CYBERWARFARE ON THE THRESHOLD OF CHANGE AND TRANSFORMATION

ŞUAY NİLHAN AÇIKALIN - TEKİN BAYKIZ

Doç.Dr, Ankara Hacı Bayram Veli Üniversitesi, İİBF Uluslararası İlişkiller Bölümü
Mail: suaynilhan@gmail.com
ORCID ID: https://orcid.org/0000-0002-5361-7667

Doktora Öğrencisi, Ankara Hacı Bayram Veli Üniversitesi, İİBF Uluslararası İlişkiller Bölümü
Mail: baykiztekin@gmail.com
ORCID ID: https://orcid.org/0000-0001-7608-9978

Abstract

Throughout human history, the concepts of threat and war have undergone various transformations in terms of content and scope. Although the concept of war has been shaped by the notion of power, the greatest transformation in the tools and methods of war and threat in the last century has emerged through technological developments. While war technologies were primarily shaped within the framework of conventional warfare at the beginning of the twentieth century, the digital revolution in the last 20 years has led to the emergence of new battlefields beyond traditional warfare domains. This study aims to analyze the evolution of cyberwarfare and evaluate it within the framework of a case study. In this literature review-based study, seven different case studies have been analyzed using the document analysis method. As a result of the study, it was observed that the tools of attack have evolved and become more complex over the years. In addition, the damage caused by cyberwarfare has also shown multidimensionality. Secondly, digitalization and the immense increase in information and communication technologies have created a dependency on information systems from a security-oriented perspective. Thirdly and lastly, although cyberattacks have increased in variety, progress has also been made in the development of defense systems within the scope of cyberwarfare.

Keywords: Cyberwarfare, hybrid warfare, cyberspace, digitalization, case study.

Makaleye Ait Bilgiler

Makale Türü:	Araştırma
Geliş Tarihi:	30.10.2024
Kabul Tarihi:	20.11.2024
Yayın Tarihi:	15.12.2024
Yayın Sezonu:	Temmuz - Aralık

Makaleye Atıf Bilgisi

NILHAN AÇIKALIN Şuay - BAYKIZ Tekin (2024). "Değişim ve Dönüşümün Eşiğinde Siber Savaş". *Muhafazakâr Düşünce Dergisi*. Yıl: 20 Sayı: 67. (200-220)

DEĞİŞİM VE DÖNÜŞÜMÜN EŞİĞİNDE SİBER SAVAŞ

ŞUAY NİLHAN AÇIKALIN - TEKİN BAYKIZ

ÖZET

İnsanlık tarihi boyunca tehdit ve savaş kavramları içerik ve kapsam bakımından çok çeşitli dönüşümler geçirmiştir. Savaş kavramı, her ne kadar güç kavramı üzerinden şekillense de son yüzyılda savaş ve tehdit araç ve yöntemlerindeki en büyük dönüşüm, teknolojik gelişmelerle ortaya çıkmıştır. 20. yüzyılın başlarında savaş teknolojileri özellikle konvansiyonel savaş çerçevesinde şekillenirken, özellikle son 20 yılda dijital devrim, geleneksel savaş alanlarının dışında yeni savaş alanlarının ortaya çıkmasına neden olmuştur. Bu çalışmada, siber savaşın evrimini analiz etmek ve vaka çalışması çerçevesinde değerlendirmek amaçlanmıştır. Literatür taramaya dayalı bu çalışmada doküman analizi yöntemiyle 7 farklı örnek olay incelenmiştir. Yapılan çalışma sonucunda saldırı araçlarının yıllar içinde farklılaştığı ve karmaşıklaştığı görülmüştür. Buna ek olarak siber savaşın verdiği zarar da çok boyutluluk göstermiştir. İkinci olarak dijitalleşme, bilgi ve iletişim teknolojilerindeki muazzam artış, güvenlikçi bir bakış açısıyla bilgi sistemlerine bağımlılık yaratmıştır. Üçüncü ve son olarak siber saldırılar çeşitlilik göstererek artmış olsa da siber savaş kapsamında geliştirilen savunma sistemlerinde de ilerleme kaydedilmesini sağlamıştır.

Anahtar Kelime: Siber Savaş, Hibrit Savaş, Siber Uzay, Dijitalleşme, Vaka Çalışması.

Giriş

İnsanlık tarihi boyunca tehdit ve savaş kavramları içerik ve kapsam bağlamında geniş çerçevede farklılaşarak dönüşüme uğramıştır. Savaş kavramı, güç kavramıyla şekillenmekle birlikte geçen yüzyıl içerisinde en büyük dönüşümü teknolojik gelişmelerle yaşamıştır. 20. yüzyıl başlarında savaş teknolojileri özellikle konvansiyonel savaş çerçevesinde şekillenirken özellikle son 20 yıl içerisinde oluşan dijital devrim savaşın gelenekselin dışında yeni alanlarda meydana gelmesine neden olmuştur (Lehto, 2018; Whyte ve Mazanec, 2023).

Bu bağlamda dijital çağ ile birlikte siber savaş kavramı da gelişmiştir. Siber savaş kavram itibarıyla, hukuk, savunma ve uluslararası ilişkiler gibi interdisipliner alanda yer alarak günümüzde askerî, ekonomik ve politik boyutlarda bir tehdit olarak kabul edilmektedir (Robinson vd., 2015). Siber savaş, doğrudan ağ teknolojisine dayalı olarak dijital altyapıya zarar vermek, veri hırsızlığı yapmak ve sistemleri manipüle etmek olarak ifade edilmektedir (Boichak, 2021; Merrin, 2019).

Siber savaşın ışık hızında gerçekleşmesi ve küresel boyutlara ulaşabilme özelliği ile diğer savaş türlerinden ayrıldığı görülmektedir. Siber savaş, saldırının başlaması ile etkisi arasındaki zamanın çok kısa olması nedeniyle ülkelerin savunma sistemleri açısından risk oluşturmaktadır. Aynı zamanda banka yazılımlarından hava savunma sistemlerine kadar çok geniş yelpazede gerçekleştirilen siber saldırılar, eş zamanlı olarak birçok ülkeyi olumsuz yönde etkileyebilecek güce sahiptir (Clarke ve Knake, 2014).

Türkçe literatüre baktığımızda siber savaş kavramının özellikle uluslararsı ilişkiler teorileri ve uluslararası hukuk kapsamında ele alındığını söylemek mümkündür (Yayla, 2013; Güntay, 2017; Keskin, 2017). İlaveten, Türkçe literatürdeki çalışmalar gerçekleşen tekil saldırıları ele alarak yöntem, araç ve sonuçları incelemeye odaklanmıştır (Çelik, 2013; Holat, 2021).

Bu çalışmada öncelikli olarak siber savaş kavramı ve ilgili kavramlar bir arka plan olarak verilmiştir. Daha sonra siber savaşın değişim ve dönüşümünü kapsayan yedi tarihî örnek olay üzerinden doküman analizi yöntemiyle değerlendirme yapılmıştır. Söz konusu örnek olayların tercih edilmelerinde etkili olan unsurlar ise; sırasıyla dünya tarihinde iz bırakması ve küresel boyutta yer alması, teknolojik zayıflığın yanı sıra zarar vermek için insani duygulara da odaklanılması, fiziksel saldırılarla eş güdümlü olması ve politik amaç güdülmesidir. Ayrıca yapılan çalışmada seçilen örnek olaylar; askerî güvenlik, ekonomi ve politika parametleri açısından ele alınmıştır.

