ULUSLARARASI İLİŞKİLERDE YENİ BİR KUVVET ÇARPANI: SİBER SAVAŞLAR ÜZERİNE BİR VAKA ANALİZİ

Serkan YENAL[1], Naci AKDEMİR[2]

Öz

Savaş her çağda farklı şekilde gerçekleştirilmiş, gelişen koşullar ve teknoloji savaşın doğasını değiştirmiştir. Başlangıçta, basit silahlarla icra edilen savaşlar ve sonuçları, gelişen silah teknolojisi doğrultusunda kapsamlı bir biçimde değişmiştir. Bu değişim bir anda meydana gelmemiş yüzlerce yıllık bir sürecin sonucu olarak ortaya çıkmıştır. Günümüzde pek çok ülkenin gündemini meşgul eden "siber savaşlar"bu sürecin son halkalarından birisidir. Çalışmamızda 1900'lü yıllardan günümüze kadar meydana gelmiş önemli siber savaş olayları arasından amaçlı örneklem yöntemi ile dokuz olay seçilmiştir. Seçilen olaylar, Vaka analizi metodu kullanılarak, NVIVO nitel analiz programı vasıtasıyla temalandırılmıştır. Tematik analiz, siber savaşların İkinci Dünya Savaşı, Soğuk Savaş ve Milenyum Evreleri olarak üç ana evreden geçtiğini ortaya koymuştur. Çalışmamız ilk örneklerine soğuk savaş ve İkinci dünya savaşında sınırlı etkiye sahip olan siber savaşın, 2000'li yıllarda zararlı yazılım ve kriptografi alanlarında meydana gelen değişim ve internet tabanlı uygulamaların hayatın her alanında yaygınlaşmasıyla yıkıcı etkilere neden olabileceğini ortaya koymuştur. Analizimiz, milenyum evresinde siber savaşın konvansiyonel bir savaşla koordineli olarak bir başka devlete isteklerini kabul ettirmek, düşman ülkelerin kritik alt yapılarını tahrip etmek, siyasi anlaşmazlık esnasında hasım ülkenin kamuoyu üzerinde psikolojik üstünlük sağlamak gibi amaçlarla işlendiğini göstermiştir. Tartışma bölümünde siber savaş vakalarından alınan dersler yorumlanmıştır.

Anahtar Kelimeler: Uluslararası Güvenlik, Siber Güvenlik, Siber Savaş, Siber Suçlar.

[1] Dr. Öğr. Üyesi, Milli Savunma Üniversitesi KHO Svn. Yön. Bölümü, syenal@kho.edu.tr, ORCID No: 0000-0002-8188-5095.
[2] Dr. Öğr. Görevlisi, Jandarma ve Sahil Güvenlik Akademisi Fakültesi, naciakdemir@jandarma.gov.tr, ORCID No: 0000-0002-4288-6482.
Makale Gönderilme Tarihi: 7 Nisan 2020. Makale Kabul Tarihi: 21 Nisan 2020.
Makale Türü: Araştırma Makalesi

A NEW FORCE MULTIPLIER IN INTERNATIONAL RELATIONS: A CASE STUDY OF CYBER WARFARE

Serkan YENAL, Naci AKDEMİR

Abstract

War has been carried out differently throughout history. Evolving conditions, coupled with technological advancements, has altered the nature of the war. The extentand the adverse impacts of wars, which were initially performed with rudimentary weapons, have also displayed dramatic changes paralel to the developments in warfare technology. This change is the outcome of a process that lasted forcenturies. Cyber warfare that has become the Tier One issues for many countries is the ultimate chain of this process. This study utilized a purposeful sampling method to select nine cases among the important cyberwar events that have occurred from the 1900s to the present day. The selected events were the med by using the Case Study approach through the NVIVO qualitative analysis program. The maticanalys is revealed that cyberwars went through three main phases, World War II, the Cold War, and the Millennium Phases. Our study has revealed that cyberwarfare, which had limited effects in the Cold War and WWII, may cause destructive effects paralel to the developments in malware writing and cryptography in the 2000s as well as the intrusion of the internet-based applications in all areas of life. Our analysis has shown that cyberwarfare is conducted to achieve various goals including administering convention altogether with cyber warfare, coercing another state to accept the sanctions, destroying critical infrastructures of enemy countries, and providing psychological superiority over the public opinion of the hostile country during the political dispute. In the discussion section, the lessons learned from cyberwarfare cases are interpreted.

***Keywords*:** International Security, Cyber Security, Cyber Warfare, Cybercrime.

Giriş

Savaş, insanlık tarihinde ilk insandan bugüne kadar var olmuştur. İnsanlar bazen çıkarlarını korumak bazen iktidarı elde etmek ve sürdürmek bazen dini gerekçeler bazen de toprak elde etmek amacıyla savaşmışlardır. Savaş günümüzde çok farklı anlamlar kazanmış aynı zamanda farklı disiplinlerin inceleme alanına girerek multidisipliner bir olgu haline gelmiştir.

İçinde bulunduğumuz döneme bakıldığında, tüm dünyada hızlı bir şekilde etkisini gösteren küreselleşme ve hızlı şekilde artan teknolojinin getirdiği büyük kolaylıklar yanında aynı zamanda savaşların yöntemlerinin ve etkilerinin de önemli oranda değiştiği görülmektedir. Yaşanılan savaşlar, önceki dönemlerden çok farklı aktörler ve sektörlerin de işin içine dâhil olmasıyla farklı bir boyuta taşınmıştır. Günümüzde savaşlar sadece iki devlet ve bunların orduları arasında yaşanmamakta, farklı sivil toplum kuruluşları yardım kuruluşları, şirketler, devlet dışı oluşumlar, terör örgütleri, uluslararası şirketler gibi unsur ve aktörler birer savaş unsuru haline gelmektedir.

İletişim teknolojilerindeki hızlı gelişmelerin bir yansıması olarak internetin hayatımızda hızlı bir şekilde yerini alması, diğer eşya, ev ve araçlardaki teknolojik gelişmelere entegre olması bu sayede giderek artan oranda kullanılan cihazların "akıllı" hale gelmesi kuşkusuz insan yaşamını kolaylaştırmaktadır. Bununla birlikte bulunulan ortam itibariyle güvenlik açıkları da ortaya çıkmakta, bu açıklardan faydalanan kötü niyetli kişiler kendi çıkarları doğrultusunda bireyler ve kurumlara saldırılar gerçekleştirmektedir. Bireyler ve kurumlar arasındaki mücadelenin bir yansıması olarak bilişim dünyası ya da siber dünya olarak da adlandırılan, dijital dünya, aynı zamanda ülkeler arasındaki mücadelenin de aktif olarak yaşandığı bir ortam halini almıştır.

Savaşlardaki bu dönüşüm, güçlü ya da zayıf devlet tanımını da değiştirmiştir. Günümüzde ordularda çok sayıda askerin çok sayıda silah, tank, uçak gibi silahların bulunması, tek başına bir devletin güçlü kabul edilmesi için yeterli değildir. Bir devlet, teknolojik gelişmelere ayak uydurup, etrafındaki tehditlerden kendini soyutlayabildiği ve caydırıcı bir unsur olabildiği ölçüde güçlü sayılmaktadır. Zira geçmişte onlarca yıllık saldırılarda verilebilecek zarar, bir tek bilgisayarla yüzlerce kat düşük maliyetlerle gerçekleştirilebilmektedir.

Siber alan ya da siber dünya olarak da adlandırılan internet dünyası pek çok imkânı insanların kullanımına açmıştır. Geçmişte çok uzun süren pek çok iş

ve işlem saniyeler içinde gerçekleşmektedir. Ülkeler, kurumlar ve bireyler pek çok bilgiye internet üzerinde ulaşmakta, kamu ve özel hizmetler bu şekilde gerçekleşmektedir. Bütün bu imkânların yanında, birey, kurum ve devletlerin siber alandaki bilgilerinin ve hizmetlerin güvenliğinin sağlanması çok önemli bir sorun haline gelmiştir. Zira artık savaşlarda bu bilgiler ve hizmetler hedef haline gelmiştir. Bu artan tehdit işletmelerin ve kurumların imajının toplumdaki bir yansıması olan kurumsal itibarın (Güleryüz ve Dalkılıç, 2019) azalmasına ve organizasyonlar ile çevrimiçi ticaret yapan firmalara güvenin azalmasına neden olmaktadır.

Günümüzde siber savaşlar, basit bilgi çalma faaliyetlerinden büyük bir nükleer reaktörü etkisiz hale getirmeye, bir insansız hava aracını yere indirmekten, büyük yolcu uçaklarını çarpıştırmaya kadar giden bir boyuta ulaşmıştır (Başaranel ve Türkşen, 2019). Kavramsal çerçeve bölümünde siber dünya ve siber savaş kavramları incelenecek, siber savaş ve siber saldırı yöntemleri anlatılacak ve siber savunmada uluslararası önlemler ve Türkiye'deki siber savunma çalışmaları anlatılacaktır.

Kavramsal Çerçeve

Günümüzde, internet günün her anında ve her yerde kullanılan bir sistem haline gelmiştir. Daha önceleri uzun zaman iş ve işlemler internet sayesinde saniyeler içerisinde gerçekleştirilebilmektedir. Yarattığı bu cazibe aynı zamanda önemli güvenlik sorunlarını da beraberinde getirmektedir. Zira her birey ve kurum, çok önemli bilgilerini internet ortamında saklamakta olup temel devlet hizmetleri internetten verilir hale gelmiştir. Bu durum suç örgütleri ve terör örgütleri gibi kötü niyetli kişi ve grupların da doğal olarak ilgilerini çekmektedir (Başaranel, 2017).

Siber dünya, siber uzay, siber ortam olarak da ifade edilen ve internet sisteminin bütününü anlatan kavramların birbirinden farklı çok sayıda tanımı yapılmıştır. Bu tanımlardan bir kısmını şu şekilde inceleyebiliriz.

Siber uzay, sanal bilgisayar dünyasına atıfta bulunur ve daha özel olarak, çevrimiçi iletişimi kolaylaştırmak amaçlı, küresel bilgisayar ağı oluşturmak için kullanılan dijital bir ortamı ifade eder (Technopedia, 2019). Diğer yandan, Beyaz Saray tarafından yayınlanan Amerika Ulusal Güvenlik Direktifi (*National Security Presidential Directive 54/Homeland*), siber uzayı "birbirine bağlı bilgi teknolojisi ağı, alt yapı ve kritik endüstrilerdeki interneti, iletişim ağlarını, bilgisayar sistemlerini ve gömülü işlemci ve denetleyicileri içeren bir kavram" olarak nitelendirir (The White House,

2008:3). Bu açıklamayla kavram içerisinde özellikle kritik sektörlerdeki internet ve bilişim sistemi kullanımı ifade edilmektedir.

Çiftçi'ye göre (2017:5), siber ortam aşağıdaki unsurlardan oluşmaktadır:

- ✓ **Donanım:** Sunucular, istemciler, bilgisayarlar, akıllı telefonlar, şifreleme sistemleri, merkezi denetleme kontrol ve veri toplama (Supervisory Control and Data Acquisitation-SCADA) sistemleri ve sensörlerden,

- ✓ **Yazılım:**İşletim sistemleri, veritabanı yazılım sistemleri, uygulama yazılımları, gömülü yazılımlardan,

- ✓ **İletişim Altyapısı:** Kablolu/kablosuz iletişim ağları, telsiz, uydu, iletişim sistemleri ve internetten oluşmaktadır.

Görüldüğü gibi yukarıdaki tanımların tümü siber uzayın tanımını teknolojik unsurları açısından yapmaktadır. Oysa insan faktörü siber uzayın en önemli parçalarından birisidir. Siber uzayı sosyo-kültürel bir ortam ele almak gerekirse, siber uzay fiziksel, mantık ve sosyal katman olmak üzere üç unsurdan oluşmaktadır (Pamphlet, 2010:8).

