır. Http://lifehacker.com/5904069/five-best-linux-distributions (Erişim tarihi: 23 Nisan 2012).

kaldırılmaya çalışıldığı ve bunun da bilgi güvenliği sorunlarına yol açtığı durumları sıkça görmek mümkündür. Örneğin bir bürokratın üst seviyede yöneticisinin istediği verileri temin etmek için kişisel bağlantılarla erişilmemesi gereken verileri paylaşıma açtırması yoluyla bilgi sızıntısı olabilmektedir.

Kurumsal içerik katmanı ve sınırları dışında internet ortamında da kontrol dışı gelişen sınırlamalar olabilmektedir. Örneğin internet üzerindeki içeriklere erişmek için web sayfalarının adresleri dışında arama motorları kullanılmaktadır. Bu da aslında araştırılan konunun anahtar kelimelerini bir arama motoruna yazarak onun gösterdiği linklerin takip edilmesi anlamına gelir. Bu da internetin sınırının tercih edilen arama motorunun çerçevesi olduğunu göstermektedir. Günümüzde arama motorları sanıldığı kadar apolitik ve bağımsız hareket edememektedir. Örneğin *Google* sunucu çiftliklerinin yer aldığı ülke olan ABD, ülke güvenliği için koyduğu sınırları dikkate alarak belirli sitelerin isimlerinin arama sonuçlarından çıkarılmasını sağlamaktadır.[27] *Google*'ın indekslediği web sayfa sayısının tüm internet göz önüne alındığında %0.004'den %12'ye kadar bir aralıkta olduğunu söyleyen farklı kaynaklar bulunmaktadır.[28] Bu durumda internet içeriğine erişimin özgürce gerçekleştiğini söylemek mümkün değildir.

Düzenleyici Katman

İnternet ve içeriğin kullanımı ulusal hukuki düzenlemelerle de sınırlanmaktadır. Gelişmiş ülkelerin birçoğunun bu konuda hukuki düzenlemeleri bulunmaktadır. Türkiye'de bu mevzuat 5651 sayılı "İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun"la belirlenmiştir.[29] İçerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcının yükümlülükleri belirlenerek, içerik katmanında belirli konuların yayınlanmasına yasaklar getirilmiştir. Bunlar Kanun'un 8. Maddesinde şöyle açıklanmıştır:

> a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;
>
> 1) İntihara yönlendirme (madde 84);
>
> 2) Çocukların cinsel istismarı (madde 103, birinci fıkra);
>
> 3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190);

27 "Google's Transparency Report: US Leads the censorship brigade", http://www.firstpost.com/tech/googles-transparency-report-us-leads-the-censorship-brigade-349101.html (Erişim tarihi: 21 Ocak 2013). *Google*'un bu konuda yayınladığı şeffaflık raporları için bkz., http://www.google.com/transparencyreport/removals/government/ (Erişim tarihi: 21 Ocak 2013); Farklı bir örnek olarak Çin'in *Google*'ü sansürleme süreci için bkz., *Miguel* Helft ve David Barboza, "Google shuts China site in dispute over Cencorship", *The New York Times*, 2010, http://148.61.6.9/cms3/assets/A710F777-E74C-F8BD-F645CFB2BE41D80C/ehr/google_shuts_china_site_in_dispute_over_censorship.pdf (Erişim tarihi: 23 Kasım 2012).

28 Http://theroxor.com/2010/10/28/the-awesome-size-of-the-internet-infographic/ (Erişim tarihi: 01 Haziran 2012); http://www.quora.com/What-percentage-of-the-web-does-Google-index-and-how-has-it-changed-over-time (Erişim tarihi: 1 Haziran 2012).

29 Kanun metni için bkz., http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm (Erişim tarihi: 1 Haziran 2012).

4) Sağlık için tehlikeli madde temini (madde 194);

5) Müstehcenlik (madde 226);

6) Fuhuş (madde 227);

7) Kumar oynanması için yer ve imkân sağlama (madde 228), suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

İnternetin kavramsal manada sunduğu özgürlük ortamı bir çok ülkede yasama katmanının belirlediği çerçevede hareket eder. Bu noktada internet erişiminin hep de vurgulandığı kadar özgür bir ortam olmadığının altı çizilmelidir. Özellikle internetin yaygınlaşmasıyla birlikte organize suç örgütlerinin ve benzeri yapılanmaların siber uzayı iletişim için kullanmaya başlaması, devletlerin takip amaçlı bu haberleşmeyi izlediği yönündeki endişeleri gündeme getirmiştir. 11 Eylül saldırılarının ardından ABD'de bu tür takip faaliyetleri *Department of Homeland Security*'nin (İç Güvenlik Birimi) kurulmasıyla, daha belirgin kurallara bağlanmıştır. Örneğin İç Güvenlik Biriminden sızan bir dosyada sosyal medyanın belirlenmiş bazı anahtar kelimelerle izlendiği görülmüştür.[30] İnternetin pornografiden telif haklarına kadar farklı konularda yarattığı problemler devletlerin hukuki düzenlemeler yapmasına sebep olmaktadır. Bu düzenlemeler sadece otoriter ülkelerde değil, demokratik ülkelerde de uygulanmaktadır. Deibert ve diğerleri tarafından yapılan çalışma zannedilenin tersine birçok ülkede erişimin nasıl kontrol altına alındığını açıkça ortaya koymuştur.[31]

Düzenleyici katmanın en büyük problemi teknolojinin ve buna bağlı olarak içeriğin günden güne hızla yenilenmesi karşısında devlet bürokrasisinin bu gelişmeyi aynı hızla takip edememesidir. Siber uzaydaki tehditler ve çeşitliliğini sayısal artışı ister istemez devlet yapısını da daha hareketli olmaya zorlamaktadır. Güncel gelişmeler bunun kolay olmadığını göstermektedir. Öte yandan Uluslararası organizasyonlar da siber savaştan terörizme kadar işbirliği oluşturmaya çalışmaktadırlar. Fakat siber uzayın kendilerine sağladığı anonim olma örtüsünden faydalanmayı arzulayan ülkeler, hareket kabiliyetlerini anlaşmalarla kısıtlamak konusunda çok da istekli değillerdir.

Gelişen Hacker Kültürü

ARPANET genişlemesi ve nükleer füzelerin bilgisayarla ateşlenmesi fikri, varolan politik gündemle ilişkilendirilmiştir. İki unsur arasındaki bağlantı, 1983'de vizyona giren, Lawrence Lasker ve Walter F. Parkes tarafından yazılan Savaş Oyunları (*War Games*) isimli filmde nükleer gerginlikte bilgisayarın nasıl rol aldığını göstererek ortaya koyulmuştu. Filmde notlarını değiştirmek üzere okulun bilgisayarına girmek için uğraşan *hacker* David Lightman eriştiği bilgisayardaki oyunun daha önce oynadıklarından farklı olduğunu

30 Department of Homeland Security, *Analyst's Desktop Binder*, http://archive.org/details/AnalystDesktopBinder-Redacted-HowDhsMonitorsYouOnTheInternet (Erişim tarihi: 7 Haziran 2012).

31 Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, *Access controlled the shaping of power, rights and rule in Cyberspace*, Cambridge Mass., The MIT Press, 2010.

görür. Lightman'ın girdiği bilgisayar nükleer füzeleri kontrol etmek üzere geliştirilmiş bir sistemdir. Görevli kişilerin nükleer füzeleri ateşlerken anahtarı çevirmekte tereddüt etmeleri üzerine özel olarak hazırlanmış *NORAD* (*North American Aerospace Defense Command* - Kuzey Amerika Hava Sahası Savunma Komutanlığı) isimli bir bilgisayar bu misyonla görevlendirilmişti. Bilgisayar'ın içindeki *WOPR* (*War Operation Plan Response*) programı muhtemel SSCB nükleer saldırısını simüle etmekteydi ve simülasyon programı nükleer saldırı senaryosuna cevap verecek şekilde kurgulanmıştı. Filmde Lightman'ın bilgisayara izinsiz olarak erişirken başlattığı programın ve simülasyon modülünün gerçek hayatta etkili olduğunu fark etmesi üzerine olaylar gelişmeye başlar. Çok sayıda insan tarafından izlenen bu film sayesinde siber uzay ve güvenliği kavramları yaygınlaşmıştır. Filmde sıkça kullanılan *hacker* kavramı da toplumda popülerlik kazanmıştır.

War Games filmi ABD'de *hacker* kültürünün yaygınlaşmasına da sebep oldu. Milwaukee, Wisconsin'in telefon kodunu (414s) kendilerine isim olarak seçen 16-22 yaşları arasındaki altı gençten oluşan bir *hacker* grubu aniden şöhret oldu. 414s ismiyle bilinen bu grup, nükleer çalışmalarıyla ünlü New Mexico'daki Los Alamos Ulusal Laboratuvarına, 10.000 hastanın tedavi edildiği New York'taki Memorial Sloan-Kettering Kanser Merkezine, Los Angeles'ta bir bankaya ve Milwaukee bölgesindeki birçok okulun bilgisayarına izinsiz olarak erişmeyi başardı. Federal İnceleme Bürosu'nun (FBI) üç yıllık takibiyle 1984'te yakalanarak mahkûm edilen grubun saldırılarının en önemli sonucu ABD'nin bilgisayar korsanlığı hakkında yasal düzenleme yapmaya yönelmesidir. Özellikle 1984'deki *Computer Fraud and Abuse Act 18 USC 1030* (Bilgisayar Sahtekârlığı ve Suiistimali Yasası) bu konuda atılan en önemli adımlardan birisidir.[32] Yasada özellikle adaletin yönetimi, ulusal savunma ya da ulusal güvenlik için kullanılan Birleşik Devletler hükümetine ait bilgisayarların güvenliği konusunun altı çizilmişti. Saldırıların ortaya koyduğu diğer bir nokta da hangi eylemlerin bilgisayar korsanlığı sayılacağı, hangilerinin sayılamayacağının netleştirilmiş olmasıdır.