Çalışmanın sonuç kısmında ise, siber savaşın geçmişten günümüze araç, yöntem ve etkilerinin dönüşümüne yer verilmiştir. Yapılan bu çalışma, siber savaş kavramının değişim ve dönüşümünün birden fazla örnek olaylarla tarihsel bir akış çerçevesinde ele alınması Türkçe literatür açısından interdisipliner boyutu ve çoklu vaka incelemesi bağlamında alanyazına katkı sağlayacağı düşünülmektedir.

Siber Savaşı Anlamak: Kavramlar ve Ötesi

Bilgisayarların ve internetin hayatımıza yoğun olarak girdiği 1990'lı yılların sonrasında, dünya yeni bir alanla tanışmıştır. Birçok faaliyette kişi ve kurumlara etkisi tartışmasız olan bilgi ve iletişim teknolojileri (information and communication technology- BİT) küresel anlamda bilgiyi saklamayı, bilgileri işlemeyi ve çok hızlı bir şekilde dağıtımını sağlamıştır. Tanımlanan bu yeni alan, siber uzay olarak adlandırılmıştır. Siber uzayın büyük boyutlara erişmesini sağlayan ise, dijitalleşme faaliyetleri olmuştur. Dijitalleşme, kişi ve kurumların geleneksel yöntemlerle yürüttükleri faaliyetleri BİT devriminden sonra siber uzaya taşıması olarak tanımlanabilir. Bu noktada fiziksel ve somut dünya tarihininin yanı sıra, sanal olan bir siber dünya tarihine de tanıklık edilmektedir.

Özellikle 2000'li yılların sonrasında her işletme, kurum ya da evde bu 'devrimi' net olarak görmek mümkündür. Bu sayede, insanların veya kurumların sanal varlıkları yeni bir alana taşınmıştır. Bilinen tarihin başlangıcından itibaren, insanlar değerli varlıklarını 'ötekilere' karşı savunmuştur. Güvenlik daimî bir ihtiyaç olarak görülmüştür. Bunu sağlamak adına küçük kurumlar için güvenlik görevlileri, daha büyük kurumlar için güvenlik şirketleri, daha da büyük organizasyonlar olan devletler hatta güvenlik organizasyonları için ordular, donanmalar ve hava kuvvetleri görev yapmıştır. Ancak siber uzayın kuralları, konvansiyonel yani geleneksel dünyanın kurallarından oldukça farklıdır.

Uluslararası sistemin aktörleri açısından yeni ve kapsayıcı bir güvenlik alanı tanımlanması zorunluluğu siber uzayın bir doğurgusu olarak karşımıza çıkmıştır. Bu bağlamda, siber güvenlik ve siber savaş kavramlarına odaklanmak gerekmektedir. Vaishnav ve diğerleri Siber-UI'nin, siber alan içindeki karmaşık karşılıklı bağımlılıkları ortaya çıkarmak için çeşitli aktörler ve işlevler arasındaki etkileşimlerin analiz edildiği entegre bir sosyo-teknik sistem olarak anlaşılması gerektiğini öne sürmektedir (2013). Bu bakış açısı, Choucri'nin siber uzayın dünya siyasetinin analizine entegre edilmesinin, özellikle çatışma ve iş birliği dinamikleri açısından geleneksel uluslararası ilişkiler çerçevelerinin

yeniden değerlendirilmesini gerektirdiği iddiasıyla paralellik göstermektedir (Choucri, 2012). Siber alanda, güvenliği sağlamak ve bir çerçeve oluşturmak amacıyla "CIA" üçlemesi (İngilizce olarak "confidentiality" gizlilik, "integrity" bütünlük ve "availability" erişilebilirlik) kullanılmaktadır. Bu kavramsallaştırma, siber güvenliğin temeli olarak görülmektedir. Temel olarak bir ihlal veya saldırıdan bahsedilebilmesi için o varlığın, yetkili olmayan kişiler tarafından erişilmiş olması, bütünlüğünün bozulması yani silinmesi veya üzerinde yetkisiz değişiklikler yapılması ve son olarak bilgilerin ihtiyaç duyulduğunda erişilebilir olmaması saldırı veya ihlal olarak kabul edilmektedir.

Öte yandan, siber savaş kavramının birçok tanımı bulunmaktadır. Shakarian, ulusal güvenliğe ciddi tehdit oluşturan veya bir ulusun güvenliğine yönelik algılanan bir tehdide yanıt olarak gerçekleştirilen, devlet ya da devlet dışı aktörler tarafından siber alanda gerçekleştirilen eylemlerle yürütülen bir politikanın uzantısı olarak tanımlamıştır (Shakarian vd., 2013). Yine Beard'a göre siber savaş, bir ulusun başka bir ulusun ait kamu ya da sivil bilgi sistemlerine saldırmak adına bilgisayarlara mahsus yazılım ve teknolojiyi kullanmasıdır (Beard, 2013). Birden fazla tanımı olsa da 2010'lar ve sonrasında ortak bir yaklaşım olarak siber savaşı, siber saldırılar yolu ile düşman bir devlete yönelik olarak gerçek savaşa benzer zararlar verilmesi ve/veya dijital yapılarının ile bilgisayar sistemlerinin hayati düzeyde yıpratılması olarak ifade etmek mümkündür.

Siber güvenlik ve siber savaş, birbirleriyle eş zamanlı gelişen iki kavram olmakla beraber kendi kavram setini de üretmiştir. Dolayısıyla bu başlığında ifade ettiği gibi aşağıda kısaca bahsedilen kavramlar vakaların analizi için bir çerçeve oluşturmuştur.

Gelişmiş Kalıcı Tehdit (Advanced Persistent Thread- APT): Genel bir tanım olan APT, amacı ne olursa olsun bir işletme veya devlet gibi belirli bir varlığı hedef alan bir kişi veya grup tarafından düzenlenen bir dizi gizli ve sürekli siber uzay ataklarıdır (CFR, 2019). Bodmer, bu tür saldırıların daha sistematik olduğunu ve basit bilgisayar korsanlığından ayırmak için bir APT'nin çeşitli özellikler taşıması gerektiğini belirtmiştir. Diğer bir deyişle, amaç ve zamanlılık önemli bir ayrıştırıcı unsurdur. Saldırıların nereden gerçekleştiği de bir başka önemli kısmı temsil etmektedir (2012). Özetle, APT'ler sürekli olan ve daha fazla bilgi ve kaynağa ihtiyaç duyan, daha organize saldırılar olarak tanımlanabilir.

Hizmet Reddi (Denial of Service– DoS) ve Dağıtılmış Hizmet Reddi (Distibuted DoS) Saldırıları: Bu tür saldırılar hedef alınan varlığın, kasıtlı olarak hizmet verebilmesini önlemek (CFR, 2019), bir başka ifade ile erişilebilirlik yönünü sekteye uğratmak için yapılır. Bu saldırıların dağıtık yapıda olması, sistematik olarak aynı zaman diliminde farklı bölgelerden yapılması etkisini arttırabilir. Bilinen ilk ve en büyük örneği, 2007 senesinde gerçekleştirilen siber olaylardır.

Siber Casusluk: Bir hedefin faaliyetleri, hareketleri ve planları hakkında bilgi toplamak için bilgisayar ağlarının kullanılması olarak açıklanabilir (CFR, 2019). Kritik verilerin gizlilik ihlali yapılarak yetkisiz kişi ve kurumların ellerine geçmesi olarak özetlenebilir.