Gelinen noktada, siber dünya, bir anlamda iletişimin bugünü ve geleceğini ortaya koymaktadır ve dünyanın iletişim olanaklarına yönelik tehditlerin de en önemli muhatabı konumundadır. Bu tehditler özel olarak bir hedefe yönelebileceği gibi siber dünyanın geneline yönelik bir boyut da alabilir. Bu noktada siber güvenlik kavramı gündeme gelmektedir.

Siber güvenlik, siber ortamı ve örgütü, kullanıcı bilgilerini korumak için kullanılabilecek araçlar, politikalar, güvenlik kavram ve önlemleri, rehberler, risk yönetimi yaklaşımları, faaliyetler, eğitim, iyileştirme uygulamaları, güvence ve teknolojilerin toplamını ifade eder. Organizasyon ve kullanıcı varlıkları arasında bağlı bilgi işlem cihazları, personel, altyapı, uygulamalar, servisler, telekomünikasyon sistemleri ve siber ortamdaki iletilen ve / veya depolanan bilgilerin toplamı bulunur. Siber güvenlik, kuruluşun güvenlik özelliklerinin ve kullanıcı varlıklarının siber ortamdaki ilgili güvenlik risklerine karşı ulaşılmasını ve bakımını sağlamak için çaba gösterir (ITU, 2020).

Bu noktada siber güvenliğin önemi gün geçtikçe artmaktadır; zira günümüzde devlet kuruluşları, finansal ve tıbbi kuruluşlar dijital olarak

devasa boyutta veri toplamakta, işlemekte ve depolamaktadır. Bu verilerin önemli bir kısmı da fikri mülkiyet, finansal veriler, kişisel bilgi veya gizlilik derecesi yüksek hassas bilgilerden oluşmaktadır (Digitial Guardian, 2019).

Kurumların, devletlerin internet kullanımı yanında bireylerin de internet ve sosyal medya kullanımı hızla artmaktadır. Bu durum, siber güvenliğin bir de bireysel boyutunu ortaya koymaktadır. Tablo:1'de internet ve sosyal medya kullanımı istatistikleri verilmektedir.

Tablo 1:
İnternet ve Sosyal Medya Kullanımı (milyar)

İnternet	Aktif Sosyal Medya	Cep Telefonu	Cep Telefonundan Sosyal Medya
4.021	3.196	5.135	2.958

Kaynak: (We are social, 2019)

Tablo-1'den de anlaşılacağı üzere, dünya genelinde 2018 rakamlarına göre, yaklaşık 4 milyar insan internet kullanmakta, yaklaşık 3 milyar 200 milyon insan aktif sosyal medya kullanmakta yine yaklaşık 5 milyar 150 milyon insan cep telefonu kullanıren bunların yaklaşık 3 milyarı mobil sosyal medya kullanıcısı bulunmaktadır. Yine ekim 2019'da yapılan araştırmaya göre, aktif sosyal medya kullanıcılarının toplam nüfusa oranı yüzde 48'e ulaşmıştır (We are social, 2019). Dünya genelinde bireylerin internet kullanımı dünya nüfusunun yaklaşık yarısına ulaşmıştır. Bu durum internet ve sosyal medyanın, devasa bir piyasa oluşturduğunu gözler önüne sermektedir. Bu istatistikler aynı zamanda dünya nüfusunun yaklaşık yarısının siber tehditlere açık olduğunu da ortaya koymaktadır. Zira internet kullanan insanların çok önemli bir yüzdesi aynı zamanda aktif sosyal medya kullanıcısı durumundadır. Kişisel bilgiler ve görüntülerin sürekli biçimde dijital ortamda tutulması, siber güvenliğin önemini ortaya koymaktadır.

Siber Savaş, bir ulus devletin başka bir ulus devletin bilgisayarlarına ya da ağlarına nüfuz etme, hasar verme veya aksamaya yol açma eylemleri olarak ifade edilmektedir (Clarke ve Knake, 2010:6). Buradan hareketle siber savaşın bazı unsurları ortaya çıkmaktadır. Bunlardan birincisi aktör, ikincisi amaç unsurudur. Aktör noktasında, siber savaşın aktörlerinin ulus devlet olması söz konusudur. Zira devlet dışı organizasyonların da siber saldırı

gerçekleştirmesi söz konusu olsa da bu durum, siber suçlar kapsamına girmektedir. İkincisi amaç unsurudur. Bu noktada bir ulus devletin diğer ulus devletin bilgisayar ya da ağlarına zarar verme amacıyla hareket etmesi beklenmelidir.

Temel Siber Saldırı Türleri[3]

İlk örnekleri 1800'lü yıllarda ortaya çıkan ve geçmişte birkaç kişiyi ya da işletmeyi etkileyen saldırılar günümüzde küresel ölçekte milyonlarca kişiyi etkileyen aynı zamanda milyarlarca dolarlık zarar meydana getiren devasa boyutlardaki saldırılara dönüşmüştür. Bu durum gelecekte, teknolojik gelişmelerin yaygınlaşması ve hayatın tüm aşamalarına nüfuz etmesi sebebiyle artarak devam edeceğe değerlendirilmektedir. Günümüzdeki siber silahlar aşağıdaki tabloda açıklanmıştır:

Tablo 2:
Günümüzde Siber Silahlar

Silah	Etki
Mantık Bombaları (logicbombs)	Bilgisayar sistemi ya da ağa, istenildiği zaman faaliyete geçen ve sunucu sisteme ciddi zarar veren kodlar yerleştirilmesi biçiminde gerçekleştirilir. Bu saldırılarda sistem kapatılabilir ya da bütün veriler silinebilir.
Tuzak Kapıları (Trapdoors)	Bir yabancı sistem ya da ağa, sonraki bir zamanda yeniden girebilmek için kod parçaları ya da sistem giriş mekanizmaları bırakılır ya da bu giriş kapıları oluşturulur.
Botnet	Birlikte çalışmaya zorlanan bilgisayarlardan oluşan bir ağın yetkisiz bir uzak kullanıcının kontrolüne girmesidir. Bu robot bilgisayar ağı, başka bilgisayarların ağına girmek için kullanılır.

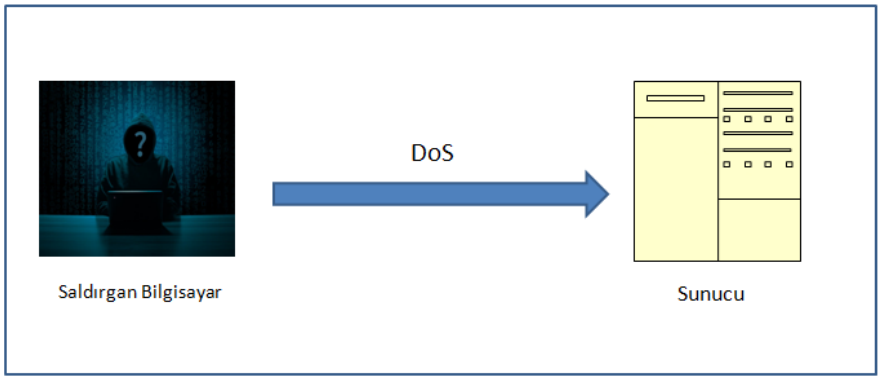
Kaynak: US Cyber War, 2020

Tablo 2'den de anlaşılabileceği üzere, günümüzdeki siber silahlar çok düşük maliyetle çok büyük sonuçlar doğurabilmektedir. Çoğu zaman kötü niyetli bir kişinin yeterli olduğu bu saldırılarda milyonlarca kişiyi etkileyen bir saldırı gerçekleştirmek mümkün olabilmektedir. Tablo 3'de tanımlanan siber

[3] Bu bölümde yer alan tüm şekiller kaynaklarından esinlenerek yeniden üretilmiştir.

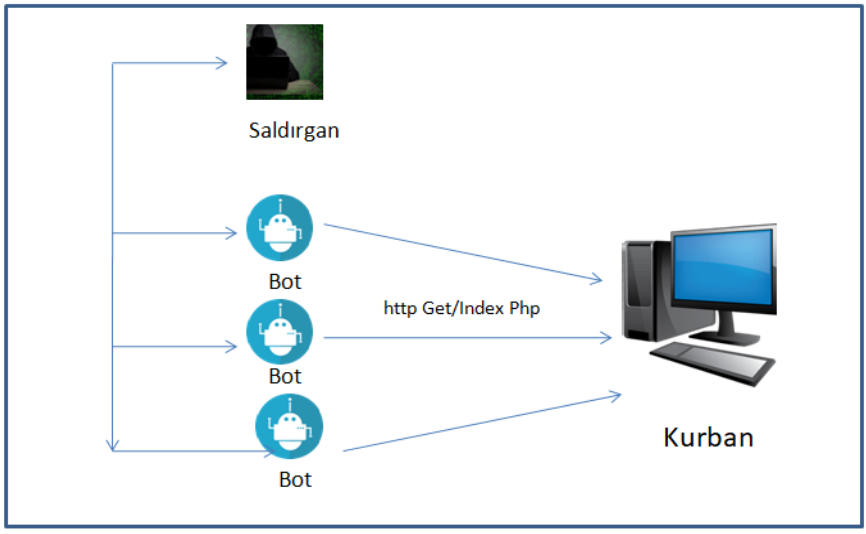
silahlar kullanılmak suretiyle siber saldırılar genel olarak aşağıdaki biçimlerde gerçekleştirilmektedir:

DoS (Denial of Service-Hizmet Reddi) Saldırısı: Bu tür saldırılarda, bir makine ya da ağı kapatarak, hedeflenen kullanıcıların ona erişiminin engellenmesi söz konusudur. DoS saldırıları, hedefi trafiğe boğarak ya da bir çökmeye neden olacak derecede fazla veri göndererek gerçeleştirilir. Her iki durumda da bu tür siber saldırıda, meşru kullanıcılar (çalışanlar, üyeler ya da hesap sahipleri) bekledikleri hizmet ya da kaynaktan mahrum kalır. DoS saldırıları genel olarak bankacılık, ticaret ve medya şirketleri gibi yüksek profilli kuruluşların internet sitelerini hedef alır ve büyük maddi kayba neden olabilir (Paloaltonetworks, 2020).



Şekil:1 DoS Saldırısı Süreci (Cloudflare, 2020a)

DDoS (Distributed Denial of Service-Dağıtılmış Hizmet Reddi) Saldırısı: Bu tür saldırılar, DoS (hizmet reddi)saldırılarının bir alt sınıfıdır. Bir DDoS saldırısı, toplu trafik olarak da bilinen, biribirine bağlı birden çok çevrimiçi cihazı içerir. Bunlar, sahte bir trafiği olan bir hedef internet sitesini bunaltmak için kullanılır. Diğer siber saldırılardan farklı olarak, DDoS saldırıları güvenlik duvarını delmeye çalışmak yerine, bazen internet sitelerini ve sunucuları, yasal kullanıcılar için kullanılamaz hale getirmeyi amaçlar. Bazen de diğer kötü amaçlı etkinlikler için hedefin güvenlik duvarını ihlal ederek, güvenlik ağlarını devre dışı bırakmak yöntemiyle çalışır (Imperva, 2020).



Şekil:2 DDoS Süreci (Cloudflare, 2020b)

Malware (Kötü Amaçlı Yazılım):Malware casus yazılım, fidye yazılımı, virüsler ve solucanlar gibi kötü amaçlı yazılımları tanımlamak için kullanılan genel bir terimdir. Kötü amaçlı yazılım, genellikle kullanıcılar riskli yazılımı yükleyen tehlikeli bir bağlantıyı veya e-posta ekini tıkladığında, bir güvenlik açığını istismar eder. Bu yazılım farklı maksatlarla kullanılabilir. Örneğin, ağın temel bileşenlerine erişimi engellemek (fidye yazılımı), kötü amaçlı yazılım veya ek zararlı yazılım yüklemek, sabit sürücüden veri ileterek gizlice bilgi almak (casus yazılım) maksatlarıyla kullanılabilir (Cisco, 2019).