1980'li yıllardan itibaren ABD'de ortaya çıkan *hacker*[33] kültürü kısa sürede dünyaya yayılarak, tecrübelerin paylaşıldığı güçlü bir ağ haline gelmiştir. Bir tanıma göre *hacker* "aklını zorlamak (sınamak) için bilgisayarlarla uğraşan kişidir."[34] Diğer bir tanım da *hacker*ların, "sistemlerin detaylarını öğrenmekten hoşlanan ve bir sistemde çalışmak için gereken asgari bilgiyi edinenlerin tersine sistemle yapabileceklerini öğrenerek onun kapasitesini zorlamayı sevenler" olduğunu vurgulamaktadır.[35]

32 Yasanın tam metni için bkz., http://www.law.cornell.edu/uscode/text/18/1031 (Erişim tarihi: 7 Haziran 2011).

33 Türkçe'de *Hacker* kelimesinin karşılığı olarak Bilgisayar Korsanı, *Cracker* içinse Güvenlik Kırıcı karşılığı kullanılmaktadır.Her iki kelimenin Türkçe karşılıklarının kelimelerin farklılığını yeterince ortaya koyamadığını düşündüğüm için kelimeleri orjinal halleriyle kullanmayı tercih ettim. Kullanılan karşılıklar için bkz., http://www.bilisimsozlugu.net/ (Erişim tarihi: 31 Temmuz 2012).

34 Vir V. Phola, *Internet Security Dictionary*, New York, Springer, 2002, s. 57.

35 Pekka Himanen, *The Hacker Ethic and the spirit of the Information Age*, New York, Random House Trade Publishers, 2001, s. 7.

1950'lerde gelişmeyen başlayan *Hippi* hareketi ile açık kaynaklı programlar arasında önemli bir bağlantı vardır. Hippilerin yerleşmiş değerlere ve kontrole karşı duruşu bilgisayar temelli teknolojinin felsefesini de inşa etmiştir. Massachusetts Institute of Technology laboratuvarlarında gelişen felsefede programcılar ya da Steven Levy'in ifadesiyle *hacker* programlar geliştirip bunların kodlarını arkadaşlarının kullanımı için paylaşırlardı. İhtiyaç duyan programcılar da yazılan kodları geliştirip kendi ihtiyaçlarına göre düzenledi. Tamamen kişisel tercihlerle ve özgürce paylaşımlar yapılırdı. Burada paylaşımın arkasındaki açık kaynak felsefesi öne çıkmaktaydı. Hippilerin de benzer felsefeye sahip olmaları bu hareketin *hacker*lar tarafından desteklenmesini sağladı.

Teknolojiye ve onun sağladığı bilgi kaynaklarına herkes tarafından erişimin sağlanması için ortak hareket etmenin ilk örneklerinden birisi *California Berkeley*'deki *Leopold Plak* şirketine halkın genel kullanımı için konulan bilgisayardı. Böylece üniversitelerin dışına doğru dürüst çıkmamış kaynaklar halkın kullanımına sunulmuştur. Bu dönemde şekillenen *hacker* felsefesinin altı temel şartı oluşmuştur:

1) Bilgisayarlara ya da dünyanın nasıl işlediğini öğrenmemize yardım edecek her şey kontrolsüz paylaşılmalı ve problemin üzerinde çalışılabilmesi için hep erişilebilir olmalıdır: *Hacker*lar kendi alanlarını sadece bilgisayarlar ve siber dünya ile sınırlı görmeyip, dünya algılarını değiştirebilecek bütün kaynakların sınırsızca paylaşılması gerektiğini belirtmektedirler. Bu konuda sınırlama getirmeye çalışan bütün güçlerin ortadan kaldırılacağı da ima edilmektedir. *Hacker*lara göre bir konunun anlaşılabilmesi için bütünün onu oluşturan küçük parçalara ayrılması gereklidir. Bu bir programın hatalarının giderilmesi (*debugging*) ya da bir donanımın içinin incelemesi olarak da anlaşılabilir. Günümüzde sıkça kullanılan tersine tasarım (*reverse engineering*) yöntemi de bir mekanizmanın nasıl çalıştığını anlamak için çokça tercih ettikleri yollardan biridir.

2) Üretilmiş bilginin ulaşılabilir olmasının yaratıcılığı arttırdığını düşünen *hacker*ler bütün bilgilerin ücretsiz olmasını savunurlar. Daha önceden yazılmış bir programın tekrar kodlanmasını emek israfı olarak görürler. Bir programın herkese açık olması halinde, başka programcılar tarafından ihtiyaçlarına göre daha kullanışlı hale getirebilecektir. Böylece herkesin kendi programı olması yerine, herkesin kullanabileceği en iyi programa ulaşılabilecektir. *Hacker*lara göre bilgi akışına izin veren her sistem bundan faydalanır. Bilgilerin özgür (*free*) olması bugün açık kaynak kodlu programların oluşmasını sağlayan temel anlayıştır.[36]

*Hacker*lar bilgi paylaşımını sağlamak amacıyla teknolojik gelişmeleri sürekli olarak takip ederek, bu teorik bilgilerini *capture the flag* (bayrağı ele geçir) yarışmalarıyla pratiğe dökerler. Bu yarışmalar sırasında özel olarak dizayn edilmiş ekipmanlarla, belirlenmiş zaman diliminde *hacker*lar ele geçirmeleri gereken hedefe ulaşmaya çalışırlar. Bazı düzenlemelerde katılımcıların sosyal becerilerini kullanarak istenilen bilgilere ulaşıp ulaşamayacakları da sınanır.

36 Özgür yazılımlardaki "free" kelimesinden ne anlaşılması gerektiği hakkında bir yazı için bkz., http://www.gnu.org/philosophy/free-sw.html (Erişim tarihi: 18 Ağustos 2012).

3) Otorite'ye güvenmemek ve adem-i merkeziyeti teşvik etmek: "Serbest bilgi değişimini teşvik etmek için *hacker*larla bilgi arasında ya da donanım arasında, sınırların ve engellerin olmadığı açık sisteme sahip olunmalıdır."[37] *Hacker*lara göre merkezi otorite kendini bürokrasi olarak ortaya koyar. Bu yüzden bürokrasinin hâkim olduğu şirketler ve üniversitelerin dürtülerini öldürdüğünü düşünürler. Bürokrasiye karşı tutumları günümüzde devlet kurumlarına ve onun sistemlerine yapılan saldırıların sebebini net olarak açıklamaktadır.

4) *Hacker*lar yaptıkları eylemlere göre değerlendirilmelidir; diploma, yaş, ırk ve ünvan gibi kriterlere göre değil: *Hacker*lar için iyi eğitimin sınıfta alınması gerekmez. Günümüzde internetin geniş kitlelere yayılmış olması bir çok insanın *hacker* olmak için gereken nitelikli bilgiye kolayca ulaşmasını sağlamaktadır. Örgün eğitim içinde olan ya da olmayan, bilgisayar konusunda sistemli eğitim alan ya da almayan herkes *hacker* olma şansına sahiptir. Siber güvenliğin bu önemli aktörlerinin dünyasında kişilerin başarısı yaptıkları eylemlerle ölçülür. Siber uzayda takma isim kullandıkları için gündelik yaşamlarında hangi yaş, eğitim, ırk ve dil grubuna ait olduklarını tahmin etmek kolay değildir.

5) Bilgisayarda sanat ve güzellikler yapabileceğine inanan *Hacker*lar ellerindeki aracı daha iyi ve kullanışlı hale getirme felsefesine kendilerini adamıştır. Steven Raymond *hacker*ların en azından *Python*, *C/C++, Java, Perl* ve *LISP* gibi programlama dillerini bilmeleri gerektiğini belirtilmektedir.[38] Onlara göre programlarken kullandıkları betiğin sadeliği ve kısalığı bir tür bilgisayar ortamında icra edilmiş sanattır. Yazılımın kodları *hacker*ın düşünce yapısının göstergesidir. Zira yalın yazılmış kodlar sayesinde bilgisayar işlemcileri (CPU) daha az çalışmakta böylece az enerji ile çok iş yapılabilmektedir.

6) Bilgisayarlar hayatınızı daha da güzelleştirebilir. Bilgisayarlar sadece *hacker*lara değil, diğer insanlara da büyük imkânlar sunmaktadır. Günümüzde kolaylıkla elde edilen birçok donanım ve yazılım *hacker*ların katkıda bulunduğu süreçle geliştirilmiştir. Örneğin *hacker*lar açık kaynak kodlu yazılımları desteklemekte ve bunların kullanılmasını teşvik etmektedirler. *Unix* benzeri özgür bir program projesinin kurucusu Richard Stallman'dan *Linux*'un ilk çekirdeğini (*kernel*) yazan Linus Torvalds'a kadar, bir çok *hacker* bunu gerçekleştirmeye çalışmıştır.[39]

1975'te yazılmaya başlayan *hacker* manifestosu[40] zamanla değişerek gelişmiştir. 2004'te yayınlanan yeni bir manifesto eğitimden bilgiye, sınıf olgusundan üretime kadar birçok konuda *hacker*ların algılarını aktarmıştır.[41] Yeni manifestodaki şu ifade konuyu net

37 Steven Levy, *Hackers Heroes of the Computer Revolution*, New York, Penguin, 2001, s. 41.

38 Eric S. Raymond, *How to become hacker*, http://catb.org/~esr/faqs/hacker-howto.html#skills1 (Erişim tarihi: 22 Haziran 2012).

39 Sam Williams, *Free as in Freedom Richard Stallman's Crusade for Free Software,* http://oreilly.com/openbook/freedom/ch11.html (Erişim tarihi: 23 Haziran 2012).