Kritik Altyapılar: Bir devlet veya ülke için yüksek öneme sahip ve ihlali durumunda ekonomi, güvenlik ve kamu sağlığı gibi etkileri olan altyapılardır. Kötü amaçlı yazılımlar ya da zararlı yazılımlar genel olarak üç kategoriye ayrılmaktadır: Virüsler; solucanlar ve Truva atları. Virüs, yayılmak için kendisini bir ana programa bağlaması gereken kendi kendini kopyalayan bir program ya da program parçasıdır. Genellikle virüslerin yalnızca bulaştığı bilgisayarda bulunup çoğalabilirler. Körü körüne her dosyaya bulaşabilir veya belirli çalıştırılabilir dosyalara saldırmak için programlanmış olabilirler. Solucan da kendi kendini çoğaltan bir programdır ancak çoğalmaya yardımcı olmak için başka bir programa ihtiyaç duymaz. Bu tür zararlı yazılımlar, saldırılarını başlatmak için herhangi bir insan etkileşimine ihtiyaç duymayan bağımsız programlardır. Solucan ve virüs arasındaki temel fark çoğalma şekilleridir. Virüsler bir ana sistemde çoğalırken solucanlar bilgisayar ağ bağlantıları üzerinden çoğalır. Truva atı ise, meşru bir program gibi görünürken bilinmeyen veya istenmeyen eylemler gerçekleştiren bir programdır (Karresand, 2003). Truva atı genellikle nihai yük yerine bir dağıtım sistemi olarak kullanılır.

Sıfırıncı Gün Açıkları: Yeni kullanılmaya başlanan bir yazılımın, daha önceden açıklarının bilinememesi sonucunda oluşan açıklardır (Farwell & Rohozinski, 2011).

Botnet: Kötü amaçlı yazılım bulaşmış ve bir grup olarak kontrol edilen bilgisayarlardan oluşan bir ağ. Botnetler genellikle spam yaymak ve dağıtılmış hizmet reddi saldırıları başlatmak için kullanılmaktadır (J. Carr, 2012).

Sızıntı ya da Sızma: Bir bilgisayardan diğerine izinsiz veri aktarımı anlamında kullanılmaktadır (Bendovschi, 2015).

Yetki Yükseltmesi: Bir kullanıcının etkisinin üstündeki haklara ihlal yoluyla erişim elde etme çabasını içeren bir siber tehdit durumunu ifade etmektedir (Proofpoint, 2023).

Kimlik Avı: Bu saldırı tipi oltalama olarak da tanımlanmaktadır. Kişilerin, parola veya kredi kartı numarası gibi bilgilerini ifşa etmeye ikna etmek için saygın kaynaklardan geldiği iddia edilen e-postalar gönderme yöntemidir (CFR, 2019).

Siber Savaş Kapsamında Örnek Olay İncelemesi

Siber savaşın değişim ve dönüşümünü kapsayan yedi tarihî örnek olay üzerinden doküman analizi yöntemiyle değerlendirme yapılmıştır. Söz konusu örnek olaylar; dünya tarihinde iz bırakması ve küresel boyutta yer alması, teknolojik zayıflığın yanı sıra zarar vermek için insani duygulara da odaklanılması, fiziksel saldırılarla eş güdümlü olması ve politik amaç güdülmesi gibi nedenlerden dolayı tercih edilmiştir. Ayrıca yapılan çalışmada seçilen örnek olaylar; askerî güvenlik, ekonomi ve politika parametleri açısından ele alınmış ve tablo 1'de sunulmuştur.

Tablo 1: Siber Savaş Kapsamında Örnek Olay İncelemesi

Askerî Güvenlik	Moonlight Maze Olayı Titan Rain Olayı Orchard Operasyonu
Ekonomi	I Love You Virüsü Stuxnet Saldırısı
Politika	Estonia DDOS Saldırıları 2016 ABD Seçimleri

Moonlight Maze Olayı

Moonlight Maze, tarihteki en eski ve en önemli devlet destekli siber casusluk kampanyalarından birini temsil etmektedir. 1990'ların ortalarında başlatılan bu operasyon çok sayıda ABD hükûmet ve askerî kurumlarını hedef almış ve büyük miktarda hassas bilginin çalınmasına yol açmıştır. Moonlight Maze, 1996 yılında başlamış ve 1998 yılına kadar devam ederek tarihte yaygın olarak bilinen ilk siber casusluk kampanyalarından biri olmuştur (Kaspersky Securelist, t.y.). Operasyon ilk olarak 1998 yılında ABD Savunma Bakanlığındaki bir bilgisayar yöneticisinin olağandışı ağ faaliyetlerini fark etmesiyle

ortaya çıkmıştır (Aktaş, 2023). Newsweek, Eylül 1999'da bu haberi yayınlayarak ABD'nin kararlı bir siber saldırı altında olduğunu ortaya koymuştur (Doman, 2018). Gelişmiş kalıcı tehdit (APT) olarak sınıflandırılan bu saldırı, temelde çeşitli yüksek profilli kuruluşlardan hassas verilerin sistematik olarak dışarıya sızdırılmasına neden olmuştur. Saldırılar öncelikle NSA, Pentagon, Enerji Bakanlığı, NASA ve çeşitli ulusal laboratuarlar gibi yüksek profilli kurumlar da dâhil olmak üzere ABD askerî, araştırma ve üniversite ağlarını hedef almıştır. Saldırganlar, gizli donanma kodları, füze yönlendirme sistemleri verileri ve diğer askerî teknolojiler de dâhil olmak üzere büyük miktarda hassas bilgi çalmıştır (Zetter, 2017). Çalınan veriler arasında, genellikle askerî amaçla kullanılan kontrol sistemlerinin bilgileri ve şemaları bulunduğu da iddia edilmiştir. Ayrıca çalınan veri miktarı o tarihe göre çok büyüktür ve 5 gigabyte'tan fazla olduğu hesaplanmıştır (Doman, 2018) .

ABD hükûmeti, saldırıları Rus devlet destekli aktörlere atfetmiş olsa da bulunan ilk kanıtlar saldırının izini süren bir Rus IP adresiyle sınırlı kalmıştır (Grant, 2024). Daha sonra yapılan incelemelerde ise, saldırının izi Moskova'dan 20 mil uzakta bulunan internet sunucularına kadar sürülmüştür. Saldırı şekilleri, sabah 8.00 ile akşam 17.00 arasında düzenli çalışma saatleri olduğunu ve Rus tatil günlerinde asla saldırmadıklarını ortaya koymuştur. Bu da eğer saldırılar Rusya tarafından gerçekleştirilmediyse devlet destekli oldukları şeklinde yorumlanmıştır (Doman, 2018). Sonuç olarak bu operasyon, Rus bir siber casusluk grubu olan, günümüzde adı "Turla" olarak geçen grup ile ilişkilendirilmiştir (Zetter, 2017).

Moonlight Maze, devletten devlete ilk önemli siber saldırı olarak kabul edilmekte ve sonraki siber casusluk operasyonları için bir emsal teşkil etmektedir (Grant, 2024; Walker, 2017). Bu saldırının sonucunda, siber güvenlik finansmanında önemli bir artışa ve bu tür saldırılara karşı korunmak için yeni teknolojilerin ve stratejilerin geliştirilmesine yol açmıştır. Moonlight Maze'den elde edilen içgörüler, sürekli teyakkuz, siber güvenliğe yatırım ve devlet kurumları ile özel sektör kuruluşları arasında iş birliğinin gerekliliğini vurgulamaktadır (Aktaş, 2023).