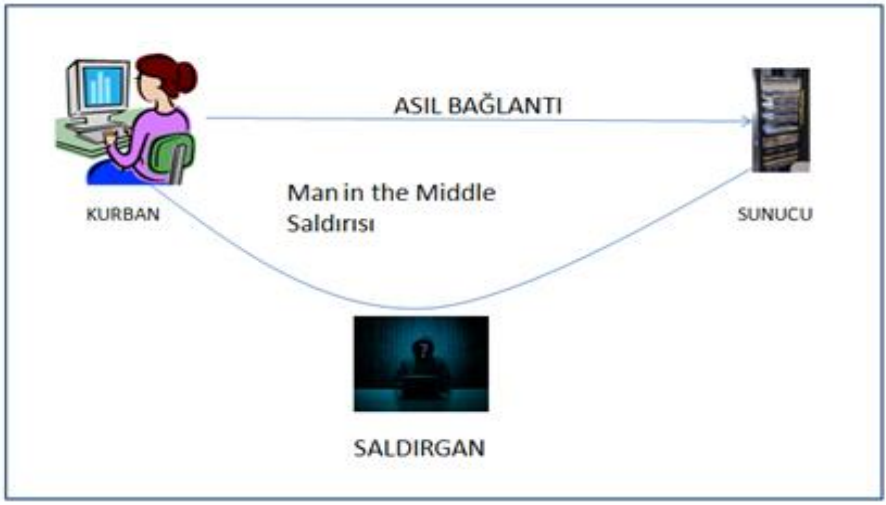
Phishing (Yemleme): Oltalama saldırıları olarak da bilinen bu saldırı türü, tarihin en eski ve etki düzeyi yüksek saldırıları arasındadır. Bu saldırı türünde e-posta ve kısa mesaj gibi araçlarla cazip sahte mesajlar göndererek parola, kimlik bilgisi vb. kişisel verilerin çalınması amaçlanmaktadır. Gönderilen virüslü dosyaların açılmasıyla birlikte kurbanların cihazları saldırganların kontrolüne girebilir ve bu şekilde maddi kayıplarla birlikte gizli bilgilerin de ele geçirilmesi söz konusu olabilir (BGA secuity, 2019).

Zararlı yazılım gibi teknik saldırılara ilave olarak, sosyal mühendislik yöntemleri de oltalama saldırılarında sıkça kullanılmaktadır. Örneğin, saldırganlar genellikle, gerçek bir kişi ya da seçilen kurbanın iş yapabileceği bir şirket biçiminde güvenilen bir varlık olarak maskelenir (Fruhlinger, 2019). Hedefi maskelenen kişi olduğuna inandıran saldırgan bu yöntemle,

genellikle finansal kontrolün zayıf olduğu ülkelerde açılan hesaplara para transferleri yapılmasını sağlarlar.

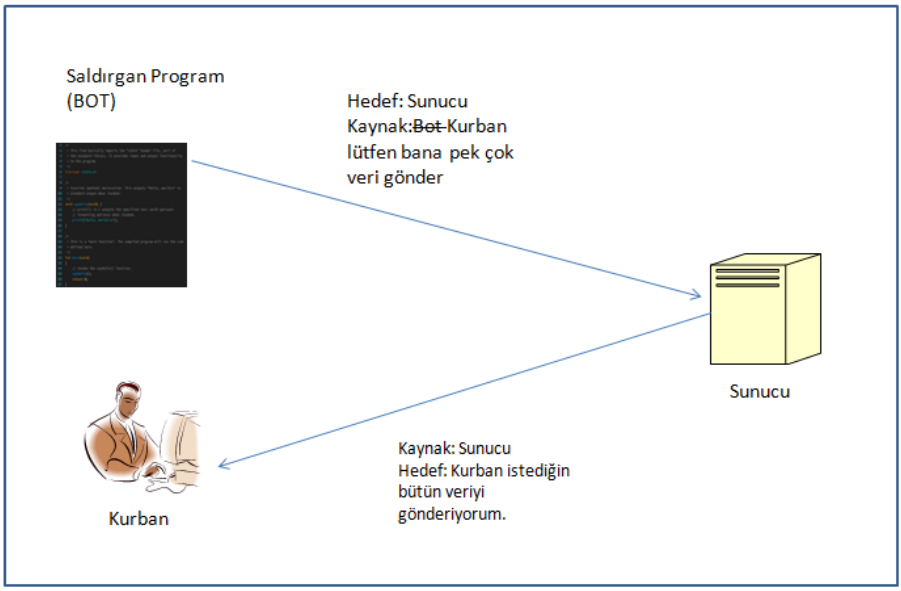
Man in the middle (MitM-Ortadaki Adam) Saldırısı: Bu tarz saldırılar, bir bilgisayar korsanının bilgisayar kullanıcısının ve sunucunun iletişimi arasına gizlice nüfuz ettiğinde gerçekleşmektedir. Ortadaki adam saldırılarının bazı yaygın türleri şu şekilde sıralanabilir (Melnick, 2018):

a) Oturum Çalma: Bu tür bir MitM saldırısında, bir saldırgan güvenilir bir istemci ve ağ sunucusu arasındaki bir oturumu ele geçirir. Saldırı yapan bilgisayar IP adresini güvenilir istemci yerine geçirir. Böylece oturumu devam ettirerek sunucuyu istemci (gerçek bilgisayar kullanıcısı) ile iletişim kurduğuna inandırır.



Şekil: 3 Oturum çalma süreci (Turk Hack Team, 2020)

b) IP Aldatmacası: Saldırganın kimliğini gizlemek, başka bir bilgisayar sistemini taklit etmek veya her ikisini birden değiştirmek için, olduğundan farklı bir kaynak adresi ile Internet Protokolü (IP) paketlerinin oluşturulmasıdır (Cloudflare, 2020c). Bu saldırı türünde, saldırgan, kurbanı güvenilen bir sistemle iletişim kurduğuna ikna etmeye çalışır ve bunu başardığında saldırı hedefine ulaşır (Melnick, 2018).



Şekil 4: IP Aldatmacası Süreci (Cloudflare, 2020c).

c) Tekrarlama: Bir saldırgan, eski iletileri yakalayıp kaydeder. Daha sonra katılımcılardan birini taklit ederek iletileri göndermeye çalışarak bir "tekrarlama saldırısı" gerçekleştirir (Melnick, 2018). Tekrarlama saldırılarının yarattığı ilave tehlike, saldırganın bir iletiyi ağdan aldıktan sonra şifresini bile çözmeye gerek duymadan her şeyi yeniden göndererek kurbanı inandırması ve saldırıyı başarıyla sonuçlandırmasıdır (Kaspersky, 2020).

Siber Savunmada Uluslararası Önlemler

İnternet, dijital olarak sunulan hizmetler, cihazlar ve gelişen teknoloji dünya ekonomilerinin "mütemmim cüz'ü" haline gelmiştir. Giderek daha fazla bağlantılı bir dünya konjonktüründe, etkili siber güvenlik mekanizmalarının oluşturulması büyük önem arz etmektedir. Artan kullanım ve teknolojiye olan bağımlılık ile güvenlik riskleri de atış göstermektedir (ITU, 2020b). Bu durum siber güvenlik konusunda bireysel ve ulusal önlemlerin yanında küresel önlemlerin de alınmasını zorunlu kılmaktadır.

Günümüzün en önemli ve etkili tehditlerinden biri konumuna gelen siber tehditler, asimetrik yapısı nedeniyle nükleer tehditlerden sonra ikinci sırada gelmektedir (Hajoary ve Akhilesh, 2020). Bu durum ülkelerin siber

savunmaya yönelik ilgisini artırmakta aynı zamanda önemli miktarlarda yatırım yapmalarına neden olmaktadır.

Oluşan risklere karşı koyabilmek için kullanıcılar, geleneksel olarak tehditleri azaltan, anti-virüs yazılımları, güvenlik duvarları, saldırı tespit sistemleri gibi mekanizmaları kullanmaktadır (Canbek, 2019:306). Bunun haricinde bireyler ve kurumlar sistem yedeklemesi, felaket kurtarma merkezleri gibi çalışmalarla veri yedeklemesi ve sistemi geri döndürmeye yönelik faaliyetlerle siber tehditlere karşı önlemler almaktadır.

Siber savunmada özellikle felaket kurtarma merkezleri önemli bir savunma mekanizması haline gelmiştir. Bu merkezler seçilirlen doğal afetlerden, fay hatlarından uzakta, mümkün olduğunca yangına karşı ek önlemler alınmış bir yapıda kurulmaya çalışılmaktadır. Bu sayede hassas verilerin, kurumsal bilgilerin, arşiv kayıtlarının muhafazası ve bir felaket gerçekleştiğinde sistemin geriye döndürülebilmesi mümkün hale gelmektedir.

Siber savunmaya yönelik bireysel, ulusal önlemlerin yanında uluslararası önlemler de alınmaktadır. Bu noktada Birleşmiş Milletler, NATO gibi uluslararası organizasonların aldıkları önlemler dikkat çekmektedir. Örneğin NATO'da toplu savunma, kriz yönetimi ve kooperatif güvenliğin temel görevlerini yerine getirebilmek için güçlü ve esnek siber savunma mekanizmlarına yatırım yapılmaktadır. NATO'da siber güvenliğe yönelik alınan önlemler kapsamında ilk olarak siber uzayı kara, hava ve denizden sonra dördüncü savaş alanı ilan etmiştir (NATO, 2019). Buna ilave olarak ittifakın süratle değişim gösteren siber tehditlere etkili bir cevap vermesini sağlamak maksadıyla Siber Savunma Sözleşmesi'ni 2016 yılında onaylamıştır. Ayrıca Siber Uzay Operasyon merkezi kurulmasına karar verilmiştir. NATO bu önlemler kapsamında uluslararası bir dizi sözleşme ve antlaşmalar hazırlamış, bunlar üye devletlerce imzalanmış ve bunların uygulamasını da üye devletler nezdinde takibini gerçekleştirmektedir.

NATO gibi Birleşmiş Milletler'in de siber savunma ile ilgili faaliyetleri bulunmaktadır. Buna göre, Birleşmiş Milletler bünyesinde kurulan Uluslararası Telekominikasyon Birliği (International Telecommunications Union-ITU), siber savunma faaliyetlerinde aktif rol almaktadır. Ayrıca "Siber Güvenlik Programı" hazırlanmakta ve üye ülkelere destek vermektedir. Bu program:

a) Üye ülkelerin ulusal siber güvenlik stratejileri belirlemesine yardımcı olmayı hedefleyen *"Ulusal Stratejiler"* (National Strategies),

b) Ülkelerde meydana gelebilecek siber güvenlik sorunlarına müdahale edebilecek ekiplerin oluşturulması, bu timlerin eğitimi ve ihtiyaçlarının karşılanması için uluslararası işbirliği yapılmasını kapsayan "Bilgisayar Olay Müdahale Ekipleri Programı" (Computer Incident Response Teams Programme-CIRT),
c) Siber güvenlik analizlerinin yer aldığı "Küresel Siber Güvenlik Endeksi" (Global Cybersecurity Index-GCI),
d) Yıllık panel, toplantı, kongre gibi etkinlikleri kapsayan "Siber Etkinlikleri" (Cyber Drills),
e) Artan siber tehditlere yönelik öngörüler belirlemeyi, üye ülkelerin önlem almasını ve kriz yönetim mekanizmalarının oluşturulmasını amaçlayan "Siber Tehdit Öngörüleri" (Cyber threat Insights) ve
f) Önemli bir tehdit haline gelen spamla mücadele konusunda üye ülkeler nezdinde girişimlerde bulunulmak, uyarılar ve önleyici mekanizmalar önermek maksadıyla oluşturulan "Spam'la Mücadele" (Combatting SPAM) olmak üzere altı stratejik plandan meydana gelmektedir (ITU, 2020b).