40 Http://manybooks.net/titles/raymondericetext02jarg422.html.

41 McKenzie Wark, *A Hacker Manifesto*, Cambridge, Harvard University Press, 2004.

bir şekilde ifade etmektedir: "bir *hack* sanal'a dokunur ve gerçeği değiştirir. Özünde bir hareketin *hack* sayılabilmesi için yenilik, stil ve teknik uzmanlıkla dolu olması beklenir."[42] Bu sadece bilgisayarla ilgili değildir. Eric S. Raymond'un ifadesiyle, " Yazılımdan başka şeylere (elektronik ve müzik) de *hacker* davranışını uygulayan insanlar var. Aslında herhangi bir bilim dalının veya sanatın en yüksek seviyelerinde onu bulabilirsiniz."[43]

Günümüzde *hacker* felsefesinden farklılaşan motivasyonlarla bilgisayar veya ağ sistemlerine zarar veren kişiler için farklı terimler kullanılmaya başlanmıştır. *Hacker*lar yeni yollar ve yöntemler ortaya koymakla tanınırlar. Bu anlamda *hacker*lardan ilk ayrışanlar *Cracker*'lardır. Bu bilgisayarların güvenlik kontrollerini kendine menfaat sağlamak amacıyla ve suç motivasyonuyla aşan kişi ya da kişilere verilen isimdir. Ne var ki, *hacker*lar ile *cracker*lar arasındaki netliğin zaman zaman kaybolduğu da ortadadır. Türkçe'de bu iki kavramı karşılayabilecek ve ayırabilecek kabul görmüş karşılıklar yoktur. *Hacker* kavramı için "üstad" kelimesini kullanan çevirileri görmek mümkün iken, *cracker* için "bilgisayar korsanı" tabiri kullanılmaktadır.[44]

Öte yandan hem *hacker*lar hem de *cracker*lar odak hedefli çalışırlar. Hedefin niteliği ve ne derece meydan okuyucu olduğu bu iki grubu teşvik eden en önemli unsurdur. *Hacker*lar iş gereği ya da kendilerine buyrulan bir hedefe ulaşmayı genelde sıkıcı bulurlar. Eğer gerekli motivasyon sağlanırsa zaman sınırlaması onlar için anlamsız hale gelir. Bu davranış biçimleri onları siber güvenlik için çalışanlara göre daha avantajlı hale getirmektedir.[45]

Siber güvenliğin önemli aktörleri haline gelen *hacker*lar/*cracker*lar devletlerin de ilgisini çekmiştir. Siber casusluktan istihbarata, güvenlikten siber suçlara kadar birçok alanda yönetime destek verebileceklerini düşündükleri bu kişilerle birlikte çalışma anlayışı pek çok devlette ortaya çıkmıştır. Fakat hem *hacker*/*cracker* felsefesinin devlet bürokrasisi içinde çalışmayı kabul etmemesi, hem de ekonomik imkanların özel şirketler kadar geniş olmaması bu işbirliği arayışlarını sınırlamaktadır. Bu nedenle devletler siber güvenliklerini sağlayabilmek için daha çok farklı donanım ve yazılım önlemleri almaktadır. Çalışanlarına sürekli eğitim vermekte ve sık sık tatbikatlar yapmaktadır. Bunların yanısıra özel firmalardan aldıkları desteklerle kendi sistemlerine yaptırdıkları *penetrasyon* testleriyle[46] muhtemel zayıflıklarını bularak kapattıkları da bilinmektedir.

---

42 Ibid., madde 71.

43 Eric S. Raymond, *How to become hacker*, http://catb.org/~esr/faqs/hacker-howto.html (Erişim tarihi: 22 Haziran 2012).

44 Http://www.belgeler.org/howto/hacker-howto/hacker-howto.html (Erişim tarihi: 22 Haziran 2012). Siber güvenlik söz konusu olduğunda *hacker*lar ve *cracker*lar dışında aktörler de vardır. *Script kiddies* ya da *lamer* tabiri bilgisayar sistemlerine izinsiz erişmek için başkaları tarafından yazılmış programları kullanan kişilere verilen isimdir. Bunların genellikle bilgisayar programlamasını ve çalışma mantığını derinlemesine bilmedikleri düşünülür.

45 Bu konudaki bilgisayar güvenliği için çalışan bir uzmanın değerlendirmesi için bkz., http://blog.lifeoverip.net/2012/06/05/siber-guvenligin-gorunen-ve-gorunmeyen-yuzleri/ (Erişim tarihi: 22 Haziran 2012).

46 Penetrasyon testleri bilgisayar güvenliğinde, bir veri işleme sistemine yapılan izinsiz girişlere verilen addır.

Değişen Dünya Dinamikleri ve NATO Üyeleri

II. Dünya Savaşı sonrasında Soğuk Savaş'ın başlamasıyla Varşova Paktı ülkelerine silah gönderilmesini kontrol etmek amacıyla ABD'de kurulan Çok Taraflı İhraç Kontrol Komitesi (*COCOM - Committee for Multilateral Export Controls*) 1947'de faaliyete geçmişti.[47] Soğuk Savaşın ilerleyen yıllarında komite silah dışında nükleer füzelerin yönetilmesinde kullanılan bilgisayar ekipmanlarının da ikinci dünya ülkelerine ihracatını bu çerçevede yasaklamıştı. Bu çerçevede 1983'te Almanya'daki Karlsruhe Üniversitesi Profesörü Werner Zorn ile Çin'deki Bilgisayar Uygulamaları Enstitüsü'nden Prof. Wang Junfeng'in iki kurum arasında ağ kurulması projesi COCOM kurallarına takıldı. Buna rağmen Zorn'un çabasıyla COCOM listesine girmemiş ekipmanlar bulundu ve Çin'e gönderildi. Ekipmanların kurulmasının ardından 20 Eylül 1987'te Almanya'dan Çin'e ilk elektronik posta gönderildi. Bu engelleme çabalarına rağmen gönderilen "*Ueber die Grosse Mauer erreichen wir alle Ecken der Welt*"[48] metinli ilk e-posta internetin dünyanın bütün köşelerine ulaşacak güçte olduğunun ilk işaretiydi.

Sanal dünyanın kuruluşuna hizmet etmiş olan ARPANET'in bir taraftan yavaşladığı için, diğer taraftan süper bilgisayarlardan oluşan NSFNET (*National Science Foundation Network*) gibi ağların kurulması sebebiyle 1990'da bütün yükübaşka omurgalara devredilerek, işlevine son verildi. Aynı yıl CERN (*European Organization for Nuclear Research*)'de çalışan Tim Berners-Lee tarafından bir çok nükleer fizikçiye ev sahipliği yapan enstitüdeki farklı bilgisayarlardaki bilgiye kolayca erişebilmek amacıyla geliştirilen protokol sayesinde bağlantı kuran ve bağlantılar oluşturmaya izin veren *world wide web* (www) formatı ortaya çıktı. İnternet üzerindeki bilgisayarlar tarafından sunulan, web sayfalarının oluşturulmasına ve ziyaret edilmesine izin veren bu adım internetin hızla gelişmesini sağladı.

Soğuk Savaşın sona ermesiyle birlikte interneti sağlayan ağlara yenileri katıldı. Fakat Soğuk Savaşın mentalitesi hala bilgi güvenliği üzerinde etkisini gösteriyordu. Bilgisayar teknolojisinin kullanımın artması ise kişisel bilgilerin saklanması ve şifrelenmesi konusundaki ihtiyaçları ortaya çıkardı. Dijital çağda vatandaşların da iletişimlerini şifreleyebilmesi gerektiği düşüncesiyle 1983'te *Massachusetts Institute of Technology* tarafından kriptografik iletişim sistemi ve metodu olarak patentlenen RSA algoritmasını kullanan Phil Zimmermann, 1991'de *Pretty Good Privacy* (PGP) isimli bir şifreleme programı yazdı ve internet üzerinden paylaştı. Fakat kısa sürede hızla yaygınlaşan programın internet üzerinden paylaşılması ABD'nin Silah İhraç Kontrol Kanunu'na uymadığı gerekçesiyle Zimmermann tutuklandı.[49] Zira Soğuk Savaş döneminde kriptografik programlar stratejik bir unsur olarak değerlendirilerek, ihraç yasağı listesine eklenmişti. Bu dönem sonrasında gereken değişiklik yapılmadığı için Zimmermann'ın geliştirdiği

47 Frank M. Cain, "Exporting the Cold War: British Responses to the USA's Establishment of COCOM, 1947-51", *Journal of Contemporary History*, Cilt 29(3), Haziran 1994, s. 501-522.