Titan Rain Olayı

Titan Rain olarak bilinen ve 2003-2006 yılları arasında meydana gelen siber olay, siber savaşın evriminde önemli bir dönüm noktasıdır. ABD hükûmeti ve savunma sektöründeki kurumların bilgisayar sistemlerini hedef alan bu koordineli saldırılar dizisinin, Çin kaynaklı olduğuna inanılmaktadır (Thornburgh, 2005). Titan Rain, devlet destekli siber tehditlerin

Moonlight Maze'den sonra yeni birini daha örneklemiş ve siber savaşın küresel manzarasında önemli bir tırmanışa işaret etmiştir. Sıfırıncı gün istismarları ve sosyal mühendislik de dâhil olmak üzere gelişmiş kalıcı tehdit (APT) tekniklerini kullanan saldırganlar, hassas ağlara yetkisiz erişim elde etmeyi başarmışlardır. Bu yöntemler, ele geçirilen sistemlerde uzun süreli, gizli bir varlığı kolaylaştırmıştır (Cyware Labs, t.y.). Böylelikle uzun süre boyunca tespit edilememiştir. Bu saldırının temel amacı; bu siber casusluk türü operasyonunun kapsamı, saldırganların askerî planlar, silah tasarımları ve diğer gizli bilgiler de dâhil olmak üzere büyük hacimli verileri sistematik olarak sızdırmaktır. Tahminlere göre terabaytlarca hassas bilgi çalınmış, bu da ulusal güvenlik ve kritik savunma yeteneklerinin potansiyel olarak tehlikeye atılması konusunda ciddi endişelere yol açmıştır.

Titan Rain'in etkisi, hükûmet ve savunma sektörlerinde siber güvenlik önlemlerinin yeniden değerlendirilmesine yol açmış, daha önce güvenli ağlar olarak kabul edilen ağlardaki güvenlik açıklarını ortaya çıkarmış ve mevcut siber güvenlik protokollerinin uzmanlar tarafından yapılacak devlet destekli tehditlere karşı yetersizliğini vurgulamıştır (Bodmer, 2012). Titan Rain'in ortaya çıkardığı zorluklara yanıt olarak etkilenen kuruluşlar; gelişmiş ağ izleme, gelişmiş erişim kontrolleri ve siber güvenlik altyapısı ve personeline artan yatırım gibi daha sıkı güvenlik önlemleri uygulamışlardır. Bu olay, ortaya çıkan siber tehditlerin ele alınmasında sağlam siber savunmaların ve uluslararası iş birliğinin artan öneminin altını çizmiştir. Tehdit istihbaratını paylaşmak ve daha etkili karşı önlemler geliştirmek için devlet kurumları, özel sektör kuruluşları ve uluslararası ortaklar arasında iş birliğinin artmasına yol açan Titan Rain, ayrıca siber uzayda devlet davranışlarını düzenleyen uluslararası normlara ve anlaşmalara duyulan ihtiyaç üzerine tartışmaları da teşvik etmiştir. Bu olay siber güvenlik tarihinde bir dönüm noktası olmuş; büyük ölçekli, devlet destekli siber operasyonların potansiyelini göstermiş ve daha gelişmiş tehdit tespit ve önleme stratejilerinin geliştirilmesinde hızlandırıcı görevi görmüştür (Benis, 2023). Bu olay, siber güvenliğin ulusal savunma ve kurumsal stratejinin temel bir unsuru olarak önceliklendirilmesinin kritik bir ihtiyaç olduğunu vurgulamıştır. Ayrıca bu olay, askerî ve istihbarat kurumları bünyesinde özel siber birimlerin kurulmasına, siber güvenlik araştırma ve geliştirme fonlarının artmasına ve siber hususların daha geniş ulusal güvenlik stratejilerine entegre edilmesine yol açmıştır. Daha da önemlisi siber uzayın; kara, deniz, hava ve uzayın yanı sıra ayrı bir savaş alanı olarak giderek daha fazla tanınmasına katkıda bulunmuştur. Bu durum ABD tarafından ilk olarak 1995 yılında General Fogleman'ın konuşmasında

bahsettiği "Enformasyon Operasyonu: Savaşın beşinci boyutu" gündemine geri dönülmesini sağlamıştır (Biernacik, 2018).

Orchard Operasyonu

İsrail hava kuvvetlerinin 6 Eylül 2007 yılında gerçekleştirdiği gizli bir hava saldırısı olan Orchard Operasyonu, modern savaşın evriminde, özellikle de siber-fiziksel saldırılar alanında önemli bir dönüm noktası olarak görülmektedir (Makovsky, 2012). Suriye'nin Al-Kibar nükleer reaktörünü hedef alan bu operasyon, elektronik savaşın konvansiyonel askerî taktiklerle birleştirilmesi sonucunda o tarihten önce görülmemiş bir ileri düzey operasyondur. Saldırı, resmî bir biçimde İsrail hava kuvvetleri tarafından gerçekleştirilmiştir (Gross, 2018). Ayrıca 21 Mart 2018 tarihinde İsrail Savunma Bakanlığı tarafından üstlenilmiştir (Ahronheim, 2018b).

Saldırı, temelde Suriye'nin hava savunma sistemlerini kesin bir şekilde etkisiz hâle getirme amacını taşımaktadı. Gizli olarak faaliyet yürüttüğü düşünülen Deyrizor bölgesindeki nükleer reaktöre erişmek amacıyla öncelikle bilgi toplanmaya başlanmıştır. İsrail istihbaratının (Mossad), Suriyeli üst düzey bir yetkilinin dizüstü bilgisayarına yurt dışındayken gizlice bir "truva atı" programı yükleyerek son derece hassas ve gizli bilgileri elde etmeyi başardığı bildirilmiştir (Stark, 2009). Daha sonra fiziksel saldırı öncesinde, İsrailli savaş uçakları Türkiye sınırına yakın Tel Abyad'daki bir Suriye radar sahasını elektronik bir saldırı ile meşgul etmiş ve ardından hassas bir güdümlü füze ile hedef almıştır. Bu hibrit saldırı, tüm Suriye radar sistemini geçici olarak bozmuştur ve İsrail kuvvetlerinin operasyon boyunca Suriye hava sahasına güvenli ve tespit edilmeden girmesine izin vermiştir (Clements, 2012). Suter saldırısı olarak adlandırılan bu saldırıda, hedefin antenlerine elektronik darbeler gönderilerek ve özelleştirilmiş sinyaller eklenerek saldırıya uğrayan hava savunma sistemi bozulmaktadır. Ağ için erişim sağlandıktan ve iletişim döngüsüne ulaştıktan sonra, operatörleri aldatmak amacıyla yanıltıcı mesajlar veya hayalî hedefler gibi veriler eklemiş ve hava savunma sistemini bozarak savunmayı tamamen devre dışı bırakmışlardır (Gasparre, 2008). Sonuç olarak İsrail jetleri, Suriye hava sahasına girebilmiş, havadan tesise yaklaşık 17 ton bomba bırakıp ve tespit edilmeden çıkabilmiştir (Ahronheim, 2018a).

Siber güvenlik perspektifinden bakıldığında Orchard Operasyonu, oldukça önemli bir yerde bulunmaktadır. Bilgi toplamak amacıyla Truva atı saldırısı ile başlatılması ve sonrasında konvansiyonel bir savaş için avantaj sağlaması son derece önemlidir. Başka bir ülkenin savunma mekanizmasının

tamamen devre dışı kalması da siber savaş boyutunu vurgulamaktadır. Ayrıca bu saldırı, Rusya yapımı hava savunma sisteminin yetersizliğini ve güvenlik açıklarını da vurgulaması açısından dikkate değerdir (Weinberger, 2007).