Avrupa Birliği'nde (AB) de siber güvenliğe yönelik önemli faaliyetler bulunmaktadır. Avrupa Birliği bünyesinde, siber güvenlik için AB Siber Güvenlik Ajansı (EU Agency for Cyber Security-*ENISA*) oluşturulmuş ve üye ülkelerde ve Birlik'in dijital ürünleri, hizmetleri ve süreç gibi faaliyetlerinde siber güvenlik sağlanması çalışmalarının koordinasyonun yapılması hedeflenmiştir. ENISA ayrıca, AB düzeyinde operasyonel işbirliğini artırmak, siber güvenlik olaylarını ele almasını talep eden AB Üye Devletleri'ne yardım etmek ve büyük ölçekli sınır ötesi siber saldırılar ve krizler durumunda AB'nin koordinasyonunu desteklemekle görevlendirilmiştir. Bu görev ENISA'nın ulusal sekretarya rolü üzerine kuruludur (Avrupa Birliği, 2020).

ENISA dışında EU Cybersecurity Act (AB Siber Güvenlik Antlaşması) hazırlanmıştır. Bu antlaşmayla ENISA'nın etkinliği artırılmıştır. Bu antlaşmayla ENISA, kalıcı bir yetki, daha fazla kaynak ve yeni görevlere sahip olmuştur. ENISA, özel sertifika programları için teknik zemine kavuşmuş, bu programların kamuoyuna duyurulması için internet sitesi hazırlanmıştır. Bu sayede Avrupa Siber Güvenlik Sertifikası çerçevesinin oluşturulmasında ve sürdürülmesinde ENISA kilit bir rolü üstlenmiştir (Avrupa Birliği, 2020).

Bu açıklamalardan da anlaşılabileceği üzere, Birleşmiş Milletler, NATO ve Avrupa Birliği'nde siber güvenlik konusuna büyük önem verildiği, siber güvenlik konusunda üye ülkelerde farkındalığı artırmak ve kuruluşların siber güvenlik faaliyetlerini koordine etmek amacıyla, ayrı birimler oluşturma yoluna gidildiği görülmektedir.

Türkiye'de Siber Savunma

Tüm dünyada meydana gelen gelişmeler, Türkiye'de de önemli ölçüde yaşanmakta, teknolojik gelişmelere paralel siber güvenlik sorunlarında da artış yaşanmaktadır. Yapılan araştırmalar, Türkiye'de önemli oranda zararlı yazılım bulunduğunu ortaya koymaktadır. Yine, Türkiye 25 milyon siber saldırı ile ABD ve Brezilya'nın ardından en fazla siber saldırıya uğrayan 3. ülke konumundadır (Siber Bülten, 2018). Bu durum ülkedeki siber güvenlik sorununun çok önemli bir boyutta olduğunu ortaya koymaktadır.

Teknoloji ve haberleşme olanaklarının bütün dünyayla birlikte Türkiye'de de hızlı bir şekilde gelişmesi, siber güvenlikle ilgili yasal metinlerin düzenlenmesi ve siber savunma alanında yeni önlemlerin alınmasını gerektirmektedir. Bu noktada öncelikle yasal metinlerin belirtilmesinde fayda görülmektedir. Türkiye'de siber alanla ilgili yasal metinler aşağıda sıralanmaktadır:

- ✓ 2813 sayılı Bilgi Teknolojileri ve İletişim Kurumumun Kuruluşuna İlişkin Kanun
- ✓ 5809 Sayılı Elektronik Haberleşme Kanunu
- ✓ 5070 Sayılı Elektronik İmza Kanunu
- ✓ 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- ✓ 6475 sayılı Posta Hizmetleri Kanunu655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname
- ✓ 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
- ✓ 6362 sayılı Sermaye Piyasası Kanunu 115. Madde
- ✓ 5271 sayılı Ceza Muhakemesi Kanunu 5. Bölüm
- ✓ 6102 sayılı Türk Ticaret Kanunu'nun 1525 inci maddesi

Türkiye'de siber suçlara yönelik de bazı düzenlemeler gerçekleştirilmiştir. Buna göre bilişim suçları Türk Ceza Kanununda (5237) (Md.243-245) aşağıdaki şekilde düzenlenmiştir:

- ✓ Bilişim sistemine girme suçu (TCK m.243),
- ✓ Sistemi engelleme, bozma, erişilmez kılma, verileri yok etme veya değiştirme suçu (TCK m.244),
- ✓ Banka veya kredi kartının kötüye kullanılması suçu (TCK m.245),
- ✓ Yasak cihaz veya program kullanma suçu (TCK m.245/a).

İdare yukarıda belirtilen kanunlarla siber suçlarla etkin mücadele etmeyi amaçlasa de mevzuatta ve uygulamada bir takım sıkıntılar olduğu aşikardır. Uluslararası yaptırım ve koordiansyon eksikliği, ulusal yasalardaki eksiklikler, kolluk kuvvetlerinin uygulamada karşılaştığı sorunlar bunlara örnek verilebilir (Çakmakkaya ve Akpınar, 2018). Fakat bu sorunlar sadece Türkiye'ye özgü değildir. Örneğin, Akdemir vd.'nin (2020) Birleşik Krallık siber suçlar kolluğunun sorunları üzerine yapmış olduğu nitel çalışma Çakmakkaya ve Akpınar (2018)'in belirtmiş olduğu Türkiye'deki siber suçlarla mücadelede karşılaşılan sorunlarla benzerlikler göstermektedir. Bu da bize siber suçların ve siber güvenliğin yerel bir sorun olmadığını, küresel bir sorun olduğunu göstermektedir.

Türkiye'de resmi olarak siber savunma konusunda politikaları belirlemek üzere, TÜBİTAK UEKAE'nın koordinatörlüğünde çeşitli kamu kurum ve kuruluşlarının temsilcileriyle oluşturulan bir çalışma grubu teşkil edilmiş ve bu grup faaliyetlerini 30 Ocak 2009'da tamamlayarak "Ulusal Sanal Ortam Güvenlik Politikası"nı hazırlamıştır (Ünver, Canbay ve Mirzaoğlu, 2009: 25).
Yine yakın dönemde 2017'de ilgili kamu kurumları, özel sektör ve akademisyenlerin katılımıyla, Savunma Sanayi Başkanlığı tarafından desteklenen ve SSTEK-Savunma Sanayi Teknolojileri A.Ş. tarafından yürütülmekte olan, Türkiye Siber Güvenlik Kümelenmesi önemli bir projedir.

Bu projeyle aşağıdaki hususlar hedeflenmektedir (Siber Küme, 2020):

- ✓ Türkiye'deki siber güvenlik firmalarının sayısını artırmak,
- ✓ Üyelerinin teknik, idari ve finansal açılardan gelişimine destek olmak,
- ✓ Siber güvenlik ekosisteminin standartlarını geliştirmek,
- ✓ Üyelerinin ürün ve hizmetlerinin markalaşmasına yardımcı olmak,

- ✓ Üyelerinin ulusal ve küresel pazarda rekabet gücünü artırmak,
- ✓ Siber güvenlik alanındaki insan kaynağı sayısını artırmak, niteliklerini geliştirmek,
- ✓ Bütün toplumda siber güvenlik bilincini geliştirmek.

Bu projenin tamamlanması ülkedeki siber güvenlik faaliyetlerinin koordinasyonu ve halkın bilinçlendirilmesi ülkenin siber dünyada ivme kat edebilmesi açısından verimli sonuçlar doğuracaktır.

20/10/2012 tarihli ve 28447 sayılı Resmi Gazete'de "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Bakanlar Kurulu Kararı (BKK)" ve 5809 sayılı Elektronik Haberleşme Kanunu ile ulusal siber güvenliğin sağlanmasına ilişkin politika, strateji ve elem planlarının hazırlanması ve koordinasyon görevi, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın sorumluluğuna verilmiş, yine aynı kanunla Türkiye'de bir "Siber Güvenlik Kurulu" teşkil edilmiştir. Kurulda, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı" ile birlikte Dışişleri, İçişleri Milli Savunma Bakanlıkları, Kamu Güvenliği Müsteşarlığı, Milli İstihbarat Teşkilatı, Genelkurmay Başkanlığı, Bilgi Teknolojileri ve İletişim Kurumu, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK), Mali Suçları Araştırma Kurulu ve Telekomünikasyon İletişim Başkanlığı yer almıştır (Terzi, 2018: 93-94). İlerleyen dönemde Cumhurbaşkanlığı sistemi ile meydana gelen değişimle birlikte, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında 9 Temmuz 2018 tarihli Resmi Gazete'de yayımlanan 703 No'lu Kanun Hükmünde Kararname ile "Ulaştırma ve Altyapı Bakanlığı" adını almıştır.

Yine Bakanlar Kurulunca alınan Ulusal Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Karar ve 5809 sayılı Elektronik Haberleşme Kanunu'na eklenen maddeler çerçevesinde Bilgi Teknolojileri ve İletişim Kurumu siber güvenlik ile ilgili faaliyetleri yürütmeye başlamıştır. Bu kurum Siber Güvenlik Kurulu'nda da yer almakta aynı zamanda Tablo-3'de belirtilen faaliyetleri yerine getirmektedir (BTK, 2020).

Bu çalışmalar, Türkiye'nin siber güvenlik konusunda önemli mesafe kat etiğini göstermektedir. Bununla birlikte ülkedeki en önemli sorunlardan bir tanesi alanda yetişmiş personel eksikliğidir. Kurum ve kuruluşlar siber güvenlik alanına ciddi yatırım yapmakta, bu alandaki önlemler almaktadır.

Bununla birlikte, alandaki açığıdoldurabilecek yeterlilikte personel bulmakta zorluk çekilmektedir. Bu sıkıntı peronel ücretlerinin yükselmesine rağmen çözülebilmiş değildir. Bu amaçla alternatif çözümler bulunmalıdır.

Siber alanda meydana gelebilecek risklere karşı eylem planları hazırlanmalı, bu alanda bir "siber risk sigortası" benzeri bir sistem geliştirilerek meydana gerebilecek kayıplara yönelik bir eskiye dönüş imkanı sağlanmalıdır (Terzi, 2019:240).

Tablo 3:
Bilgi Teknolojileri ve İletişim Kurumunun Siber Güvenlik Faaliyetleri

Faaliyet	Eylemler
Siber Güvenlik Stratejisi ve Eylem Planı	Siber Güvenlik Kurulunun oluşturulasını müteakip, ülkemizin mevcut durumu ve dünya örnekleri de incelenerek Ulusal Siber Güvenlik Stratejisi ve Eylem Planları oluşturulmuştur. İlk olarak 2013'te Ulusal Güvenlik Stratejisi ve 2013-2014 Eylem Planı hazırlanmıştır.
Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Sektörel Siber Olaylara Müdahale Ekibi (Sektörel SOME)	Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı çerçevesinde siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması amacıyla, USOM ve Sektörel SOME kurulmuştur.
Siber Güvenlik İnisiyatifi	Sektör Paydaşlarının katılım sağladığı ve hedefi siber güvenlik alanında çalışmalar yapmak, sektör paydaşlarını toplayarak fikir alışverişi sağlayarak sonuçları Bakanlığa sunmak amaçlı, İnternet Geliştirme Kurulu çatısı altında kurulmuştur.
Siber Güvenlik Tatbikatları ve farkındalık çalışmaları	Siber güvenlikte farkındalığı artırabilmek amacıyla meydana gelebilecek sorunlara ilişkin siber güvenlik tatbikatları ve farkındalık çalışmaları gerçekleştirilmektedir.