48 Büyük Duvarın ötesinde dünyanın bütün köşelerine ulaşacağız.

49 Diana Saco, "Colonizing Cyberspace "National Security" and the Internet", Jutta Weldes, Mark Laffey ve Hugh Gusterson (der.), *Cultures of Insecurity: States, Communities, and the Production of Danger,* Minneapolis, University of Minnesota Press, 1999 içinde, s. 261-290.

ve dağıttığı program için de bu kanunu ihlalden dava açıldı. Takip eden dönemde kriptografik yazılımlar ve siber güvenlik elele ilerlemeye devam ettiği için ulusal güvenliği ilgilendiren konularda yavaş yavaş hukuki düzenlemeler yapıldı. ABD'deki yasal düzenlemede şifreleme programlarının kolay kırılabilecek olanlarına "düşük kuvvette", zor kırılabilecek olanlarına "yüksek kuvvette" sınıflaması yapıldı. Böylece Zimmermann'ın davası düştü.[50]

Yeni Güvenlik Ortamında NATO'ya Yönelik Tehditler

Soğuk Savaş'ın bitmesiyle siber uzay yoğun şekilde paylaşılan ve geniş kullanıcı kitlesine sahip bir alana dönüştü. Devletler güvenlik haberleşmelerinden kamusal hizmetlerine kadar birçok bilgiyi buradan sunmaya başladılar. Öte yandan işlemcilerin günden güne daha da hızlanması kamusal hizmetlerde otomasyon imkânı sağladığı için, bilgisayar daha çok kullanılmaya başlandı. Özellikle su, gaz, elektrik dağıtımı gibi hizmetlerin yanında havayolları, karayolları ve denizyollarının kontrolü de bilgisayar sistemlerince yapılmaya başlandı. Günümüzde çokça tartışılan bu alt yapıya saldırının önemli siber tehditler arasında olduğunu belirtmekte fayda vardır.[51]

İnternetin ve bilişim teknolojilerin bu denli hayatımıza girdiği bu dönemde, Aralık 1994'de Rus birlikleri Çeçenistan'ın başkenti Grozni'ye girdiler. Ağır silahlarla şehre giren Rus birlikleri Çeçen direnişinin kısa süreceğini zannediyordu. Fakat sahadaki gerçekler beklentilerle uyuşmayınca Soğuk savaş sonrasında ilk defa askeri bir çatışma internet ortamına da yansıdı. Çeçenler bütün medya imkânlarını, özellikle de interneti kullanarak bilgi savaşının (*information war*) ilk örneklerini verdiler. Çeçenlerin internete yüklediği ölü Rus askerlerinin resimlerini gören anneler, çocuklarını kurtarmak için harekete geçtiler. Bu bilgi ve propaganda internetin savaş alanı olarak kullanıldığı ilk örneklerden birisiydi.[52]

Bu yeni dönemde internet sadece iletişimin yapıldığı bir ortam olmaktan çıkıp, korunması gereken bir alan haline gelmeye başladı. Rus-Çeçen çatışmasında internetin kullanılması ister istemez alternatif tehditleri akla getirince uluslararası sistemin güçlü ülkeleri muhtemel saldırılara karşı hazırlık yapmaya başladılar. Ulus devlet düzeyindeki hazırlıklar bütün aktörler açısından yeterince etkin olamayınca uluslararası yapılar devreye girmeye başladı. Bunun öncülerinden olan NATO, daha 1999'da üyelerini askeri haber-

50 Simon Singh, *The Code Book The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, New York, Anchor Books, 2000, s. 293-316.

51 Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *The Information Security Journal: A Global Perspective*, Cilt 18 (1), 2009, s. 1-7. Bu konuda Uluslararası İlişkiler teorisi açısından farklı bir tartışma için bkz, Myriam A. Dunn, "Securing the digital age; The challenges of complexity for critical infrastructure protection and IR Theory", Johann Ericksson ve Giampiero Giacomello (der.), *International Relations and Security in the Digital Age*, New York, Routledge, 2007 içinde, s. 85-105.

52 Graeme P. Herd, "Information Warfare and the Second Chechen Campaign," Sally Cummings (der.), *War and Peace in Post-Soviet Eastern Europe*, Washington, D.C., Confict Studies Research Center, 2000 içinde, s. 31-42.

leşme sistemlerine karşı yapılabilecek saldırılar hakkında uyarmış ve hazırlıklı olmalarını istemişti.[53] Fakat ilk siber saldırılar beklenenden erken geldi.

1999'ta NATO güçlerinin, dağılma sürecindeki Yugoslavya'da Sırp hedeflerini bombalamaya başlamasıyla birlikte beklenmedik siber saldırılar başladı. 9 Nisan 1999'da Londra merkezli güvenlik firması *Mi2g*'nin, Sırp *hacker*ların NATO'nun yeterli hazırlığı bulunan askeri komuta-kontrol ağına değil de üye ülkelerin ekonomik alt yapılarına saldıracakları konusunda uyarılar göndermiş olması sonucu değiştirmedi.[54] Sırp ve Rus *hacker*lar tarafından NATO'ya ve üye ülkelerin askeri haberleşme sistemlerine yönelik siber saldırılar yapıldı.[55] Saldırılar sırasında en çok kullanılan saldırı yöntemi DDoS (*Distributed Denial of Service*- Dağıtık Servis Dışı Bırakma Saldırısı) tekniğiyle sunucuların işlemcilerinin isteklere cevap veremez hale getirilmesiydi. Saldırıda NATO'nun uluslararası web sayfasını ve e-posta trafiğini barındıran yaklaşık 100 sunucu hedef alınmıştı.[56] İlaveten *Ping* doygunluğu (*saturation*) saldırısı ve binlerce zararlı bilgisayar virüsü içeren e-postalar kullanıldı. NATO sunucularıyla birlikte ABD Savunma Bakanlığı'nın alt yapısına da saldırılar düzenlendi.[57] Bunun sonucunda ABD Ordusu ve Hava Kuvvetleri sistemlerini virüslerden arındırabilmek için bir hafta sonu dünyadaki tüm sunucularını kapatmak zorunda kaldılar. Hatta Pentagon'dan uzmanların müteakip hareketleri izlemek amacıyla Sırp bilgisayarlarına sızdıkları ve daha büyük stratejik zararların oluşmasını bu yolla önledikleri bile iddia edilmişti.[58] Saldırılar yakından incelendiğinde bazı sitelerde *hacker*ların "Çok Yaşa Büyük Sırbistan ve Kara El (*Black Hand*) bu siteye el koydu" ifadelerini sunuculara yüklediği görüldü. *Hacker*ların gruplarına ismini verdikleri "Kara El" grubu I. Dünya Savaşı sırasında kurulmuş gizli bir Sırp örgütüydü. Artan saldırılar araştırıldığında Sırplara ilaveten, Rus ve Çinli *hacker*ların da eylemleri desteklediği görüldü. [59] Bu olayla birlikte reel politikadaki siyasi ittifakların siber alanda da devam ettiği anlaşıldı. Fiziksel ve sanal alan arasındaki bu ilişki, siber dünyanın uluslararası sistemin aktörleri tarafından hukuki olarak düzenlenmesi gerektiği fikrini gündeme getirdi.

53 Vernon J. Ehlers, *Information Warfare and International Security*, 6 Ekim 1999, http://www.nato-pa.int/archivedpub/comrep/1999/as285stc-e.asp (Erişim tarihi: 28 Kasım 2012).

54 "Serbian Cyber Attack intensifies on NATO Financial Institutions and Public Utilities Next", http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/presrel080499.php (Erişim tarihi: 12 Ocak 2013).

55 Ibid.

56 Sverre Myrli, *173 DSCFC 09 E BIS - NATO and Cyber Defence*, http://www.nato-pa.int/default.Asp?SHORTCUT=1782(Erişim tarihi: 28 Kasım 2012).

57 Kenneth Geers, *Strategic Cyber Security*, Tallinn, CCD COE Press, 2011, s. 82.

58 Julian Borger, "Cyberwar could spare bombs", *The Guardian*, 5 Kasım 1999, http://www.guardian.co.uk/world/1999/nov/05/balkans (Erişim tarihi: 22 Haziran 2013).

59 "Non-Military Asymmetric Challenges", *Whitehall Papers,* Cilt 49 (1), 2000, s. 50-68.

NATO Değişirken: Yeni Güvenlik Kuralları

11 Eylül 2001'de New York ve Washington'da çeşitli hedeflere yolcu uçaklarını çarparak yapılan terör saldırıları, uluslararası sistemdeki güvenlik tanımlarını, tehditleri ve gündemi tamamen değiştirdi. Soğuk Savaş sonrasında nispeten silikleşen milli güvenlik kavramı birçok ülkenin listesinde yeniden ilk sıraya oturdu. Terörizmle savaş sadece saldırıya uğrayan hükümetin değil, neredeyse sistemdeki tüm aktörlerin gündemine girdi ve ABD'nin önderliğinde hızla başladı. Saldırıların tozunun kalkmasının hemen ardından, saldırıları gerçekleştiren teröristlerin kendi aralarında internet üzerinden haberleşmiş olduklarının ve kullandıkları uçakları daha önce simülasyon programında çalışmış olduklarının anlaşılması, internet ortamının terörist saldırılar için kullanılmakta olduğu fikrini kuvvetlendirdi.[60]

11 Eylül sonrasında tansiyonun yüksek olduğu dönemde uluslararası alanda en çok tartışılan konulardan birisi NATO üyelerinden birine karşı gerçekleşmesi mümkün olan "Dijital Felaket" (diğer adıyla dijital 9/11) senaryosuydu. Siber terör ve terörist grupların sanal ortamı kullanmaları ihtimali, muhtemel bir dijital *Pearl Harbour* beklentilerini yükseltmişti.[61] Devletlerin siber sistemlerine yönelecek saldırılarla ekonomik ve diğer kritik alt yapılarının vurularak etkisiz hale getirilebileceği, bunun da ülkedeki güvenliği derinden sarsacağı düşünülüyordu.[62] Bu tür endişelerin milli güvenlikle yakından ilişkilendirilmesi sonucu, takip eden süreçte birçok ülke siber güvenlik stratejilerini ulusal güvenlik belgelerine eklediler ve düzenli olarak güncellediler.[63]

Bu ülkeler içinde en ilginç örneğin Estonya olduğunu söyleyebiliriz. Estonya internet kullanımının en yüksek olduğu ülkelerden birisidir. Her vatandaşın devlet kurumlarına ve bankalarına internet üzerinden bağlanmasına imkân veren bir dijital kimliğe sahip olduğu ülkede, 355 devlet kuruluşu sanal dünyada yer almaktadır. 2001'de kullanıma alınan veri değişim katmanı *X-Road* programı Estonya'daki kamu kurumları ile vatandaşları birbirine bağlamaktadır. Bu e-devlet uygulamaları açısından en yaygın uygulama örneğidir. Ayrıca Estonya 2005'te bilgisayar ağları üzerinden yerel seçim oylamasına izin vererek de bir ilke imza atmıştır. 2010 verilerine göre, Estonya'nın 1.46 milyonluk nüfusunun %75'i internet kullanıcısıdır.[64]

60 T. L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning." *Parameters*, Cilt 33 (1), Mart 2003, s. 114-122.

61 Alison Mitchell, "To Forestall a 'Digital Pearl Harbor", U.S. Looks to System Separate From Internet", *The New York Times,* 17 Kasım 2001, http://www.nytimes.com/2001/11/17/technology/17INTE.html?pagewanted=all (Erişim tarihi: 28 Kasım 2012).