I Love You Virüsü

Aşk Böceği ya da Aşk Mektubu solucanı olarak da bilinen "I love you" virüsü, Mayıs 2000'de ortaya çıkmıştır. E-posta ekleri yoluyla hızlı ve etkili bir şekilde yayılmasıyla öne çıkan bu bilgisayar solucanı, 2000'lerin başında internet ile yeni tanışan insanların sayısının fazlalığı ile hızla yayılmıştır. Virüsün karmaşık sosyal mühendislik stratejileri kullanması, etkisini en üst düzeye çıkarmasında etkili olmuştur. "ILOVEYOU" gibi dikkat çeken elektronik posta başlığı ve 'Love-Letter-For-You.txt.vbs' (dosyanın uzandısından anlaşılacağı üzere, bu dosya visual basic diliyle yazılmış bir solucan türü zararlı yazılımdır) gibi yanıltıcı bir isim taşıyan bir ek içermektedir. Bu ismin ilgi çekici olması nedeniyle sadece teknolojik zayıflıklardan değil ayrıca insanların duygusal ve merakla ilgili zayıflıklarından da faydalanılmıştır (Chinnaraj, 2024; S. Li, 2023).

Solucan etkinleştirildikten sonra, bulaşan bilgisayar içinde bir takım faaliyetleri başlatılmıştır. Bilgisayarda bulunan görüntüler, ses dosyaları ve belgeler de dâhil olmak üzere ele geçirilen bilgisayardaki çeşitli dosya türlerinin üzerine yazarak kişisel ve profesyonel verileri ortadan kaldırılmıştır. Dahası solucan, kullanıcının adres defterindeki tüm kişilere kopyalar göndererek kendini yaygınlaştırmış ve bu da etkisini önemli ölçüde artırmıştır. Bu kendi kendini kopyalama özelliği, hızlı bir şekilde küresel olarak yayılmasında önemli bir faktör olarak öne çıkmıştır (Krajnyk, 2024).

"I Love You" virüsünün etkileri hem hızlı yayılımı hem de verdiği zarar açısından çok büyük olmuştur. Dünya çapında tahminen 45 milyon bilgisayar etkilenmiş olup sadece bireysel kullanıcıları değil işletmeleri ve devlet kurumlarını da etkilemiştir. Milyarlarca dolar olarak tahmin edilen zararların mali sonuçları da oldukça büyük olmuştur. Bu maliyetler; veri kaybı, sistem kurtarma çabaları, iş kesintileri ve üretkenliğin azalmasını gibi nedenler olarak ortaya çıkmıştır (Chinnaraj, 2024).

Bu olay, siber güvenlik paradigmalarının yeniden değerlendirilmesine yol açmış ve giderek birbirine daha fazla bağlanan bir ortamda daha detaylı siber güvenlik önlemlerinin alınması zorunluluğunun altını çizmiştir. Mevcut güvenlik protokollerinin kırılganlığını ve iyi tasarlanmış tek bir kötü amaçlı yazılımın büyük zarar verme potansiyelini gözler önüne sermiştir. Kurumlar siber güvenlik altyapısına ve personel eğitimine önemli kaynaklar

ayırmaya başlamıştır (Schwarz, 2024). Teknoloji sektörü yeni ortaya çıkan siber tehditlere karşı daha sofistike ve öngörülü savunmaların gerekliliğini kabul ettiğinden, bu olay antivirüs yazılımı ve güvenlik protokollerindeki gelişmeleri hızlandırmıştır.

Ayrıca, "I Love You" virüsü kullanıcı davranışları ve farkındalığı üzerinde kalıcı bir etki yaratarak, tanıdık kaynaklardan gelenler de dâhil olmak üzere istenmeyen e-postalar ve ekler konusunda dikkatli ve şüpheci olunması gerektiğini vurgulamıştır. Bu olay hem bireyleri hem de kuruluşları hedef alan kapsamlı siber güvenlik eğitim programlarının ve farkındalık kampanyalarının geliştirilmesini teşvik etmiştir.

Stuxnet Saldırısı

2010'da tespit edilen Stuxnet zararlı yazılımı, siber güvenlik tarihinde dönüm noktası niteliğinde bir saldırı olarak görülmektedir. Bir bilgisayar solucanı olarak kategorize edilen bu karmaşık kötü amaçlı yazılım, özellikle İran'ın nükleer programının ayrılmaz bir parçası olan endüstriyel kontrol sistemlerine zarar vermek için kasıtlı olarak tasarlanmıştır. Stuxnet'in doğasında bulunan karmaşıklık ve hedefine kendi kendine ilerleme kabiliyeti, onu daha önceki siber tehditlerden ayırarak siber savaşın ilerlemesinde yeni bir çağın habercisi olmuştur.

Stuxnet, Windows işletim sistemlerindeki ve Siemens endüstriyel yazılımındaki birden fazla sıfırıncı gün açığından yararlanarak çok yönlü bir saldırı stratejisi yürüterek ilerlemiştir. Bu taktik, sıfırıncı gün açıkları siber güvenlik alanında son derece nadir bulunan bir araç olduğundan son derece etkili olmuştur. Bir başka ifade ile solucan yerleştirildikten sonra otonom bir şekilde ilerleyerek merkez ile bağlantısız bir şekilde faaliyetlerine devam edebilmiştir. Stuxnet, uranyum zenginleştirme için tasarlanmış santrifüjlere zarar vermek için programlanabilir mantık kontrolörlerinin (PLC'ler) manipüle edilmesini amaçlamıştır. Saldırının bu yönü, dijital ve fiziksel alanların yakınlaşmasını örneklemesi ve siber saldırıların somut, bedensel hasar verme kapasitesini göstermesi açısından oldukça önemli olmuştur (Farwell ve Rohozinski, 2011). Solucan, santrifüjlerin dönüş hızlarında küçük, periyodik değişiklikler yaparak arızalara ve hatalara neden olacak şekilde programlanmıştı. Aynı zamanda bu faaliyetlerini gizlemek için operatörlere aldatıcı geri bildirimler ilettiği de iddia edilmiştir (Lachow, 2011).

Stuxnet'in benzersiz karmaşıklığı, devlet destekli olduğu iddia edilen oluşumuyla birleştiğinde, siber savaşta çok önemli bir dönüm noktası

oluşturmuş. Hiçbir zaman resmî olarak doğrulanmamış olmasına rağmen solucanın, ABD ve İsrail arasındaki ortak bir çabayla geliştirildiği ve bir ulus tarafından diğerine karşı kullanılan bir siber silahın ilk örneklerinden biri olduğu varsayılmaktadır (Çelik, 2013).

Ayrıca Stuxnet, siber güvenlik endüstrisinde ve araştırma topluluğunda önemli ilerlemelere yol açarak kötü amaçlı yazılım analiz metodolojilerinde, saldırı tespit sistemlerinde ve daha güvenli endüstriyel kontrol sistemlerinin geliştirilmesinde iyileştirmeleri teşvik etmiştir. Bu olay ayrıca siber güvenlik sorunlarıyla mücadelede devlet kurumları, özel sektör kuruluşları ve akademik kurumlar arasında iş birliğinin artmasını da teşvik etmiştir (Collins ve McCombie, 2012).

Estonia DDOS Saldırıları

2007 yılında Estonya'ya yapılan siber saldırılar; büyük ölçekli, siyasi amaçlı siber savaşın ilk örneklerinden birini işaret ederek siber güvenlik tarihinde ufuk açıcı bir olayı temsil etmektedir. Bu olay birkaç hafta boyunca devam etmiş ve devlet portalları, finansal sistemler ve medya ağları da dâhil olmak üzere Estonya'nın dijital altyapısının geniş bir yelpazesine yönelik bir dizi gelişmiş, koordineli dağıtılmış hizmet reddi (DDoS) saldırısını içermektedir. Mevcut analizler, bu saldırıların büyük olasılıkla Rusya bağlantılı siber aktörler tarafından düzenlendiğini öne sürse de siber adli analizin doğasında var olan zorluklar nedeniyle kesin atıfta bulunmak zordur.