Kaynak: BTK, 2020

METODOLOJİ

Analiz Yöntemi

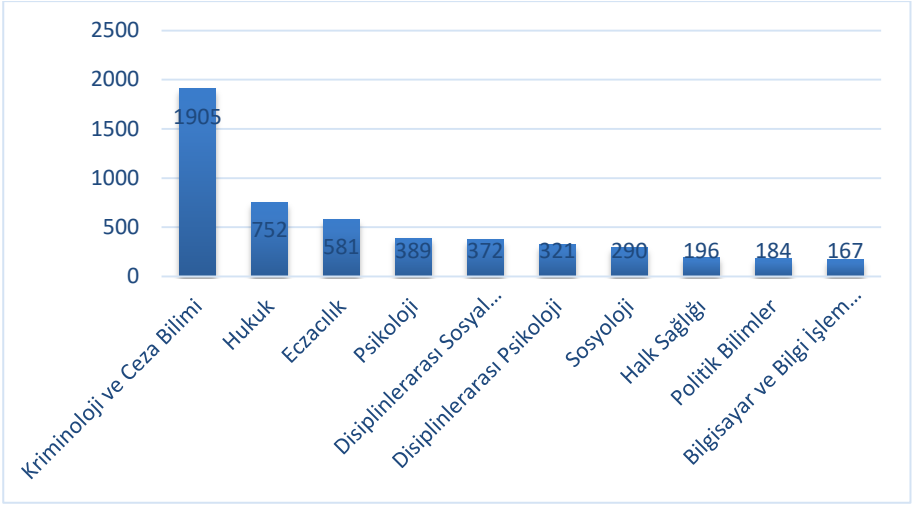
"Case Study"nin karşılığı olarak kullanılan vaka incelemesi konusunda yazında farklı adlar kullanılmaktadır. Bunlar arasında olay incelemesi, örnek olay çalışması, örnek olay inceleme yöntemi, vaka ya da durum çalışması gibi isimler yer almaktadır (Aytaçlı, 2012:2). Bu çalışmada vaka incelemesi kavramı kullanılmıştır.

Vaka incelemesi, ilgili bir belgenin tarihini ve kapsamlı analizini içeren bir araştırma yöntemidir. Vaka incelemesi metodolojisinin ayırt edici yönü, gözlemlenen durumdaki benzersiz özellikleri ve ilginç farklılıkları ortaya çıkarmayı amaçlamasıdır (Sammut-Bonnici ve Mc Gee, 2014). Bu amaçla vaka incelemesi çalışmalarında incelenen vaka ile ilgili olarak kapsamlı analizler gerçekleştirilir ve dikkat çeken özellikleri vurgulanır.

Genel olarak vaka çalışmaları; "nasıl" veya "neden" sorularının sorulduğu, araştırmacının olaylar üzerinde çok az kontrolü olduğu ve odağın gerçek yaşam bağlamında çağdaş bir fenomen olduğu durumlarda tercih edilen bir yöntemdir (Yin, 2003: 1). Bu yöntemde araştırma konusu üzerinde nasıl ve neden sorularına cevaplar aranarak bir derinlemesine analiz yapılması söz konusudur.

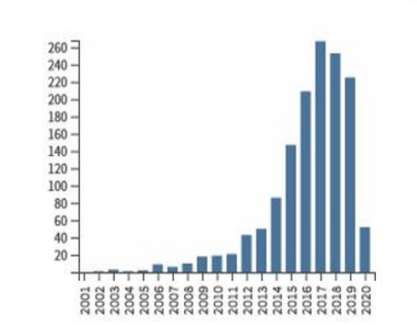
Vaka çalışmaları, "betimsel, bulgusal, eleştirel, program uygulaması, program etkileri, olasılıksal, bütünsel, öyküsel, tıbbi ve gömülü" olmak üzere farklı biçimlerde gerçekleştirilmektedir (University of Florida, 2020). Sosyal bilimlerde sıklıkla, betimsel, bulgusal, eleştirel, bütünsel ve öyküsel vaka çalışmaları kullanılmaktadır.

Kriminoloji gibi sosyoloji araştırmalarında yaygın olarak kullanılan vaka analizi yöntemi (Geis, 1991; Heap ve Waters, 2019) siber suç ve siber güvenlik çalışmalarında da sıklıkla kullanılmaya başlanmıştır. Web of Science veri bankası üzerinde SCI, SCI-Expanded ve SSCI gibi uluslararası endekslerde yayınlanmış makaleler üzerinde yaptığımız çalışma bu önermemizi desteklemektedir. Anılan endekslerde taranan makalelerden 6.521 tanesi Vaka analizi yöntemini kullanmışken, bunların 1.905 tanesi kriminoloji ve ceza bilimi, 372 tanesi disiplinler arası sosyal bilimler ve 290 tanesi de sosyoloji alanında yayınlanmıştır. Web of science veri bankası üzerinde yapmış olduğumuz bu analize ilişkin grafikler Şekil 5,6 ve 7'de sunulmuştur.

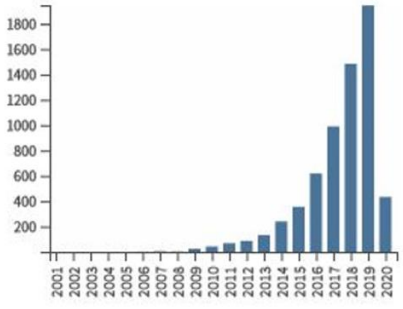


Şekil-5: Vaka Analizlerinin Kullanıldığı Disiplinler

Siber suçlar, siber güvenlik ve siber savaş konularında vaka analizi yöntemi kullanan ve anılan indekslerde taranan 1.422 makale tespit edilmiştir. Bu makalelerin yayın yılları ve atıf sayıları incelendiğinde Vaka analizine duyulan ilgi görülmektedir.



Şekil-6: Yayın Sayıları



Şekil-7: Atıf Sayıları

Analitik Strateji

Örneklem Yöntemi ve Veri

Araştırmamızda örneklem yöntemi olarak amaçlı örneklem kullanılmıştır. Amaçlı örnekleme, araştırmacının amaçları doğrultusunda zengin içeriğe

sahip olayları seçmesi gerektiğinde en uygun yöntemdir (Gerrish ve Lacey, 2010). Patton'a (2002) göre bu metot bir konu hakkında derinlemesine bilgi elde etmenin en etkili yollarından birisidir. 1900-2020 yılları arasında meydan siber savaş olayları internet sayfaları ve veri bankaları aracılığı ile taranmıştır. Elde edilen veriler NVIVO nitel analiz programına aktarılmıştır. Amaçlı örnekleme (*purposive sampling*) yöntemi ile tespit edilen 25 önemli siber saldırı ve siber savaş olayı[4] arasından bilgi yoğun 9 vaka seçilmiştir.

Analiz Süreci

Seçilen vakalar yinelemeli veri analizini içeren bir süreçte iki yazar tarafından ayrı ayrı temalandırılmıştır. Yinelemeli veri analizi genellikle araştırmacı yanlılığını önlemek için temel bir yöntem olarak kabul edilir (Creswell vd., 2003). Bunun nedeni ise her yazarın bakış açısının veri analizi sürecine yansıtılmasıdır. İki yazar tarafından oluşturulan temalar tekrar bir araya getirilmiş ve nihai halini almak üzere düzenlemeler yapılmıştır.

VAKA ANALİZİ

Siber Savaş Güncesi

Bu bölümde siber savaşların tarihsel evrimi, vaka analizi yöntemi ile incelenecektir. Vaka analizi maksadıyla seçilen örnek olaylara ait gazete habeleri, veri güvenliği raporları, söyleşi ve anılan dönemlere ait hatıra kitaplarından oluşan veri NVIVO nitel analiz programı vasıtasıyla incelenmiştir. Yapılan tematik analiz sonucunda vakalar, *İkinci Dünya Savaşı*, *Soğuk Savaş*, *Milenyum* dönemleri olmak üzere üç evrede temalandırılmıştır (Şekil-8). Internet teknolojileri 1990'lı yıllardan itibaren iş ve özel hayatımızda artan bir sıklıkla kendine yer bulmaya başlamıştır. 1991-2000 yılları arasında önemli siber saldırı olayları meydana gelmediği için son evre 2000'li yıllardan başlatılmıştır.

İkinci Dünya Savaşı Evresi

Bu dönemde meydana gelen ilk siber saldırılar olarak nitelendirebileceğimiz iki olay mevcuttur. Bunlardan birincisi Alan Turing ve Gordon Welchman tarafından geliştirilen BOMBE isimli elekro-manyetik makinenin Almanların Enigma kodlarının kırılmasında kullanılması olayıdır. Nazi Almanyası İkinci Dünya savaşı sırasında şifreli haberleşmesinde rotor mekanizmaları aracılığı ile olasılık üreten Enigma elekro-manyetik sistemini kullanıyordu (Wright, 2017). Bilgisayar biliminin de kurucularından sayılan İngiliz matematikçi Turing Bombe adını verdiği şifre kırıcıyı tasarladı, daha sonra dönemin ünlü kod kırıcısı Welchman bu tasarımda değişiklikler

[4] Tespit edilen saldırılara ait çizelge EK-A'da sunulmuştur.

yaparak kod kırma aşamalarını en aza indirgedi (Deavours ve Kruh, 1990). BOMBE, Almanların şifreli haberleşmelerini deşifre ederek müttefiklere önemli stratejik üstünlük sağlamıştır

İkincisi ise ilk etik korsan olarak tarihe geçen Rene Carmille'nin Nazi Almanya'sının Fransa işgali esnasında delikli-kart makinelerinin Yahudilerin kişisel verilerini takip etmede kullanılmasını engellemesi olaydır. Rene Carmille delikli-kart bilgisayarı uzmanı ve Nazi işgali altındaki Fransa'daki direniş grubunun mensubuydu. Fransa'daki Vichy yönetiminin bilgi işleme amacıyla kullandıkları bilgisayarlara sahip olan Carmille, Nazilerin delikli-kart makinelerini Yahudilerin takibi için kullandıklarını tespit ettikten sonra, makinelere bürokratik anahtarlar ekleyerek bu makineleri sabote etmiştir. Böylece pek çok insanın hayatını kurtarmıştır (Wills, 2017).

1960'lı yıllarda Amerikan hükümeti adına çalışan bilim insanlarının kendi aralarında haberleşmelerini sağlamak amacıyla kurulan internet, 1990'lı yıllara gelindiğinde yaygınlaşmaya başlamıştır (Campbell-Kelly, Garcia-Swartz, 2013). Bu nedenle ikinci dünya savaşı döneminde bildiğimiz manada ağlar üzerinden bilgisayar sistemlerine yapılan bir saldırıdan söz etmek mümkün değildir. Ancak örnek olaylar teknolojik imkânlar vasıtasıyla düşmanların kullandıkları cihazları etkilemenin mümkün olduğunu ve böylelikle düşman ülkelere stratejik avantajlar sağlamanın mümkün olduğunu göstermektedir. Burada örneklendirilen iki olay siber saldırı ve siber savaşların başlangıç noktasının karşı tarafın hassasiyetlerini istismar etmek üzerine kurulduğunu da bizlere göstermektedir.

Soğuk Savaş Evresi

Batı Blok'u ülkeleri ve Doğu Blok'u ülkeleri arasında 1947-91 yılları arasında cereyan eden Soğuk Savaş dönemi, İkinci Dünya Savaşı'nın acı tecrübeleri karşısında yeni bir konvansiyonel savaşa girmeyi göze alamayan ülkelerin arasındaki savaş dışı unsurlarla güç ve psikolojik üstünlüğün kabul ettirilmeye çalışıldığı bir dönemdir. Bu dönemin karakteristiğini yansıtan ve gerçek manada siber savaşın başlangıcı olarak da kabul edebileceğimiz olay, 1982 yılında Rusya'ya ait Sibirya doğalgaz boru hattına Amerikan Merkezi İstihbarat Teşkilatı (CIA) tarafından gerçekleştirildiği iddia edilen saldırıdır (Russel, 2004). Sibirya doğalgaz boru hattı saldırısı Rus ajanlarının onu çaldığına inandırıldıkları bir yazılımın içine gizlenen Truva Atı aracılığı ile gerçekleştirilmiştir (Wired, 2004). Bu saldırıda kullanılan Truva atı yazılımı boru hattı bağlantıları ve kaynakları için standart basınç seviyesinin üzerinde basınç elde etmek için pompa hızları ve valf ayarlarının değiştirilmesinde kullanılmıştır (Safire, 2004).