62 Lene Hansen ve Helen Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly*, Sayı 53, 2009, s. 1155-1175.

63 Bazı örnekler için bkz: İngiltere, "The UK Cyber Security Strategy", http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf (Erişim tarihi: 23 Kasım 2012); Canada, " Canada's Cyber Security Strategy", http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf (Erişim tarihi: 23 Kasım 2012); Estonya, "Cyber Security Strategy", http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (Erişim tarihi: 28 Kasım 2012).

64 Heidi Seybert, "Internet use in households and by individuals in 2011", *European Commission Eurostat Industry, trade and services Statistics in focus*, 66/2011, http://epp.eurostat.ec.europa.eu/portal/page/portal/product_details/publication?p_product_code=KS-SF-11-066 (Erişim tarihi: 22 Kasım 2012).

Soğuk Savaş'ın sona ermesinin ardından demografik dağılımında Rus kökenli nüfusun günden güne artışıyla birlikte Estonlarla Ruslar arasında çıkan gerginlik giderek artmıştı. Bu tansiyon iç politikaya da yansımış ve Estonya'nın başkenti Tallinn'e Kızıl Ordu'nun girişinin ifadesi olarak 1947'de yapılan"Talin'in Kurtarıcısı" heykeli (Rusça adıyla МонументосвободителямТаллина) Nisan 2007'de şehir merkezinden Tallinn'deki askeri mezarlığa taşınmıştı. Buna karşı çıkan Rus kökenli Estonya vatandaşlarının meydanlarda gösterileri devam ederken, 27 Nisan akşamı gece yarısından sonra *Ping* yoğunluyla başlayan siber saldırılar, çok hızlı bir şekilde servis dışı bırakma saldırısına dönüştü.[65] Bu arada birçok Rus internet forumunda Estonya'daki adresler hedef olarak gösterildi ve teknik bilgisi olmayanlar için bile saldırıyı gerçekleştirmenin yöntemleri detaylı olarak açıklandı.[66]

Ülkedeki *Hansabank* ve *SEB* gibi bankalar siber saldırılara hazırlıklı oldukları için ilk gün yapılan saldırılardan büyük zarar görmediler. Fakat hazırlıksız olan Estonya hükümet siteleri hızlıca işlevlerini yerine getiremez hale geldi. Başkanlık ve Parlamento siteleri, bütün bakanlık siteleri, siyasi partilerin siteleri hedefler arasındaydı. Estonya'daki altı büyük medya kuruluşu ve iletişim firmaları da saldırıdan nasibini aldı. Ülkede IP'leri kontrol eden ve izleyen sistemlerin olmaması tehdidi daha hissedilir hale getirmişti. Saldırılara cevap verecek tek kurum ülkedeki e-seçimleri düzenleyen ve alt yapısını hazırlayan uzmanlar topluluğuydu.

28 Nisan'da zirve noktasına ulaşan saldırılar daha sonra azalmaya başladı. 3 Mayıs'ta *Ping* taşması tabir edilen saldırılar yeniden başladı. Rusya'nın II. Dünya Savaşı'nda Nazi Almanya'sını yendiği gün olan 9 Mayıs'da *Botnet* saldırıları başladı. 11 Mayıs'da yavaşlayan saldırılar, 18 Mayıs'ta tekrar başladı ve 23'üne kadar devam etti.[67] Birçok Rus sitesinin katıldığı bu saldırılar sırasında Rusya'daki *http://2ch.ru* ve *http://forum.xaker.ru* siteleri kullanıcılarının basit programlarla saldırıya katılımını teşvik ettiler. Kullanıcıların katılımını sağlayarak kanal genişliği doldurmak amacıyla yapılan bu saldırılarda *Ping* komutunun nasıl kullanacağı da bu sitelerde etraflıca anlatıldı.[68] Başka bir sitede de saldırıların 9 Mayıs gece yarısında yapılması tavsiye edilmişti.

X-Road sistemini çökertmek için özel olarak düzenlenmiş veri paketlerinin yönlendiricilere (*router*) gönderildiği bu saldırılar sırasında dağıtık servis dışı bırakma saldırısı ile ABD, Kanada, Rusya, Türkiye, Almanya, Belçika, Mısır, Vietnam gibi ülkelerden gelen IP'ler kaydedilmişti. Saldırılara karşı önlem olarak Estonya hükümeti bant genişliğini 2

65 Salih Bıçakcı, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler*, Cilt 9 (34), Yaz 2012, s. 205-226.

66 Ibid.

67 Joshua Davis, "The Botnet Attacks on Estonia", *Wired*, 3 Eylül 2007, http://www.wired.com/images/press/pdf/webwarone.pdf (Erişim tarihi: 23 Kasım 2012); Jose Nazario, "DDoS and Security Reports: The Arbor Networks Security Blog", http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/ (Erişim tarihi: 28 Kasım 2012).

68 Örnek site için bkz: http://forumnov.com/lofiversion/index.php?t109658.html (Erişim tarihi: 22 Kasım 2012); Bıçakcı, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", s. 205-226.

Gbps'ten 8 Gbps'e çıkardı. Özel sektör de sunucularının sayısını ve alan genişliğini arttırdı. Yine de zor durumda kalan Estonya Savunma Bakanı Dr. Jaak Aaviksoo NATO'ya ve diğer ülkelere yardım çağrısında bulundu.[69] Oluşturulan geçici (*ad hoc*) yardım grupları Estonya'da göreve başladılar. NATO'nun 1999 Sırp bilgisayar korsanlarının saldırısı sonrasında artarak büyüyen siber güvenlik ilgisi Estonya'nın uğradığı saldırılar sonrasında gözle görülür hale geldi.

Estonya'ya yapılan siber saldırılar uluslararası güvenlik açısından bir milat oldu. Siber saldırının hangi durumlarda savaş sebebi sayıldığı ve nasıl algılamamız gerektiği konularında tartışmaların başlamasını sağladı.[70] Estonya sonrasında uluslararası güvenlik örgütleri siber saldırılara nasıl cevap verecekleri sorusuna odaklandılar. 9/11 sonrasında internetin terörizm amaçlı kullanımı konusunda dikkatli olunmasını salık veren raporlar, Estonya saldırısından sonra siber saldırılar ve savaşlar konusunu gündemlerine aldılar. Güvenlik örgütleri bütün üyelerinin siber saldırılara karşı aynı seviyede hazırlanması için gereken önlemleri almaya başladılar.

NATO'nun 2008'te gerçekleşen Bükreş Zirvesi sonrasında yayınlanan deklarasyonda NATO, üyelerinin bilişim sistemlerini siber saldırılara karşı güçlendirme konusuna kararlılığını devam ettireceğini ilan etti. Zirvede siber savunma siyaseti kabul edildi ve bunu geliştirecek yapılar ile gerçekleştirecek otoriteler oluşturulmasına karar verildi. Ayrıca NATO'nun siber güvenlik politikasının esasının savunma olduğu vurgulandı. Üyelerinin kilit bilişim sistemlerinin korunması yanında, istekte bulunmaları halinde siber saldırılara karşı koyma kapasitelerinin de desteklenmesine karar verildi. Zirve sonrasında siber savunma alanında NATO ile milli otoritelerin arasındaki ilişkinin güçlendirilmesi konusunda da mutabık kalındı.[71] İttifak üyelerinin siber savunma konusunda tecrübelerini paylaşmaları ve gerektiğinde birbirlerine yardım etmeleri konusunun altı çizildi.

Bükreş Zirve'sinin ardından siber güvenlik alanında iki önemli gelişme oldu. Zirveden sonra NATO Siber Savunma Yönetimi Otoritesi'nin (*Cyber Defense Management Authority*) Brüksel'de kurulmasına karar verildi.[72] Siber savunma kapasitesini bir merkezde toplayarak harekat kabiliyetini arttırmak isteyen NATO, bununla yetinmeyerek Estonya Tallinn merkezli Siber Savunma İşbirliği Mükemmeliyet Merkezini (CCD COE - *Cooperative Cyber Defence Centre of Excellence*) kurdu. Her ne kadar, Estonya Savunma Bakanlığı bu merkezin kurulması için NATO'ya 2007 saldırıları öncesinde teklif ver-

69 Henry Meyer ve Ott Ummelas, "Estonia Asks NATO to Help Foil 'Cyber Attack' Linked to Russia", *Bloomberg*, 17 Mayıs 2007, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abGseMma5MjU&refer=europe (Erişim tarihi: 23 Kasım 2012).

70 Bu konudaki tartışmalar için bkz., David M. Keely, "Cyber Attack! Crime or Act of War?", *USAWC Strategy Research Project*, 2011, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA553344 (Erişim tarihi: 23 Kasım 2012); James P. Farwell ve Rafal Rohozinski, Rafal, "Stuxnet and the Future of Cyber War", *Survival*, Cilt 53(1), 2011, s. 23-40.

71 *NATO Bucharest Summit Declaration*, 03 Nisan 2008, http://www.nato.int/cps/en/natolive/official_texts_8443.htm (Erişim tarihi: 23 Kasım 2012).

72 Rex B. Hughes, "NATO and Cyber Defence: Mission Accomplished?", Cilt 1(4), 2009, http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf (Erişim tarihi: 28 Kasım 2012).

diklerini açıkladıysa da, merkez ancak Ekim 2008'de kurulabildi.[73] Merkez'in 30 kişilik personelden oluşmasına ve aşağıdaki görevleri yerine getirmesine karar verildi:

1) Siber uzayla ilgili konularda ittifak için doktrinler ve kavramlar üretmek;
2) NATO'ya üye ülkeler için eğitim kursları, atölye çalışmaları yapmak ve tatbikatlar düzenlemek;
3) Araştırmalar yapmak ve gelişmeler üzerine toplantılar düzenlemek;
4) Geçmiş ve halihazırdaki saldırıları çalışarak dersler çıkarmak;
5) Devam eden saldırılarda eğer istenirse tavsiyelerde bulunmak.