Estonya devleti, 2000 yılından itibaren yaptığı atılımlar ile çağının belki de çok ilerisinde dijitalleşmeye yönelmiştir. Hatta internete erişimi, her insan için bir insan hakkı olarak değerlendirmiştir. 2007 yılı öncesinde okullarda eğitim, vergi ödeme sistemi, vatandaşların dijital kimliklere sahip olması gibi o zamanlar için devrim niteliğinde gelişmeler yapılmıştır. Ancak dijital dünyaya bu derece bağımlı olma hâli bütün dünyaya ders olacak bir saldırı ile tüm dünyaya siber güvenlik vurgusu olan bir "uyandırma çağrısına" dönüşmüştür. Estonya hükûmetinin Tallinn'de Sovyet döneminden kalma bir savaş anıtı olan Bronz Asker'in yerini değiştirme hamlesi, Estonya'nın Rusça konuşan azınlığı arasında ciddi bir muhalefete yol açmış ve Moskova'dan sert tepkiler alarak Estonya ile Rusya arasında zaten gergin olan ilişkileri daha da kötüleştirmiştir. Bunu izleyen siber saldırı, jeopolitik anlaşmazlıkların siber alana geniş kapsamlı sonuçlarla yayılmasının bir örneği olarak misilleme önlemi olarak görülmüştür.

Saldırganlar, Estonya'nın siber altyapısını aşırı trafik hacmiyle boğmak ve böylece etkisiz hâle getirmek için ağırlıklı olarak botnet'leri (virüslü bilgisayarlardan oluşan bir ağ) kullanarak bir dizi gelişmiş teknik kullandılar. 27 Nisan 2007 tarihinde başlayan ve yaklaşık 3-4 hafta süren DDOS türü saldırıların yoğunluğu ve süresi o zamana kadar görülmemiştir. Estonya toplumunun geniş bir kesimini ve günlük yaşamı etkilemiştir (Davis, 2007).

Bu siber saldırıların sonuçları derin ve çok boyutlu olmuştur. Online bankacılık, hükûmet operasyonları ve medya yayıncılığı da dâhil olmak üzere kritik hizmetleri kesintiye uğratmış ve milyonlarca avro olduğu tahmin edilen önemli ekonomik yansımalara yol açmıştır. Dahası bu olaylar Estonya'nın yüksek oranda dijitalleşmiş toplumunun doğasında bulunan ve hükûmet ve günlük işlemlerinin büyük bir kısmı için internet tabanlı altyapıya büyük ölçüde güvenen güvenlik açıklarını ortaya çıkarmıştır (Landler ve Markoff, 2007). Ancak saldırıların doğası gereği, kamu ve özel kuruluşlar ülke dışındaki kaynaklardan gelen erişimi engelleyerek kendilerini savunmak amacıyla birçok web sitelerinin dünyanın geri kalanı için engellenmesi ile sonuçlanmıştır (Czosseck vd., 2011)Estonia was one of the most developed nations in Europe regarding the ubiquitous use of information and communication technology (ICT. Yıkıcı olmasına rağmen DDoS saldırıları, herhangi bir fiziksel hasar yaratmamıştır ve gerçek siber savaş seviyesine yükselmemiştir (Ranger, 2018).

Anlık operasyonel ve ekonomik etkilerin ötesinde, 2007 Estonya siber saldırıları küresel toplum için zorunlu bir uyandırma çağrısı işlevi görmüştür. Bu saldırılar; siber savaşın modern, dijital bağımlı toplumlarda konvansiyonel askerî müdahaleye gerek kalmadan yaygın bir bozulma yaratma potansiyelinin altını çizmiştir. Bu farkındalık, ulusal ve uluslararası siber güvenlik stratejilerinin ve savunma duruşlarının çok önemli bir şekilde yeniden değerlendirilmesine yol açmıştır.

Olayın hemen ardından dönemin Estonya Savunma Bakanı Jaak Aaviksoo, NATO'ya 5. maddenin hükümlerinin yani kolektif meşru müdafaanın, uygulanmamasını talep ettiklerini bildirmiştir. Ancak NATO, o tarihlerde siber saldırıları açık bir askerî eylem olarak tanımadığından bu kapsamda değerlendirilmediğini bildirmiştir (Traynor, 2007). Bu olaydan sonra Estonya, siber dayanıklılığını artırmak için önemli tedbirler almış ve uluslararası camia ile kolektif adımlar atmıştır. NATO'nun bir üyesi olarak Siber Savunma Mükemmeliyet Merkezi, Talinn'de kurulmuştur. Bu kurum o zamandan beri siber savunma araştırmaları, eğitimi ve iş birliği için önde gelen küresel bir merkez hâline gelmiştir. Ayrıca Estonya, 2008 yılında kamu-özel

sektör iş birliği ve uluslararası iş birliğini vurgulayan kapsamlı bir ulusal siber güvenlik stratejisi geliştirmiştir ve uygulamaya koymuştur. Buna göre Estonya, siber güvenlik konusunda uluslararası iş birliğini artırmayı, yasal çerçeveyi geliştirmeyi, farkındalığın arttırılmasını ve savunma alanında bir dizi önlemler almayı stratejik amaç olarak belirlemiştir (Czosseck vd., 2011) Estonia was one of the most developed nations in Europe regarding the ubiquitous use of information and communication technology (ICT.

Özetle, 2007 yılında Estonya'ya yapılan siber saldırılar, siber güvenliğin evriminde kritik bir dönüm noktasına işaret ederek siber çatışmaların önemli ve somut sonuçlar doğurduğu bir dönemin başlangıcına işaret etmiştir. Bu olaylar hem ulusal hem de uluslararası düzeyde sağlam siber güvenlik çerçevelerinin gerekliliğini vurgulamış, siber tehditlere karşı hükûmetler arası iş birliğini artırmış ve altyapı dayanıklılığı ile halkın hazırlıklı olmasının önemini ortaya koymuştur. Saldırı sonrasında, 2004 yılından beri NATO üyesi olan Estonya'ya hem NATO'dan hem de Avrupa Birliği'nden çok fazla destek gelmiştir. NATO 2008 yılında, Kooperatif Siber Savunma Mükemmeliyet Merkezi'ni Talin'de kurmuştur ve o tarihten beridir eğitim, araştırma ve geliştirme, danışma ve siber olaylardan çıkarılan derslerin değerlendirildiği bir merkez olmuştur.

2016 ABD Seçimleri

Rusya'nın, 2016 ABD başkanlık seçimlerine müdahale ettiği iddiası; siber güvenlik, siyaset bilimi ve uluslararası ilişkilerin çağdaş yıllıklarında dönüm noktası niteliğinde bir olaydır. Haziran 2016'da, ABD Demokratik Ulusal Komitesi (DNC) ağlarında şüpheli Rus tehdit aktörleri keşfedilmiştir. Saldırganlar, Cumhuriyetçi başkan adayı Donald J. Trump hakkındaki araştırmalara ve DNC yetkilileri arasındaki e-posta ve yazışmalara erişim sağlamıştır (Nakashima, 2016). Başkanlık kampanyası süresince tehdit aktörleri, WikiLeaks gibi aracılar vasıtasıyla DNC yazışmalarını yayınlayarak üst düzey parti yetkilileri arasındaki çekişmelerle ilgili bilgileri ifşa etmiştir ve DNC başkanı olan Debbie Wasserman Schultz'un istifasına yol açmışlardır (Roberts vd., 2016). Tehdit aktörleri, Hillary Clinton'ın kampanyasının başkanı John Podesta'yı da zorlayan bir takım gizli bilgi ve verileri yayınlamışlardır (Wikileaks, 2016). İç Güvenlik Bakanı ve Ulusal İstihbarat Direktörü ortak bir açıklama yayınlayarak uzun süren siber casusluk kampanyasının Rus aktörlerin işi olduğunu iddia etmişlerdir. Barack Obama yönetimi, daha sonra Rus istihbarat yetkililerine yaptırım uygulamış ve ABD'de çalışan şüpheli memurları sınır dışı etmiştir (The White House, 2016). DNC'nin ifşa edilmesinin, Batı demokrasilerindeki seçim sistemlerini

manipüle etmek ve ABD, Fransa, Almanya ve diğer yerlerdeki demokratik sürece olan inancı zayıflatmak amacıyla yürütülen daha büyük bir Rus casusluk kampanyasının parçası olduğuna inanılmaktadır. Temmuz 2018'de ABD Adalet Bakanlığı ve FBI, GRU olarak bilinen Rus askerî istihbarat teşkilatının bu olaydan sorumlu olduğuna inanılan on iki yetkilisini suçlamışlardır. Ekim 2018'de Birleşik Krallık hükûmeti, söz konusu sızıntının Rus askerî istihbaratının eylemi olduğunu açıklamıştır (The UK National Cyber Security Centre, 2018).