Detaylarına Amerikan Hava Kuvvetleri eski sekreteri ve Başkan Reagan'ın danışmanı Thomas Reed'in Soğuk Savaş dönemini anlatan "Uçurumun Kenarında: İçeriden Birinin Gözünden Soğuk Savaş Tarihi" (*At the Abyss: An Insider's History of the Cold War*) adlı kitabından ulaşılan bu saldırı sonucunda herhangi bir can kaybı yaşanmamış ancak Batı Blokunun psikolojik üstünlük elde etmesine katkıda bulunmuştur.

Milenyum Evresi

Analizin bu bölümüne 2000-2010 yılları arasında meydana gelen önemli siber savaş maksatlı siber saldırılar dâhil edilmiştir. Daha önce Metodoloji bölümünde de belirttiğimiz gibi, internet teknolojilerinde meydana gelen değişimler, yeni saldırı türlerinin ortaya çıkışı ile paralel olarak bu dönemde çok sayıda siber saldırı meydana gelmiştir. Bunlardan önemli etkileri olan ve zengin içeriğe sahip altı vaka seçilmiştir. NVIVO nitel analiz programında yaptığımız tematik analiz neticesinde vakalar *bir devletin bir başka devlete siber saldırısı* ve *devlet dışı unsurların bir devlete siber saldırısı* olarak temalandırılmıştır. Vakalar bu temalara uygun olarak tartışılacaktır.

Bir Devletin Bir Başka Devlete Siber Saldırısı: Önceki bölümlerde de ifade ettiğimiz gibi günümüz uluslararası ilişkiler konjonktüründe devletlerin konvansiyonel silahlar kullanarak birbirlerine iradelerini kabul ettirmeleri pek mümkün değildir. Bu nedenle açıkça veya gizli olarak gerçekleştirilen siber savaş yöntemleri devletlerin çıkarlarını temin etme ve karşı tarafın milli güç unsurlarını zayıflatmak/etkisiz hale getirmek için önemli araçlar haline gelmiştir.

2007 yılı içerisinde Estonya devlet kurumları ve bankacılık sektörü başta olmak üzere özel işletmelere yönelik zombi bilgisayarlar vasıtasıyla DDos saldırıları yapılmıştır. Özellikle bankacılık ve lojistik sektörü hedef alan saldırılar Estonya'da hayati hizmetlerin aksamasına, maddi zararın oluşmasına ve prestik kaybına neden olmuştur (NATO Siber Operasyonlar Raporu, 2017). Bu saldırıların Tallinn'de bulunan Sovyet dönemine ait bir anıtın yer değiştirmesinden kaynaklı Rusya ile Estonya arasındaki siyasi gerilim esnasında gerçekleşmesi, siber saldırıların Rus hükümeti tarafından desteklendiği iddialarını güçlendirmiştir (Ottis, 2008; Estonian World, 2013).

Ukrayna kaynaklı çevrimiçi devlet sitelerinin yanı sıra finans ve enerji şirketlerine ait sitelere 2017 yılında NotPetya fidye yazılımı ile yapılan saldırılar yaklaşık olarak 300 milyon dolarlık bir zarara neden olmuştur (Wired, 2018). CIA bu saldırının Rus askeri siber savaş birimlerince yapıldığını öne sürmüştür (Nakashima, 2018). Olumsuz sonuçlarının diğer

ülkelere yansıması ve tehdidin uluslararası bir sorun haline gelmesi bu saldırıyı daha önceki saldırılardan farklı kılan unsurlardan birisidir (Cnet, 2020).

Şekil-8: Siber Savaş Güncesi (Şekildeki görseller sırasıyla Mauro Sbicego, Danil Sorokin ve Markus Spiske' ait olup, Unsplash'den alınan izin ile şekle aktarılmıştır.)

Devletlerin siber saldırıyı sınırları belli nihai bir hedefe ulaşmak için kullandıkları bir başka örnek ise İran'daki nükleer santrale yapılan Stuxnet veya Olimpik Oyunlar olarak bilinen saldırıdır. Saldırının kaynağı hakkında kesin bir bilgi sahibi olunmasa da, saldırıyı İran ile politik anlaşmazlıklar içerisinde bulunan ABD veya İsrail tarafından gerçekleştirildiği öne sürülmektedir (Rosenbaum, 2012; CSO, 2017). Her ne kadar saldırı 2010

yılında gerçekleşmiş olsa da, bu eylem aslında 2006 yılında başlayan bir siber saldırı programının son halkasıydı. İran'ın uranyum zenginleştirme programını sekteye uğratmak maksadıyla denetim kontrol ve veri toplama (SCADA) sistemleri Haziran ve Temmuz aylarında gerçekleşen iki ayrı saldırı ile hedef alınmıştı. Harici bellek ile sisteme nüfuz eden bilgisayar solucanı, SCADA sistemlerini denetleyen Siemen Step 7 yazılımını hedef almıştır (Kushner, 2013). Bu zararlı yazılım bir yandan bilgisayar kontrollü elektro-mekanik ekipmana hasar verecek komutlar yollarken, diğer yandan ana kontrol ünitelerine sahte geri beslemeler göndermiştir (McAfee, 2020). Bu saldırının santralde bulunan 948 uranyum zenginleştirme santrifüjüne zarar verdiği tahmin edilmektedir (Holloway, 2015). Bu ise İran'ın uranyum zenginleştirme gayretlerini sekteye uğratmış, ABD ve müttefiklerinin elde etmek istedikleri sınırları belirli milli hedefe ulaşma imkânı sağlamıştır.

Stuxnet saldırısı daha önce incelediğimiz Estonya saldırısından farklı olarak, bilgisayar sistemlerine harici bir donanım ile nüfuz etmiştir. Sistem bileşenlerindeki hassasiyetleri istismar ederek cihazların uzaktan kontrol edilebileceğini, kritik alt yapı ve tesislere bu yolla fiziksel zararlar verilebileceğini göstermiştir. Santralde görevli bir işçinin harici belleğinin enfekte edilmesiyle başlayan bu saldırı, bize insanların güvenlik hatalarının da bilgisayar sistemleri ve internet ağlarına ciddi hasarlar verilmesinde etkili olduğunu göstermiştir.

Rusya ve Gürcistan arasında devam eden savaş esnasında 2008 yılında Gürcistan'a yapılan siber saldırılar ise, siber savaşın başka bir boyutunu ortaya koymaktadır. Gürcistan'daki farklı sektörleri hedef alan siber saldırılar Estonya saldırısı benzeri ekonomik ve sosyal açıdan yıkıcı sonuçlar vermiştir (BBC, 2020). Şu ana kadar incelediğimiz örneklerde siber saldırılar/siber savaş milli bir hedefe ulaşmak için tek başına kullanılan bir araç iken Gürcistan saldırıları siber savaşın konvansiyonel savaşı destekleme aracı olarak da etkili olabileceğini ortaya koymuştur (Hollis, 2008).

Devlet Dışı Unsurların Bir Devlete Siber Saldırısı:

Siber savaş sadece devletlerin mahdut hedefli saldırılarla karşı tarafa kendi iradesini kabul ettirmek veya sosyo-ekonomik zararlar vermek amacıyla değil aynı zamanda kişi veya grupların da bir egemen devlete veya yönetime saldırısı şeklinde olabilmektedir. 2010 yılında gerçekleşen Myanmar siber saldırıları buna güzel bir örnek teşkil etmektedir. Yirmi yıllık aradan sonra ilk defa gerçekleşecek seçim öncesi Myanmar internet ağı DDos saldırılarının hedefi olmuştur (BBC, 2010). Bu saldırılarla seçim öncesi ve esnasında bilgi akışı engellenmeye çalışılmıştır. Bu saldırıları seçimleri

manipüle etmek isteyen muhalif grupların gerçekleştirdiği iddia edilmiştir (NBC News, 2010).

Anonymous adlı internet korsan grubu tarafından başlatılan ve her yıl tekrarlanan OpIsrael DDos saldırıları İsrail'in Gazze bölgesindeki uygulamalarını protesto etmek maksadıyla 2013 yılında başlamıştır (Hürriyet, 2013; Anadolu Ajansı, 2017). Bu siber saldırılarda sadece hükümete ait web siteleri servis dışı bırakılmamış, pek çok web sitesinin kontrolü ele alınarak bu sitelere Filistin'i destekleyici mesajlar bırakılmıştır (Haaretz, 2019).

Myanmar ve İsrail örnekleri, siber saldırıların devletlerin ve meşru yönetimlerin çevrimiçi faaliyetlerinin devlet dışı unsurlarca da sekteye uğratılabileceğini göstermektedir. Özellikle İsrail örneği etik korsan olarak adlandırılan unsurların gelecekte bir güç merkezi haline gelebileceğini veya bu ve benzeri yapılanmaların lejyoner asker mantığı ile egemen devletler veya çıkar gruplarınca kiralanarak siber savaşlarda kullanılabilecekleri fikrini güçlendirmektedir.

TARTIŞMA

İnternet teknolojilerinin hayatımızın her alanına nüfuz etmesiyle siber suç, siber saldırılar ve siber savaş gibi kavramlar günlük hayatımızın bir parçası haline gelmiştir. Siber uzayın olumsuz yansımaları olan bu kavramlar sadece bireyler için devletler ve organizasyonlar için de ciddi tehditler arz etmektedir. Bu çalışmamızda vaka analizi ve tematik analiz yöntemleri kullanılarak siber savaşın tarihsel evrimi analitik bir yaklaşımla incelenmiştir. Amaçlı örnekleme (purposive sampling) yöntemiyle seçilen bilgi yoğun olaylar NVIVO nitel analiz programı aracılığı ile analiz edilmiştir. Analizimiz sonucunda siber savaşların İkinci Dünya Savaşı, Soğuk Savaş ve Milenyum olmak üzere üç farklı evreden geçtiği tespit edilmiştir. Tartışmamızın ilk bölümünde bu üç evrenin özellikleri karşılaştırılacaktır. İkinci bölümde ise her bir evrede ele alınan vakalardan alınan dersler tartışılacaktır.

Dönemsel Özellikler

İkinci Dünya Savaşı sayısız yıkıcı sonuçlarına rağmen, devletlerin savaş esnasında birbirlerine taktik ve stratejik üstünlük elde etme çabalarında teknolojiyi bir kuvvet çarpanı olarak kullanmaları savaş esnasında ve savaş sonrası dönemde önemli teknolojik yeniliklerin yapılmasına ve yeni fikirlerin ortaya çıkmasına neden olmuştur. Bu bağlamda, siber savaşın başlangıcı olarak bu dönemi inceleme ihtiyacı doğmuştur. İncelememiz bu

dönemde meydana gelen iki olayın; (1) Enigma cihazı tarafından oluşturulan şifrelerin Turing ve Welchman tarafından geliştirilen BOMBE cihazıyla kırılması, (2) Rene Carmille'nin Nazilerin kişisel verileri takip ettiği sisteme müdahalede bulunarak süreci sabote etmesi başka sistemlere nüfuz etmeyi hedefleyen korsanlık (hacking) olayının ilk örnekleri olabileceğini göstermiştir. Bu iki olay siber savaşın sadece ağlarla birbirine bağlı sistemlere yapılan çevirimiçi sadırılardan ibaret olmadığını, gerçek dünyadaki bilgi işleme ve depolama özelliği olan kritik hedef ve altyapılara yapılan çevirimdışı sabotaj olaylarını da kapsadığını öne süren siber savaş kavramının geniş tanımı kapsamında siber savaş/siber saldırı değerlendirilimiştir (Gervais, 2011; Lucas, 2017).

Henüz internet teknolojisinin var olmaması nedeniyle bu faaliyetler bir başka sisteme fiziksel sızma (Carmille örneği) ve başka bir sistemin ürettiği verileri değiştirme (Turing ve Welchman örneği) ile sınırlı kalmıştır.