Estonya'ya yönelik siber saldırıların üzerinden henüz bir yıl geçmişti ki Ağustos 2008'de Güney Osetya yüzünden Rusya Federasyonu ile Gürcistan arasında çıkan çatışma siber güvenlik konusunu yeniden gündemin üst sıralarına taşıdı. Daha önce Osetler ile Gürcistan hükümeti arasındaki çatışmalar nedeniyle 1992'de Güney Osetya'da Rusya, Gürcistan ve Güney Osetya birliklerinden oluşan bir barış gücü oluşturulmuştu.[74] Rusya tarafından kumanda edilen bu güçteki uyum planlandığı kadar iyi olmayınca çatlak sesler yükselmeye başladı. Gürcistan ve Rusya arasındaki gerginlik hızla arttı ve 7 Ağustos 2008'te Gürcistan kuvvetlerinin ayrılıkçı grubun provokasyonuna cevap vermesiyle hızla yükselen olaylar sıcak çatışmaya dönüştü. 8 Ağustos'ta Rus güçleri Gürcistan'a askeri operasyonla karşılık verdiler. Bu arada 7 Ağustos 2008 akşam saatlerinde Gürcistan'a karşı siber saldırılar başladı. Gürcistan enformasyon alt yapısının Estonya kadar gelişmiş olmaması saldırının verdiği zararın etkisini azalttı. Ama saldırı sırasında olayların gelişimi ve izlenen yöntemler neredeyse Estonya'dakinin aynısıydı.[75] Gürcistan NATO'ya üyelik isteğini belirtilmiş olmasına rağmen, bu henüz gerçekleşmediği için NATO'nun koruması altına girememişti. Siber saldırıları yapan Rusya ve Türkiye merkezli siteler incelendiğinde, bu sitelerin ABD'den çalınmış kredi kartlarıyla açıldığı belirlendi.[76] Ayrıca saldırılar için gönderilen *spam* postaların Rusya'nın önemli siber suçlularından Rus İş Ağı (*Russian Business Network*) tarafından gönderildiği tespit edildi. St. Petersburg merkezli bu ağ, NATO tarafından hazırlanan bir raporda da saldırganlık eğilimiyle suçlanmıştı.[77]

Gürcistan'a yönelik siber saldırılarda gördüğümüz en önemli unsur gerçek bir hibrit savaş niteliği taşımasıydı. Geleneksel savaş yöntemlerini kullanan Rusya, eş zamanlı olarak siber saldırıları da başlatmıştı. Düzensiz saldırı yöntemlerini geleneksel yöntemlerle birleştirerek yapılan bu saldırılara hibrit strateji tanımlaması yapılıyor. Rusya saldı-

73 Sverre Myrli, *173 DSCFC 09 E BIS - NATO and Cyber Defence*, http://www.nato-pa.int/default.Asp?SHORTCUT=1782(Erişim tarihi: 28 Kasım 2012).

74 Rui Gomes Da Silva, "180 Pcnp 09 E Rev 1 - Georgia and NATO", http://www.nato-pa.int/Default.asp?SHORTCUT=1776 (Erişim tarihi: 29 Ekim 2012).

75 Dancho Danchev, "Coordinated Russia vs Georgia cyber attack in progress", 11 Ağustos 2008, http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 (Erişim tarihi: 25 Ekim 2012).

76 Ibid.

77 Myrli, *173 DSCFC 09 E BIS - NATO and Cyber Defence*.

rısı sonrasında NATO, Gürcistan saldırısını incelemek üzere Siber Savunma Yönetimi Otoritesi'nden (CDMA) bir uzmanı bölgeye gönderdi. 8 Ağustos'ta başlayan saldırılar bir hafta içinde son bulan saldırıların yoğunluğu Estonya'da elde edilen tecrübelerin haklılığını doğruluyordu.

Siber Saldırının Yeni Boyutları

Siber güvenlik dünyasındaki tehditlerin çoğunluğu birden fazla değişkenle ortaya çıkar. Tehdidin çok boyutluluğu savunma için de benzer bir yaklaşımı zorunlu kılmaktadır. Her ne kadar hamleler gizlilik gerektirse de, gelişmiş ağ güvenlik çözümleri ortaklıkların kurulmasına ihtiyaç duymaktadır. Özellikle servis dışı bırakma (DOS- *Denial of Service*) yaygın olarak yapılan saldırılardan birisidir. Herhangi bir grup saldırganın farklı yerlerden yapılan saldırı türüne dağıtık servis dışı bırakma (DDOS - *Distributed Denial of Service*) ismi verilmektedir. Servis dışı bırakma saldırısı adından da anlaşılacağı gibi hizmet veren sunucu bilgisayarın verdiği servisi yerine getiremez hale gelmesidir. Bazı durumlarda hizmet durmaz ama o kadar yavaşlar ki, sunulan hizmetin niteliği açısından anlamsız hale gelir. Servis dışı bırakma saldırısında sunucu bilgisayarın ağ kaynakları tüketilmeye çalışılır. Bu saldırılar sırasında sunucu bilgisayarın bellek ve işlemci gücü de önemli rol oynar. DOS saldırıların farklı çeşitleri vardır. Dağıtık olsun ya da olmasın saldırılarda değiştirilmiş (*spoof*) IP numaralarıyla saldırıların yapılması mümkündür.

Günümüzde bireysel saldırıların yanı sıra grup halinde saldırılar da sıkça görülmektedir. Grup halinde saldırılar farklı yöntemlerle yapılabilir. Gönüllü grupların katılımıyla büyük katılımcıları organize eden *Anonymous* saldırıları bu türe örnek olabilir. Ayrıca bu tür saldırıları gerçekleştirmek için kullanılan *botnet*'ler de siber dünyanın önemli tehditlerinden birisidir.[78] *Botnet*ler organize edilmiş saldırıya ya da verilen emiri yerine getirmeye planlanmış sistemlerdir. *Botnet*'ler "*bot master*" adı verilen kişiler tarafından kurulurlar. *Bot master*lar yazdıkları program ya da *web* sayfaları aracılığıyla zararlı yazılımlarını farklı bilgisayarlara yayarlar. Bu yazılımları kullanmaya başlayan bilgisayarlar farkında olmadan *botnet* içine dâhil olurlar. *Bot master*'ın emirini bekleyen bu bilgisayarlara "zombi" ismi verilir. *Botnet*ler genişliklerine göre farklı sunucu alternatifleriyle yönetilirler.[79] *Botnet*ler bilgi çalmaktan *spam*e, siber şantajdan kanundışı eylemler için dosya aktarımına ve reklam servislerinden gelir elde etmeye kadar farklı alanlarda kullanılabilir.

Yetenekleri ve sınırları bu kadar geniş olan bu siber ordu organize suç örgütleri tarafından da sıkça kullanılmaktadır. Takip edilmesi ve bulunması zor olan bu sistemde, genelde yakalananların masum *zombi* bilgisayar sahipleri olması hukuk sistemlerini ve polis örgütlerini zora sokmaktadır. Son zamanlarda *botnet*lerin hızlıca pazarlanan bir meta

78 CCD COE- Joint Report, "Legal Implications of Countering Botnets", 5 Kasım 2012, http://www.ccdcoe.org/articles/2012/LegalImplicationsOfCounteringBotnets.pdf (Erişim tarihi: 30 Kasım 2012).

79 Zheng Bu, Pedro Bueno, Rahul Kashyap, ve Adam Wosotowsky, *The New Era of Botnets*, McAfee Labs White Papers, http://www.mcafee.com/us/resources/white-papers/wp-new-era-of-botnets.pdf (Erişim tarihi: 24 Aralık 2012).

halini geldiğini ve *botnet* sahiplerinin ellerindeki gücü isteyenlere belirli bir ücret karşılığında kiraladıklarını görüyoruz. Bu da güvenlik güçlerinin işlerini daha da zorlaştırıyor.

Gürcistan saldırısından bu yana siber güvenlik sahasında ortaya çıkan en büyük gelişme *Stuxnet*'tir. Haziran 2010'da ortaya çıkan bu bilgisayar solucanı hem yayılma tarzı, hem de politik olarak kullanılış şekliyle dikkati çekmiştir. *Stuxnet*'in en önemli özelliği spesifik olarak bir anakartı (PLC) hedef alacak şekilde programlanmış olmasıdır. *Microsoft Windows* işletim sistemleri aracılığıyla yayılan bu solucan, Siemens'in S7 300 modüllerini hedef almaktaydı. *Hacker*lar tarafından spesifik olarak bir endüstriyel PLC'ye (Programlanabilir Kontrol Cihazı) ve SCADA'ya (*Supervisory Control and Data Acquisition* - İzleme, Kontrol ve Veri Toplama Sistemi) yönelik saldırı çok sık görülen bir uygulama değildir. Stuxnet'in *Microsoft Windows* sistemlerindeki ilk gün açığını (*Zero Day Exploit*) kullandığı, saldırı sonrasında yapılan çalışmalarla ortaya çıktı.[80]İlk gün açığı yazılımların piyasa çıkarılması sonrasında belirlenen zayıf noktalardır. Bu tip açıklardan genelde iki şekilde haberdar olunur; ya firmalar açığı ilan ederler ya da firmanın bile haberi yokken *hacker*lar tarafından bulunarak internette çeşitli forumlarda açıklanması sayesinde yayılır. İnternet üzerinde bu açıkları pazarlayan *hacker*lar olduğu gibi, yazılım üreticisi firmalar da açıkları bulan kişilere belirli miktarlarda ödemeler yaparak, açıklar bir soruna dönüşmeden bilgi sahibi olmaya ve sorunu gidermeye çalışırlar.[81]

Stuxnet saldırısında dikkat çeken bir husus, Siemens PLC'lere ulaşmak için *MS Windows* sistemlerin açığını kullanan solucanın hedefine ulaşıncaya kadar eriştiği hiç bir bilgisayara zarar vermemiş olmasıdır.[82] Esasında zarar vermemesi solucanın ömrünü ve hedefe ulaşabilme yüzdesini de yükseltmiştir. *Stuxnet*'in görevini yerine getirebilmek için çalıntı dijital imzaları kullanması da bundan önceki örneklerde görülmemiş bir uygulamaydı.[83] Solucan Siemens karta ulaştığında bağlı bulunduğu motorun çalışma hızını farklı aralıklarla değiştirecek şekilde makinaya müdahale etmiştir.