Bu siber vakada hedef alınan başlıca kuruluşlar, Demokratik Ulusal Komite (DNC) ve Demokratik Parti'ye bağlı önemli kampanya yetkilileriydi. Failler bu kurumların dijital altyapılarına başarılı bir şekilde sızarak çok sayıda hassas veriyi yasa dışı yollardan elde etmişlerdir. Bu olay, Rus istihbarat aygıtları tarafından düzenlendiği iddia edilen, devlet destekli bir siber saldırı olarak kabul edilmektedir. Bu operasyonun temel amacı kamuoyunu manipüle etmek ve ABD başkanlık seçimlerinin sonucunu etkilemek gibi görünmektedir. Bu vaka, siber yeteneklerin jeopolitik etki aracı olarak kullanılmasında önemli bir tırmanışı temsil etmekte ve geleneksel casusluk, bilgi savaşı ve seçim müdahalesi arasındaki sınırları belirsizleştirmektedir. Saldırganlar, titizlikle hazırlanmış kimlik avı e-postaları ve diğer aldatıcı mekanizmalar yoluyla insani zaaflardan faydalanarak son derece sofistike sosyal mühendislik taktikleri kullanmışlardır. Ayrıca hassas verilere yasa dışı erişim elde etmek ve sürdürmek için e-posta sistemlerindeki ve ağ altyapılarındaki teknik açıklardan da yararlanmışlardır (Rid, 2016). Bu taktiklerin etkinliği hem teknik siber güvenlik önlemlerinin hem de kapsamlı kullanıcı eğitiminin bu tür saldırıları engellemedeki büyük öneminin altını bir kere daha çizmektedir.

Bu müdahalenin sonuçları, seçimin kendisi üzerindeki anlık etkinin ötesine geçerek derin ve çok yönlü olmuştur. Olay, Amerikan toplumu içinde önemli bir anlaşmazlık yaratarak mevcut siyasi bölünmeleri şiddetlendirerek yeni fay hatları oluşturmuştur. Halkın seçim süreci de dâhil olmak üzere demokratik kurumlara olan güvenini sarsmıştır.

Sonuç

Bu çalışmada, dünya tarihinde iz bırakan ve küresel boyutta yer alan, teknolojik zayıflığın yanı sıra zarar vermek için insani duygulara da odaklanan, fiziksel saldırılarla eş güdümlü olan ve politik amaç güdülen 7 farklı örnek olay incelenmiştir. Bu vakalara ilgili saldırı türü, etkilenen kurum/devlet ve yaşanan saldırının önemini içeren değerlerndirmeler gerçekleştirilmiştir.

İlk olarak, 1998 yılında yaşanan ulus-devlet destekli ilk siber casusluk kampanyalarından biri olarak kabul edilen ve siber savaşta yeni bir dönem

başlattığı düşünülen Moonlight Maze saldırısı ele alınmıştır. Rusya'ya atfedilmiş olan ve gelişmiş kalıcı tehdit türü kullanılan bu saldırıda, ABD hükûmeti ve savunma sektöründeki kurumlar etkilenmiştir.

İkinci olarak 2003 yılında Çin destekli ilk siber istihbarat operasyonu olması özelliğini taşıyan Titan Rain saldırısı incelenmiştir. ABD hükûmeti ve savunma sektöründeki kurumların etkilendiği gelişmiş kalıcı tehdit türü kullanılan bu saldırı, siber güvenliğin devletler için kritik verilerin korunması üzerindeki önemini açıkça göstermiştir.

Üçüncü olarak 2007 yılında yaşanmış olan İsrail ve ABD operasyonu olduğu iddia edilen siber casusluk türünü içeren Orchard Operasyonu ele alınmıştır. Suriye'nin Deyrizor bölgesinde nükleer faaliyetler sürdüğü düşünülen tesisin etkilendiği bu saldırı, gelişmiş elektronik/dijital araçların, farkedilmeksizin bir ülkenin savaş yetenekleri ile birlikte kullanılarak etkisini artırdığını göstermiştir.

Dördüncü olarak 2000 yılında ortaya çıkan, e-posta sistemlerinin güvenlik açıklarını ve siber güvenlikteki insan faktörünü vurgulamış olan "I love you Virüsü" incelenmiştir. Solucan ve karmaşık sosyal mühendislik türü olan bu siber saldırı sonucunda dünya genelinde bireyler ve kurumlar etkilenmiştir. Beşinci olarak 2010 yılında gerçekleşen sosyal mühendislik, gelişmiş toolkit, gelişmiş kalıcı tehdit türlerini içeren Stuxnet saldırısı incelenmiştir. Kontrollü bir test ortamı dışında fiziksel hasara neden olan ilk siber operasyon örneği olarak bilinen bu saldırı İran'ın nükleer programı ve Natanz'da bulunan uranyum zenginleştirme tesislerini etkilemiştir.

Altıncı olarak aynı sene içinde yaşanmış olan DDOS türü kullanılan Estonya saldırısı incelenmiştir. Estonya'nın hem kamu hem de özel sektörüne yapılmış olan ve Rusya'ya atfedilen bu saldırı, modern dijital altyapının kırılganlıklarını vurgulayarak uluslararası toplum için bir "uyandırma çağrısı" olmuştur. Yedinci olarak 2016 yılında gerçekleşen kimlik avı, sosyal mühendislik ve siber casusluk türlerini içeren ABD Başkanlık Seçimine Müdahele saldırısı ele alınmıştr. ABD'yi etkileyen bu saldırı, seçim süreçlerinde zayıflıkları ortaya sunduğu için önem teşkil etmektedir.