Soğuk Savaş dönemi ise Batı ve Doğu Bloklarının olası bir nükleer savaşın yıkıcı sonuçlarından duyulan endişeden dolayı karşı tarafa siyasi iradesini teknolojik ve psikolojik üstünlük sağlama çabaları ile kabul ettirme olarak karakterize edilebilir. İnsan istihbaratı ve casusluk faaliyetlerinin yanı sıra teknolojik casusluk gayretlerinin yoğunlaşması da bu dönemin özelliklerinin doğal bir sonucudur. Rus istihbarat birimlerinin teknolojik casusluk çabalarını fark eden CIA, Rusların elde etmeyi arzuladıkları bir yazılıma Truva Atı gizlemiş ve böylece Sibirya doğal gaz boru hattında patlamaya neden olmuştur. Fiziksel bir hedefi bilgisayar yazılımı ile imha eden bu olay gerçek manada ilk siber saldırı olayıdır.

Milenyum evresi ise, internet ve programcılık teknolojilerinde meydana gelen değişime paralel olarak siber saldırıların arttığı bir dönemdir. Siber savaşın devletlerin ve organizasyonların güvenliği için ciddi bir tehdit unsuru haline gelmesi bu dönemin en önemli karakteristiğidir. Gelişen tehdit nedeniyle NATO siber uzayı dördüncü savaş boyutu olarak tanımlamış; Çin, Rusya ve ABD gibi süper güçler siber savaş orduları kurmaya başlamıştır. Ayrıca, ilk dönemlerde verilen zararlar sınırlı kalmakla birlikte, zararlı yazılım ve kriptografi teknolojilerinde meydana gelen gelişmeler, saldırılarda uğranılan zararların büyük boyutlara ulaşmasına neden olmuştur.

Alınan Dersler

Özellikle milenyum evresinde meydana gelen olaylar incelendiğinde, siber savaşlar sadece devletler arasında cereyan etmemiş, devlet dışı unsurlar da egemen devletleri ve meşru yönetimleri hedef almıştır. Bu durum siber saldırı ve siber savaş kavramlarının uluslararası hukuk kapsamında ele

alınması ve uğranılan maddi hasarın karşı taraftan tazmini gibi yaptırımların uygulanmasını gerektirmektedir. Fakat internet trafiğinin çeşitli programlar vasıtasıyla yönlendirilmesi ve yapılan saldırıların büyük çoğunluğunu zombi (Botnet) olarak adlandırılan dünyanın çeşitli bölgelerinde bulunan enfekte edilmiş bilgisayarlarca yapılması hukuksal yaptırım gayretlerini sekteye uğratacaktır.

Bu nedenle siber caydırıcılık ön plana çıkacaktır. Dijital bilgi ve teknolojik alt yapı üstünlüğüne sahip olan, sadece defansif siber güvenlik değil ofansif siber savaş kabiliyetine haiz ülkeler kendilerine yöneltilen tehditleri en az zararla atlatırken mütekabiliyet esasları dâhilinde hasım ülke ve organizasyonlara etkili yanıt verebilecektir. Bu kapsamda Dijital Dönüşüm Ofisi ve Bilgi Teknolojileri ve İletişim Kurumu (BTK), Siber Güvenlik Kümelenmesi gibi kurum ve kuruluşların dijital dönüşüm, eğitim ve teknolojik gelişim konularında ortaya koydukları inisiyatif Milenyum evresi ve müteakip evrelerde oluşacak tehditleri bertaraf etmede büyük önem taşımaktadır.

İnternet teknolojilerinin hayatımızın her boyutuna nüfuz etmiş olması ve elektronik cihazların birbirleri ile daha fazla bağlantılı olması, şirketlerin üretim, depolama ve satış gibi fonksiyonlarını giderek dijitalleştirmesi, ülke ekonomilerini ve gündelik hayatta sağlık, ulaştırma gibi hayati hizmetleri siber saldırılara karşı hassas konuma getirmiştir. Estonya ve Ukrayna saldırıları dijital bağlılığın bu sakıncalarını ortaya koymuştur. İki ülkede uğranılan maddi hasarlara ilave olarak temel hizmetler aksamış, günlük yaşam üzerine olumsuz etkiler göstermiştir.

Rus-Gürcü savaşı sırasında uygulanan yöntem, siber savaşın konvansiyonel savaş ile orkestra edilebileceğini ve önemli bir kuvvet çarpanı olabileceğini gözler önüne sermiştir. Siber savaş sadece savaş sistemlerinin devre dışı bırakılması ve askeri birlikler arasında koordinasyonu sekteye uğratmak kapsamında kullanılmamış, halk üzerinde psikolojik baskı kurularak, halkın savaşma azim ve iradesinin zayıflatılmasına katkıda bulunmuştur.

Stuxnet ve Sibirya doğal gaz boru saldırıları ise, fiziksel hedeflerin siber savaş vasıtaları ile imha edilebileceğini göstermiştir. Bu saldırılar, İnternet ağları vasıtasıyla yapılmamış, bilgisayar sistemlerine yapılan sızmalar ile sistemlerdeki hassasiyetler istismar edilmiştir. Bu iki saldırıyı diğerlerinden ayıran bir başka yönü ise insan unsurunun istismar edilmiş olmasıdır. Sibirya saldırısında istihbarat birimlerinin özensizliği ve bilgi eksikliği, İran saldırısında ise tesiste çalışan bir işçinin dikkatsizliği istismar edilmiştir. Stuxnet saldırısında hedef olan işçinin çevrimiçi alışkanlıkları takip edilmiş, sosyal mühendislik yöntemleri ile harici bellek enfekte edilmiştir. CIA

tarafından ayartılmış olma olasılığı da düşünülebilir. Ancak her iki senaryoda da alınması gereken ders, dijital öğe taşıyan harici bellek ve kişisel bilgisayar gibi dijital vasıtaların kritik tesis ve sistemlere bağlanmasının engellenmesidir. Böylece, siber güvenlik zincirnin en zayıf halkası olarak değerlendirilen insan unsurundan kaynaklanan riskleri en aza indirgemek mümkün olabilecektir. Bu husus çalışma protokollerinde belirtilmeli ve hassasiyetle takip edilmelidir.

Sonuç Yerine

Savaşlar insanlık tarihinin başlangıcından bu yana varlığını sürdürmüştür. Savaşlar yaşanılan acı gelişmeler, yıkımlar ve ölümlerle eş anlamlı kullanılmaktadır. Bununla birlikte savaşlar ve insanlar arası çıkar çatışmaları bir taraftan ağır sonuçları doğururken diğer taraftan da insanlığının teknolojik olarak gelişiminin de gerekçeleri arasında yer almaktadır.

Tarih içerisinde insanların birbirleriyle olan mücadelesi zaman geçtikçe topluluklar, sonraki aşamada da ülkeler arasında gerçekleşmiştir. Ülkeler arasındaki bu mücadele savaşın gelişimi ve değişimiyle doğru orantılı olarak farklı araçlarla sürdürülmektedir.

Çağımızın savaşları, geçmiş dönemlerdekinden oldukça farklı hale gelmiştir. Geçmişte yaşanan savaşlarda insanların güç mücadelesiyle başlayan süreç günümüzde teknoloji yarışı haline gelmiştir. Teknoloji ve ülkelerin sahip olduğu ekonomik güç savaşları da şekillendirmektedir.

İki ülkenin ordularının karşı karşıya geldiği klasik konvansiyonel savaşlar ortadan kalkmış orduların yanında pek çok farklı aktör savaş alanında yerini almıştır. Artık ülkelerin yerini zaman zaman farklı topluluklar, gruplar terör örgütleri almaktadır.

Bu yapılanma içerisinde savaşların teşkili de farklı cereyan etmektedir. Artık ülkeler, senelerce sürecek bir konvansiyonel savaşta verilebilecek zararı bir siber saldırı ile gerçekleştirebilmekte, düşmanın bütün teknolojik alt yapısını durdurarak işlemez hale getirebilmektedir. Aynı şekilde ekonomik araçlarla düşmanın savaşma azim ve kararlılığını bir kaç hamleyle çökertebilmektedir.

Bu konjonktürde siber güvenliğin önemi artmış, ülkeler bu alanda ciddi yatırımlar gerçekleştirmeye başlamıştır. Siber güvenlik alanında ülkelerin gerçekleştirdikleri faaliyetler yanında uluslararası organizasyonların bu alanda yürüttükleri faaliyetlerde de ciddi atılımlar göze çarpmaktadır.

Siber güvenlik alanında faaliyet gösteren kurum ve kuruluşların çalışmaları olumlu olmakla beraber bunlara verilen destek artırılmalıdır. Ayrıca, siber güvenlik alanında bir risk sigortası sistemine benzer bir yapı geliştirilerek, saldırı meydana geldiğinde zararların karşılanması ve eskiye dönüş imkanları araştırılmalıdır.

Kaynaklar

5237 Sayılı Türk Ceza Kanunu. (2020).

Akdemir, N., Sungur, B. ve Başaranel, B.U. (2020). Güvenlik Bilimleri Dergisi Özel Sayısı, 113-134. doi:10.28956/gbd.695956.

Authanvil. (2020). Secure Identity and Access Management.
https://authanvil.com/blog/3-types-of-password-security-attacks-and-how-to-avoid-them(adresinden 07/01/2020 tarihinde alındı).

Acunetix. (2020). What is SQL Injection (SQLi) and How to Prevent it.https://www.acunetix.com/websitesecurity/sql-injection/ (adresinden 02/01/2020 tarihinde alındı).

Anadolu Ajansı. (2017). Türk Hackerlardan İsrail'e Siber Saldırı. https://www.aa.com.tr/tr/dunya/turk-hackerlardan-israile-siber-saldiri/955178(adresinden 21/01/2020 tarihinde alındı).

Anley, C. (2002). Advanced SQL Injection in SQL Server Applications. NGSSoftware Insight Security Research (NISR) Publication.

Avrupa Birliği. (2020). https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act (adresinden 09/01/2020 tarihinde alındı).

Avrupa Komisyonu. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (adresinden 24/12/2019 tarihinde alındı).

Başaranel, B.U. (2017). Online Terrorist Financing. M.Conway, L. Jarvis, O. Lehane, S. Macdonal ve L. Nouri (Eds.) Terrorist's Use of the Internet: Assessment and Response, 136, 95-108. Amsterdam: IOS Press.

Başaranel, B.U. ve Türkşen, U. (2019). Counter-Terrorist Financing Law and Policy: An Analysis of Turkey. Routledge.

BBC. (2020). Burma hit by massive net attack ahead of election. https://www.bbc.com/news/technology-11693214. (adresinden 21/01/2020 tarihinde alındı).

BBC. (2020). UK says Russia's GRU behind massive Georgia cyber-attack. https://www.bbc.com/news/technology-51576445. (adresinden15/01/2020 tarihinde alındı).

BGA security. (2019). https://www.bgasecurity.com/2019/09/phishing-oltalama-saldirisi-nedir/. (adresinden 28/12/2019 tarihinde alındı).

BGA Security. (2020). https://www.bgasecurity.com/2011/11/dictionary-sozluk-saldrlar/. (adresinden 07/01/2020 tarihinde alındı).

BTK. (2020). https://www.btk.gov.tr/siber-guvenlik-kurulu. (adresinden 08/01/2020 tarihinde alındı).

Campbell-Kelly, M. ve Garcia-Swartz, D.D. (2013). The History of the Internet: The Missing Narratives. Journal of Information Technology. 28(1), 18-33.

Cisco. (2020). What are the most common cyber attacks.https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks. (adresinden 28/12/2019 tarihinde alındı).

Cloudflare. (2020a). What is a Denil-of-Service (Dos) Attack. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/. (adresinden 05/01/2020 tarihinde alındı).

Cloudflare. (2020b). What is DDos Attack. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. (adresinden 05/01/2020 tarihinde alındı).

Cloudflare. (2020c). What is IP Spoofing? https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/. (adresinden 04/01/2020 tarihinde alındı).

Cnet. (2020). US: Russia's NotPetya the most Destructive Cyberattack ever. https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/. (adresinden15/01/2020 tarihinde alındı).