Saldırılardan zarar gören ülkeler arasında İran (%58.85) ve Endonezya (%18.22) ilk sıraları alırken, Hindistan, Azerbaycan, Amerika Birleşik Devletleri, Pakistan da listede yer almıştır. Solucanın yazılışı ve gerektirdiği teknik birikim açısından sınırlı sayıda programcının yazabileceği belirtilen saldırıyı kimin yaptığı konusunda bir çok spekülasyon yapıldı.[84] Saldırılan ülkenin İran olması ve nükleer zenginleştirme faaliyetlerini geciktirmesi hasebiyle *Stuxnet*'i kimin yazdığı yönünde

80 Nicolas Falliere, Liam O Murchu veEric Chien, "W32.Stuxnet Dossier Version 1.4", Şubat 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (Erişim tarihi: 20 Kasım 2012).

81 Andy Greenberg, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits", *Forbes*, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/ (Erişim tarihi: 02.08.2012).

82 Falliere, *W32.Stuxnet Dossier.*

83 Patrick Fitzgerald ve Eric Chien, "The Hackers Behind Stuxnet", http://www.symantec.com/connect/blogs/hackers-behind-stuxnet (Erişim tarihi: 29 Kasım 2012).

84 Larry Seltzer, "Who's Behind Stuxnet? The Americans? The Israelis?",http://securitywatch.pcmag.com/hacking/283762-who-s-behind-stuxnet-the-americans-the-israelis (Erişim tarihi: 29 Kasım 2012).

tahminlerde bulunmak mümkün olabilir.[85] Fakat bunu kesin kanıtlarla ortaya koymak sanıldığı kadar kolay değildir.[86]

Stuxnet'in bulunmasından kısa bir süre sonra 1 Eylül 2011'te *Duqu* isimli *Trojan* Budapeşte Teknoloji ve Ekonomi Üniversitesi tarafından kamuoyuna duyuruldu. *Duqu*'nun bir çok özelliğinin *Stuxnet*'le aynı olması, *Stuxnet*'in *kernel*'ine ulaşabilen kişi(ler) tarafından yazıldığının iddia edilmesine sebep oldu. Temelde benzerliklerin fazla olması bu kanaati oluşturmuştu. Fakat *Duqu*'nun temel görevi endüstriyel kontrol sistemleri hakkında istihbarat toplamaktı. Bunu gerçekleştirebilmek için şifreleri kopyalıyor, belirli işlemlerin nasıl yapıldığını anlamak için ekran görüntüsü alıyor, bir çok dokümanı çalıyordu.[87]

Duqu'nun siber casusluk olarak kullanımı ile ilgili tartışmalar sürerken, İran Ulusal Bilgisayar Acil Müdahale Ekibi (CERT-*Computer Emergency Response Team*) *Maher* tarafından 28 Mayıs 2012'te bir *Flame Malware* (kötücül yazılım) bulunduğu açıklandı.[88] Alışılmışın tersine bu yazılım 20 megabit ağırlıktaydı ve sadece istihbarat toplamak üzere olduğu her haliyle belliydi. Yerel ağlarla ve USB bağlantısıyla yayılabilen solucanın 1000 kadar bilgisayara bulaştığı tahmin ediliyordu. Bu kötücül yazılım (*malware*) yerleştiği bilgisayardaki her türlü sesi, ekran görüntüsünü ve klavyede yazılan her şeyi kayıt edebilmesinin yanı sıra, ağ trafiğini takip ettiği ve *Skype* konuşmalarını da kaydettiği belirtildi.[89] Girdiği bilgisayarda *bluetooth*'u etkin hale getirebilen solucan, çevredeki *bluetooth*'u açık cihazların listesini oluşturmaktaydı. Özellikle *AutoCAD* çizimleri, PDF ve metin formatındaki dosyaları topladığı, hatta Arapça ve İbranice metinleri analiz edebildiği ve bu dökümanlara ait yer etiketi (*geotagging*) var ise bunları da topladığı iddia edilmiştir.[90]

Bu araştırmanın derlenmesinin bittiği 2012'de *Flame*'in benzer özelliklerini taşıyan bir başka kötücül yazılım daha bulundu. *Gauss* adı verilen yazılım özellikle Lübnan'daki bankaların sunucularında ortaya çıktı. Bu yazılım da, *Flame*'e benzer şekilde farklı internet programlarında kullanıcı adlarını ve şifreleri çalabilmekteydi. Ayrıca ağ bağlantı bilgilerini, işlemlerini, dosya dizinlerini toplamaktaydı. Yerleştiği bilgisayarın BIOS, CMOS ve RAM bilgilerini kaydetmekteydi. Bulaştığı bilgisayarlara takılan USB'lere yerleşerek

85 Paul K. Kerr, John Rollins, Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, http://www.fas.org/sgp/crs/natsec/R41524.pdf (Erişim tarihi: 02 Ağustos 2012).

86 Aleksandr Matrosov, Eugene Rodionov, David Harley, *Stuxnet under the Microscope- Revision 1.31* http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf (Erişim tarihi: 31 Temmuz 2012).

87 *Duqu: A Stuxnet-like malware found in the wild*, http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf (Erişim tarihi: 31 Temmuz 2012).

88 Sabari Selvan, "Flame worm - Iran uncovers Stuxnet-style malware", 28 Mayıs 2012, http://www.ehackingnews.com/2012/05/flame-worm-iran-uncovers-stuxnet-style.html (Erişim tarihi: 23 Kasım 2012).

89 Ibid.

90 Antiy Labs, *Analysis Report on Flame Worm Samples Version 1.3*, http://www.antiy.net/downloads/Analysis-Report-on-Flame-Worm-Samples.pdf (Erişim tarihi: 4 Ağustos 2012).

başka bilgisayarları etkileme kapasitesine de sahipti. Bütün sahip olduğu bilgileri komuta kontrol sunucusunda görebilmekte ve ilave modülleri indirerek kapasitesini arttırabilmekteydi.[91]

Türkiye'de Siber Güvenlik

NATO'nun bütün üyelerinin siber kabiliyetlerini arttırma ve ortak bir düzlemde çalışabilir hale getirme çabaları, Türkiye'nin siber güvenlik konusundaki çalışmalara hız verdi. Türkiye'de yetkililer uzunca bir süre siber tehditleri sadece siber suç seviyesinde değerlendirdi. Hatta önemli güvenlik kurumlarına yapılan saldırılar terörle mücadele çerçevesinde ele alındı.[92] Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (Tübitak) bünyesinde kurulan birimler ve ulusal bilgi güvenliği kapısıyla devlet kurumlarındaki siber güvenlik bilinci arttırılmaya çalışıldı. 27 Ekim 2010'da toplanan Milli Güvenlik Kurulu'nda siber tehditler tartışılarak, Milli Güvenlik Siyaset Belgesi'ne girmesine karar verildiği ilan edildi. 25-28 Ocak 2011'de Tübitak ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) ortaklığıyla *I. Ulusal Siber Güvenlik Tatbikatı* icra edildi. Tatbikat sonrası yayınlanan rapordaki bulgular Türkiye'nin siber saldırılara açık olduğunu ve konunun kamu kuruluşlarında yeterince ciddiye alınmadığını ortaya çıkardı.[93]

2011'de Emniyet Genel Müdürlüğü'nde Bakanlar Kurulu kararıyla Bilişim Suçlarıyla Mücadele Daire Başkanlığı kuruldu. Bu dönemde mahkeme kararlarıyla *Youtube* ve *Blogspot* gibi sayfalara erişimin yasaklanmasını protesto etmek için *Anonymous* grubunun İçişleri Bakanlığı'ndan Büyük Millet Meclisi'ne kadar 20 farklı kuruma saldırması tehditin ne derece büyüdüğünün yakından farkedilmesini sağladı.[94] Öte yandan *Redhack* isimli grubun 2012'de Ankara Emniyet Müdürlüğü, İçişleri Bakanlığı, Dışişleri Bakanlığı ve Kara Kuvvetleri Komutanlığı da dahil olmak üzere birçok kamu kuruluşuna yaptığı saldırılar ve bu saldırıların medyada yer bulması, Türkiye'de siber tehdit algısının oluşmasını hızlandı. Bunun üzerine 20 Ekim 2012'de toplanan Bakanlar Kurulu, "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"ı onayladı. Bu kararda siber güvenlik kurulunun Ulaştırma, Denizcilik ve Haberleşme Bakanlığı başkanlığınca oluşturulmasına karar verildi. Ulaştırma, Denizcilik ve Haberleşme Bakanı başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği müsteşarı, Milli İstihbarat Teşkilatı müsteşarı, Genelkurmay Başkanlığı Muhabere, Elektronik ve Bilgi Sistemleri başkanı, Bilgi Teknolojileri ve İletişim Kuru-

91 Kaspersky Lab Global Research and Analysis Team, *Gauss: Abnormal Distribution,* http://www.securelist.com/en/downloads/vlpdfs/kaspersky-lab-gauss.pdf (Erişim tarihi: 12 Ağustos 2012).

92 "PKK'nın en önemli hacker'ı yakalandı", *Hürriyet*, 19 Kasım 2008, http://hurarsiv.hurriyet.com.tr/goster/printnews.aspx?DocID=10393202 (Erişim tarihi: 21 Ocak 2013).

93 Tübitak ve BTK, "I. Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu", 2011, http://www.uekae.tubitak.gov.tr/uekae_content_files/siber_tatbikat_raporlari/USGT_2011_tr.pdf (Erişim tarihi: 23 Ocak 2013).

94 "Türkiye'ye Siber Saldırı", *Hürriyet*, http://www.hurriyet.com.tr/teknoloji/20440458.asp (Erişim tarihi: 11 Ocak 2013).

mu başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu başkanı, Mali Suçları Araştırma Kurulu başkanı, Telekomünikasyon İletişim başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmasına karar verildi. Bu kurulun görevi "kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda yer alan sistemlerin güvenliğinin sağlanmasına ve gizliliğin korunmasına yönelik tedbirlerin alınması ve bilgi ve iletişim teknolojilerine ilişkin kritik altyapıların işletiminde yer alan gerçek ve tüzel kişilerce uyulması gerekli usul ve esasları düzenlemek" olarak belirlenmiştir.[95] Siber Güvenlik Kurulu'nun toplantıları sonrasında Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 18.2.2013 tarihli ve 412 sayılı yazısı üzerine, Bakanlar Kurulu'nun 25.3.2013'de onayıyla, 20 Haziran 2013'de Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 4890 sayılı Resmi Gazete'de yayınlandı. Stratejik yaklaşımında nispeten zayıflıklar bulunan belgede Eylem Planı'nın detaylandırıldığı görülmektedir. Ulusal siber güvenlik strateji eylemlerini şöyle sıralamaktadır:

1. Yasal düzenlemelerin yapılması,
2. Adli süreçlere yardımcı olacak çalışmaların yürütülmesi,
3. Ulusal siber olaylara müdahale organizasyonunun oluşturulması,
4. Ulusal siber güvenlik altyapısının güçlendirilmesi,
5. Siber güvenlik alanında insan kaynağının yetiştirilmesi ve bilinçlendirme faaliyetleri,
6. Siber güvenlikte yerli teknolojilerin geliştirilmesi,
7. Ulusal güvenlik mekanizmanlarının kapsamının genişletilmesi. [96]

Siber güvenlik eylem planının sonunda stratejik eylemlerin uygulanması için oluşturulan detaylı bir takvim yer almaktadır. Farklı kamu kurum ve kuruluşlarına paylaştırılan görevlerin Eylül 2014'de bitmiş olması beklenmektedir. Siber güvenlik için gerekli olan hamlelerin detaylı olarak listelendiği bu eylem planı teorikte optimum düzeyde olsa da pratik de uygulanabilirlik sorunlarına sahiptir. Siber Güvenlik eylem planında yer alan işlemlerin küçük kısmının bile tamamlanmasının, Türkiye'nin siber güvenlik altyapısı için büyük bir katkı sağlayacağı açıktır. Türkiye planladığı siber güvenlik eylemlerini gereği gibi yerine getirmeyi başarırsa, NATO'nun istediği siber savunma seviyesine de yaklaşmış olacaktır.

95 *Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar*, http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf (Erişim tarihi: 18 Ocak 2013).

96 *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*, Resmi Gazete, Sayı 2013/4890, 20 Haziran 2013, http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf (Erişim tarihi: 18 Ağustos 2018).

Sonuç

Günümüze kadar oluşan gelişmeler de siber dünyanın getirdiği nimetlerin günden güne artmasıyla birlikte güvenlik açısından problemlerin sayısı da artmıştır. Öte yandan bütün reel kavramlarımızın başına siber ön takısıyla oluşturduğumuz ifadelerle, kavram karmaşası da artmaktadır: Siber terörizm, siber savaş, siber tehdit, siber çeteler, v.b. Siyasi değerlendirmelerimizde sınırlarının nerede başlayıp nerede bittiğini bilemediğimiz kavramlar siber uzayın farklı yapılanması nedeniyle durumu daha da karmaşıklaştırmaktadır.

Siber uzayın gelişen ortamı henüz uluslararası sistem ve hukukun bütünüyle kapsayabildiği bir alan değildir. Halihazırda bütün ülkeler "milli" siber alanlar oluşturmaya çalışmaktadırlar. Gerek ABD'nin kendine yönelen bir saldırı olduğunda interneti kapatma gayretleri, gerekse İran'ın *Stuxnet* sonrasında kapalı internet oluşturma çabaları sınırların belirlenmesine yönelik doğum sancılarıdır.

Aktörlerin belirsizliği ve siber uzayın hızı ulus devletleri internet karşısında aciz bırakmaktadır. Büyük ve simetrik devlet yapılarının yeni ortaya çıkan bu tehditlere karşı eski organizasyonlarla karşılık vermekte zorlandığı görülmektedir. Siber tehditlerle mücadele edebilmek için devletlerin asimetrik ve hızlı tepki veren organizasyonlara ihtiyacı vardır. Tehdidin niteliğini derinlemesine anlamak, geliştirilecek tedbirlerin tutarlılığını arttıracaktır.

Siber güvenlik alanında donanım ve yazılımın önemini vurgularken bütün bu altyapıyı kullanacak olan insanların en önemli halka olduğunun unutulmaması gereklidir. Tüm önlemlere rağmen siber uzayın sunduğu nispeten kontrolsüz yapı, *Stuxnet*, *Flame* gibi saldıranın belirsiz olduğu ama verilen zararın büyük olduğu olaylara neden olmaktadır. Büyüklüklerine bakılınca saldırıların arkasında devletlerin olduğu tahmin edilmektedir. Fakat siber uzayın kendine has yapısı böyle bir saldırının kimin tarafından yapıldığını kanıtlamayı güçleştirmektedir. Öte yandan siber uzayda her an fark edilmeden birçok siber casusluk faaliyeti de gerçekleşmektedir. Sanıldığının tersine siber güvenlik dünyasında açıkça ilan edilen saldırılardan ziyade sessizlikle icra edilenler daha etkin ve korkutucudur. Bu tür operasyonlar *Stuxnet*'te olduğu gibi web sayfalarının ele geçirilmesinden daha etkili eylemlerdir.

Gelecekte Siber güvenliği etkileyecek en önemli unsur insan ve teknolojinin yaygınlığıdır. Gelecek nesiller küçük yaşlardan itibaren bilişim teknolojileriyle büyüdükleri için bilişim teknolojilerine daha hakim olduklarını görüyoruz. Bilişim teknolojilerinin evlerimizin ve işlerimizin her noktasında artan hakimiyeti insan unsuruyla birleştiğinde gelecek yıllarda nasıl bir dünyada yaşayacağımızı tahmin etmek zor olmayacaktır.

Öte yandan devletlerin siber uzayı yakından takip ederek, vatandaşlarını takip eden teknolojilere yönelmeleri de çokça tartışılan noktalardan birisidir. İnternetin getirdiği özgürlük ortamının genişlemesi devletlere olayların kontrolden çıkabileceği bir medyanın var olduğu hissini vermektedir. Bu durumda devletler de internet üzerinden bireysel hak ve özgürlükleri ihlal edecek şekilde insanları izlemeye başlamışlardır. Fakat bunu fark eden insanların (çoğunlukla *hacker*ların) önderliğinde muhalefet grupları da oluşmaya

başladı. Devletlerin kontrolü arttıkça buna karşı oluşan protest gruplarının saldırıları da artmaktadır. Ortaya çıkan şiddet sarmalı ise siber güvensizliği arttırmakta ve siber çatışmanın en üst seviyesi olan siber savaş ihtimalini sık sık gündeme getirmektedir.

Siber savaşın bu denli yüksek sesli konuşulması devletlerin muhtemel çatışma ihtimaline karşın büyük yatırımlar yaparak hazır olma sürecini başlatmaktadır. Siber silahlar ve güvenlik araçları sağlamak için gelişen endüstri beraberinde bu konuda hacmi artan ekonomi günden güne büyümektedir. Muhtemeldir ki, bir gün tehdidin belirsizliği ya da imkansızlığı haline bakılmaksızın genişleyen siber güvensizlik alanı ve onun ekonomisi, varlıklarını anlamlandırmak için çatışmayı teşvik eder hale geldiğini göreceğiz. Böyle bir sürece engel olmak siber güvenlik için atılacak en önemli adımdır.

Siber uzayın getirdiği nispeten özgürlükçü ifade ortamına zarar vermeden esnek ve dinamik çözümler üretilmelidir. Günümüz güvenlik algılarının bu anlamda büyük değişimlere ihtiyacı vardır. Devletlerin siber uzayın oluşturduğu sanal gerçekliği derinden anlaması ve buna uyumlu yapılar oluşturması zorunludur. Bu süreç tam anlamıyla gerçekleşinceye kadar siber güvenliğin sağlanması da kolay değildir.

Summary

Westphalian state system has been deeply affected from the civilianization of the cyber space. It is possible to see the traces of nuclear war and its competition in this new post-Cold War period. The contemporary threats against the cyber space and their vague boundaries could clearly be seen in the examples. Cyber-attacks in this new security environment towards long lasting alliance NATO and its members are giving important clues for the future. In this article, one discussed defensive measures of NATO for these new threats and the process which determined the cyber security strategies. Upon this cyber defense strategy, NATO tries to level the cyber capabilities of its members and takes the necessary steps to achieve this goal. The Lisbon summit endorsed the preparation of a new strategy that includes cyber defense and protection of the critical information infrastructure.While this capacity building process was continuing, the detection of Stuxnet has sparred a new debate on how to protect the critical infrastructure facilities which not only affected Iranian nuclear centrifuges but also the infrastructures of other countries. Other Stuxnet malware variations such as Gauss, Flame appeared short after the detection of Stuxnet which increased cyber security concerns. Turkey as a NATO member has added cyber security concept to its national security agenda. Follow-up, Turkey also announced its national cyber strategy with an action plan.