Creswell, J. W., Plano Clark, V. L., Gutmann, M. L. ve Hanson, W. E. 2003. Advanced Mixed Methods Research Designs. TASHAKKORI, A. veTEDDLIE, C. (Eds.) Handbook of Mixed Methods in Social and Behavioral Research. Thousand Oaks, Calif.: SAGE Publications.

CSO. (2017). What is Stuxnet, Who Created it and How Does it Work?. https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html. (adresinden 21/01/2020 tarihinde alındı).

Çakmakkaya, B.Y. ve Akpınar, T. (2018). Bilişim Suçları ile Mücadelede Karşılaşılan Sorunlar. Balkan ve Yakın Doğu Sosyal Bilimler Dergisi, 04 (03), 123-29.

Çiftçi, H. (2017). Siber Savaşın Temelleri. H. Çiftçi, & H. ÇİFTÇİ (Dü.) içinde, Her Yönüyle Siber Savaş (s. 01-26). ANkara: TÜBİTAK.

Deavours, C.A. ve Kruh, L. (1990). The Turing Bombe: Was it Enough? Cryptologia, 14(4), 331-49.

DNS Stuff. (2020). https://www.dnsstuff.com/sql-injection. (adresinden 07/01/2020 tarihinde alındı).

Estonian World. (2013). Turning around the 2007 Cyber Attack: Lessons from Estonia. https://estonianworld.com/security/turning-around-2007-cyber-attack-lessons-estonia/.(adresinden 17/01/2020 tarihinde alındı).

Fruhlinger, J. CS Online. https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html. (adresinden 02/01/2020 tarihinde alındı).

Gervais, M.K. (2011). Cyber Attacks and the Laws of War. *Journal of Law Cyber Warfare, 1*(1), 525-79.

Guardian, D. (2019). https://digitalguardian.com/blog/what-cyber-security. (adresinden 28/12/2019 tarihinde alındı).

Güleryüz, İ. ve Dalkılıç, O.S. (2019). Kurumsal Sosyal Sorumluluk Projelerinin Kurumsal İtibar Üzerine Etkisini Belirlemeye Yönelik Bir Araştırma. International Social Sciences Studies Journal, 5 (33), 2089-98.doi: 10.26449/sssj.1425.

GERRISH, K. ve LACEY, A. (2010). The Research Process in Nursing, John Wiley and Sons.

Geis. (1991). The Case Study Method in Sociological Criminology. Feagin, J.R., Orum, A. ve Sjoberg, G. (Eds.) A Case for the Case Study,

Haaretz. (2019). Pro-Palestinian Hackers Breach 120 Israeli Websites. https://www.haaretz.com/israel-news/.premium-pro-palestinian-hackers-breach-120-israeli-websites-1.7084034. (adresinden 21/01/2020 tarihinde alındı).

Hajoary, P.K. ve Akhilesh, K.B. (2019). Role of Government in Tackling Cyber Security Threat. Smart Technologies, Springer, Singapur.

Herjavec, R. (2019). Herjavec: https://www.herjavecgroup.com/history-of-cybercrime/. (adresinden 24/12/2019 tarihinde alındı).

Heap, V. ve Water, J. (2019). Mixed Methods in Criminology. Routledge.

Herjavec, R. History of Cybercrime. Herjavec Group: https://www.herjavecgroup.com/history-of-cybercrime/. (adresinden 28/12/2019 tarihinde alındı).

Holloway, M. (2015). Stuxnet Worm Attack on Iranian Nuclear Facilities. http://large.stanford.edu/courses/2015/ph241/holloway1/.(adresinden 15/01/2020 tarihinde alındı).

Hürriyet. (2013). İsrail'deki İnternet Sitelerine Siber Saldırı. https://www.hurriyet.com.tr/teknoloji/israildeki-internet-sitelerine-siber-saldiri-40798112. (adresinden 21/01/2020 tarihinde alındı).

Imperva. (2020). https://www.imperva.com/learn/application-security/denial-of-service/. (adresinden 05/01/2020 tarihinde alındı).

ITU. (2020). https://www.itu.int/en/ITUT/studygroups/com17/Pages/cybersecurity.aspx. (adresinden 05/01/2020 tarihinde alındı).

ITU. (2020b). https://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx. (adresinden 09/01/2020 tarihinde alındı).

ITU İnternet Sitesi.
https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. (adresinden 20/12/2019 tarihinde alındı).

Kaspersky. (2020).
https://www.kaspersky.com/resource-center/definitions/replay-attack. (adresinden 04/01/2020 tarihinde alındı).

Kushner, D. (2013). The Real Story of Stuxnet. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.(adresinden15/01/2020 tarihinde alındı).

Lucas, G. R. (2017). Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. Oxford University Press.

Manageengine. (2020).
https://www.manageengine.com/log-management/cyber-security-attacks/what-is-brute-force-attack.html. (adresinden 07/01/2020 tarihinde alındı).

McAfee. (2020). What is Stuxnet? https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html.(adresinden15/01/2020 tarihinde alındı).

Melnick, J. (2018). https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Man-in-the-middle%20(MitM)%20attack. (adresinden 04/01/2020 tarihinde alındı).

Nakashima, E. (2018). Russian military was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes. The Washington Post.

https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html. (adresinden13/01/2020 tarihinde alındı).

NATO Siber Operasyonlar Raporu. (2017). 2007 Cyber Attacks on Estonia. https://www.stratcomcoe.org/download/file/fid/80772. (adresinden16/01/2020 tarihinde alındı).

NBC News. (2010). Cyber Attack Cripples Myanmar Days before Vote. http://www.nbcnews.com/id/40006682/ns/world_news-south_and_central_asia/t/cyber-attack-cripples-myanmar-days-vote/#.XpK9e5lS8uU. (adresinden 21/01/2020 tarihinde alındı).

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. 7th European Conference on Information Warfare Kongresi bildiriler kitabı içinde.

Paloaltonetworks. (2020). https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos. (adresinden 05/01/2020 tarihinde alındı):

Pamphlet, T. (2010). Cyberspace Operations Concept Capability Plan. https://fas.org/irp/doddir/army/pam525-7-8.pdf.(adresinden19/01/2020 tarihinde alındı).

Patton, M. (2002). Qualitative Research and Evaluation Methods. Thousand Oaks, Calif.: SAGE.

Russel, A. (2004). CIA Plot Led to Huge Blast in Siberian Gas Pipeline. The Telegraph. https://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html. (adresinden 04/02/2020 tarihinde alındı).

Rosenbaum, R. (2012). Richard Clarke on Who Was Behind the Stuxnet Attack. Smithsonian Magazine. https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/. (adresinden 22/01/2020 tarihinde alındı).

Safire, W. (2004). The Farewell Dossier. The New York Times. https://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html (adresinden 04/02/2020 tarihinde alındı)

Siber Bülten. (2018). https://siberbulten.com/sektorel/trky/turkiyeye-yapilan-siber-saldiri-sayisi-25-milyon/ (adresinden 10/01/2020 tarihinde alındı).

Siber Küme. (2020). https://siberkume.org.tr/hakkinda/ adresinden (adresinden 10/01/2020 tarihinde alındı).

Technopedia (2019). https://www.techopedia.com/definition/2493/cyberspace. (adresinden 18/12/2019 tarihinde alındı).

Terzi, M. (2018). Bilgi ve İletişim Teknolojilerine Dayalı Oluşumlar ile Bu Oluşumların Uluslar arası İlişkilere Güvenlik Bağlamındaki Etkisi:Siber Terörizm. Kara Harp Okulu Bilim Dergisi, 28 (1), 73-108.

Terzi, M. (2019). E-Government And Cyber Terrorism: Conceptual Framework, Theoretical Discussions And Possıble Solutions. Tesam Akademi, 6 (1), 213-247.

The White House. (2008). Memorandum For Recıpıents Of Nspd-54/HSPD-23.http://www.lloydthomas.org/5-SpecialStudies/nspd-54Jan08.pdf. (adresinden 18/12/2019 tarihinde alındı).

Turk Hack Team. (2020). https://www.turkhackteam.org/siber-guvenlik/1850624-session-hijacking-ve-session-security-nedir-siber-guvenlik-kulubu.html. (adresinden 10/01/2020 tarihinde alındı).

US Cyber War. (2020). https://sites.google.com/site/uscyberwar/cyber-weapons. (adresinden 07/01/2020 tarihinde alındı).

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2009). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler. Ankara: BTK Bilgi Teknolojileri ve İletişim Kurumu.

We Are Social. (2019). https://wearesocial.com/blog/2019/10/the-global-state-of-digital-in-october-2019. (adresinden 21/12/2019 tarihinde alındı).

White, S.P. (2018). Understanding Cyberwarfare: Lessons from the Russia-Georgia War. https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/. (adresinden 05/02/2020 tarihinde alındı).

Wills, M. (2017). WWII and the First Ethical Hacker. JSTOR Daily. https://daily.jstor.org/wwii-and-the-first-ethical-hacker/. (adresinden 03/02/ 2020 tarihinde alındı).

Wired. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/. (adresinden 19/02/2020 tarihinde alındı).

Wright, J. (2017). The Turing Bombe Victory and the first Naval Enigma Decrtpts. Cryptologia, 41(4).

Zerosecond. (2020). https://www.zerosecond.com.tr/single-post/2019/01/15/Drive-by-Download-Sald%C4%B1r%C4%B1lar%C4%B1. (adresinden 05/01/2020 tarihinde alındı).

EK-A: TARİHTEKİ SİBER SALDIRI VE SİBER SAVAŞ OLAYLARI		
S.No	**YIL**	**OLAY**
1	1939	Askeri Şifrelerin Kırılması (BOMBE).
2	1940	İlk Etik Korsan (Rene CARMİLLE).
3	1982	Sibirya Doğal Gaz Boru Hattı Saldırısı.
4	1999	NASA ve Savunma Bakanlığı Siber Saldırısı.
5	2003	ABD savunma şirketlerine Çin tarafından yapıldığı iddia edilen siber saldırılar (Titan Rain).
6	2006-2010	İran uranyum zenginleştirme tesislerine yönelik Stuxnet saldırısı.
7	2007	Estonya siber saldırıları.
8	2007	Pentagon'a ait email hesaplarının siber korsanlarca ele geçirilmesi.
9	2008	Rus-Gürcistan savaşı esnasında Gürcistan'a yapılan siber saldırılar.
10	2008	ABD askeri bilgisayarlarına siber saldırı.
11	2009	Vietnam'a politik nedenlerle yapılan DDos saldırıları (Vulcanbot).
12	2010	Myanmar (Bruma) siber saldırıları.
13	2010	Japonya-Güney Kore siber savaşları.
14	2010	Hindistan'a Çin tarafında yapıldığı iddia edilen siber saldırılar.
15	2011	Kanada Hükümetine ve ticari işletmelere ait sitelere siber saldırılar.
16	2011	İran petrol şirketlerine yönelik 'wiper' isimli zararlı yazılım saldırısı.
17	2011	ABD savunma bakanlığına ait 24.000 dosyanın siber korsanlarca çalınması.
18	2012	Suudi Arabistan Aramco ve Katar RasGas şirketlerine ait tesislerinde kullanılan bilgisayar sistemlerine yönelik siber saldırılar.
19	2013	Güney Kore siber saldırıları.
20	2013	Singapur siber saldırıları.
21	2013	İsrail' e yöneli siber saldırılar (OpIsrael).
22	2014	ABD'ye İran tarafıdan yapıldığı iddia edilen siber saldırılar (Operation Cleaver).
23	2014	Çin kaynaklı Özgürlük Ordusu üyelerince yapılıdığı öne sürülen ABD savunma bakanlığı bilgisayarlarından bilgi çalınması olayı.
24	2015	ABD Beyaz Saray'a ait bilgisayar sistemlerine Rus siber korsanlar tarafından yapıldığı öne sürülen siber saldırılar.
25	2017	Ukrayna siber saldırıları.