Sonuç olarak doküman analizi ve vaka araştırma yöntemlerinin kullanılması ile incelenen önemli siber saldırılara bakıldığında üç önemli sonuç ortaya çıkmaktadır. İlk olarak; bu tarihler arasında, saldırı araçlarının çeşitlendiği ve geliştiği görülmüştür. Ayrıca verilen zararın da çok boyutlu olması gözlemlenmiştir. Büyük mali kayıplara neden olabilen vakalara, fiziksel alana da etki eden saldırı vakalarına da rastlanmıştır. Ayrıca konvansiyonel

savaş yöntemleri ile iç içe şekilde kullanıldığı da görülmüştür. İkincil olarak dijitalleşme, bilgi ve iletişim teknolojilerinin incelenen yıllar arasında büyük artışı, bilişim sistemlerine bir bağımlılık oluşturduğu çok net olarak görülmüştür. Hem özel sektör hem de kamunun sahip olduğu sağlık, savunma ve kritik altyapılar gibi çok önemli veriler ve hizmetler, siber uzay olarak tanımlanan alanda yerini almıştır. Üçüncü olarak gözlemlenen bir diğer sonuç ise, saldırgan tarafının yeni açıklar bulup tehdit yaratabildiğidir. Ancak savunma mekanizmalarında da gözle görülür bir artış olduğu ifade edilebilir. İncelenen kaynaklarda savunma tarafının öğrenilen dersleri sayesinde, o tür saldırıyı hiç deneyimlememiş devlet veya kurumlara da kazanılan deneyimler yardımıyla bir güvenli alan oluşturduğu görülmüştür. Dolayısıyla savunma tarafı bir adım geriden de saldırılarda kullanılan yöntem ve teknolojileri yakalamayı başarmıştır. Kısacası, 2000'lerin başlarında felaket sonuçlar yaratan saldırıların günümüzde hiçbir etkisi olmayacak noktaya gelinmesi; siber güvenlik konusunda başta devlet olmak üzere tüm aktörlerin yüksek bütçeler ayırmasını, savunma şirketlerinin sürekli olarak kendini yenilemesini ve farkındalık eğitimlerinin yaygınlaşmasını sağlamıştır. Son olarak kavramsal çerçeve açısından bakıldığında da yaşanan saldırıların önemli bir dönüştürücü olduğunu görmek gerekir. Bir başka ifade ile her saldırı aynı zamanda yeni kavramların da bir literatür oluşturmasını sağlamıştır. Siber savaşın kavramsal olarak da oldukça dinamik ve değişken yapıda olduğunu söylemek mümkündür.

Kaynakça

Ahronheim, A. (2018a, Mart). *After a decade Israel admits: We bombed Syria nuclear reactor in 2007—The Jerusalem Post* [Newspaper]. The Jerusalem Post. https://www.jpost.com/Arab-Israeli-Conflict/After-a-decade-Israel-admits-We-bombed-Syria-nuclear-reactor-in-2007-546573

Ahronheim, A. (2018b, Mart 21). *Liberman: Squabbling over credit for strike on Syrian reactor an "embarrassment"*. The Jerusalem Post | JPost.Com. https://www.jpost.com/israel-news/liberman-praises-israels-strike-on-syrian-reactor-livni-recalls-events-546640

Aktaş, M. (2023, Mart 7). Unraveling the Moonlight Maze: The State-Sponsored Cyber Espionage Campaign that Changed.... *Medium*. https://medium.com/@mertaktas1283/unraveling-the-moonlight-maze-the-state-sponsored-cyber-espionage-campaign-that-changed-1a79e129b358

Beard, M. (2013). Cyberwar and just war theory. Applied ethics, risk, justice and liberty, 1-12.

Bendovschi, A. (2015). Cyber-Attacks- Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, 28, 2015, 24-31. https://doi.org/10.1016/S2212-5671(15)01077-1

Benis, M. (2023, Ocak). *(23) Titan Rain: The 2005 Cyber Attacks on the US Department of Defense | LinkedIn* [Blog]. LinkedIn. https://www.linkedin.com/pulse/titan-rain-2005-cyber-attacks-us-department-defense-michael-benis/

Biernacik, B. (2018). The Fifth Dimension of War–Cyberspace. How to Secure This Area: The Approach of Selected States and International Organizations to Cybersecurity. *Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu*, 83(6), 2018, 63-84.

Bodmer, S. (2012). *Reverse deception: Organized cyber threat counter-exploitation*. McGraw-Hill.

Boichak, O. (2021). Digital War: Mediatized Conflicts in Sociological Perspective. in The Oxford Handbook of Digital Media Sociology. (Ed.) Deana A. R., Sarah S.

Carr, J. (2012). *Inside cyber warfare* (2nd ed). O'Reilly.

CFR. (2019). *Tracking State-Sponsored Cyberattacks Around the World*. Council on Foreign Relations. https://www.cfr.org/cyber-operations

Chinnaraj, S. (2024, Şubat). *(22) The Infamous "I Love You" Virus: A Cybersecurity Milestone | LinkedIn* [Blog]. Linkedin. https://www.linkedin.com/pulse/infamous-i-love-you-virus-cybersecurity-milestone-chinnaraj-tbzfc/

Choucri, N. (2012). *Cyberpolitics in International Relations*. The MIT Press. https://doi.org/10.7551/mitpress/7736.001.0001

Clements, R. (2012, Eylül 10). New details of Israel's 2007 attack on the Syrian Nuclear reactor emerge. *The Aviationist*. https://theaviationist.com/2012/09/10/op-orchard/

Collins, S., McCombie, S. (2012). Stuxnet: The emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, 7(1), 2012, 80-91. https://doi.org/10.1080/18335330.2012.653198

Cyware Labs. (t.y.). *Remembering Operation Titan Rain—Titan Rain Cyber Attack*. Cyware Labs. Geliş tarihi 12 Eylül 2024, gönderen https://cyware.com/news/remembering-operation-titan-rain-c54ad3e4

Czosseck, C., Ottis, R., Talihärm, A.-M. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *International Journal of Cyber Warfare and Terrorism*, 1(1), 2011, 24-34. https://doi.org/10.4018/ijcwt.2011010103

Çelik, Ş. (2013). Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme. *Dokuz Eylul University Law Review*, 15(1), 2013, Article 1.

Davis, J. (2007, Ağustos 21). *Hackers Take Down the Most Wired Country in Europe | WIRED* [Newspaper]. The Wired. https://www.wired.com/2007/08/ff-estonia/

Doman, C. (2018, Ocak 22). The First Sophistiated Cyber Attacks: How Operation Moonlight Maze made history. *Medium*. https://medium.com/@chris_doman/the-first-sophistiated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7

Farwell, J. P., Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, 53(1), 2011, 23-40. https://doi.org/10.1080/00396338.2011.555586

FBI. (2014, Aralık 19). *Update on Sony Investigation—FBI* [Press Release]. https://www.fbi.gov/news/press-releases/update-on-sony-investigation

Gasparre, R. (2008, Mart 10). The Israeli "E-tack" on Syria – Part II - Airforce Technology. Airforce Technology. https://www.airforce-technology.com/features/feature1669/

Grant, P. (2024, Nisan 15). Moonlight Maze: Russian Espionage, Hacking, and Cyber Warfare in the Lead-Up to the 2016 Election. *Medium*. https://medium.com/@petergrant_14485/moonlight-maze-russian-espionage-hacking-and-cyber-warfare-in-the-lead-up-to-the-2016-election-a8fdbee51309

Griffin, A. (2017, Haziran 27). *Chernobyl's radiation monitoring system has been hit by the worldwide cyber attack*. The Independent. https://www.independent.co.uk/tech/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html

Gross, J. A. (2018, Mart 21). *Ending a decade of silence, Israel confirms it blew up Assad's nuclear reactor* [Newspaper]. Times of Israel. https://www.timesofisrael.com/ending-a-decade-of-silence-israel-reveals-it-blew-up-assads-nuclear-reactor/

Güntay, V. (2017). Uluslararasi Sistem ve Güvenlik Açisindan Değişen Savaş Kurgusu; Siber Savaş Örneği. *Güvenlik Bilimleri Dergisi,* 6(2), 2017, 81-108.

Holat, O. (2021). Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelenmesi. *Abant Kültürel Araştırmalar Dergisi,* 6(11), 2021, 105-121.

Kaspersky Securelist, A. (t.y.). *Moonlight Maze is a historic cyberespionage campaign* [Logbook]. APT Kaspersky Securelist. Geliş tarihi 14 Eylül 2024, gönderen https://apt.securelist.com/apt/moonlight-maze

Keskin, Ş. (2017). Realizm ve Liberalizm Işığında Siber Savaş ve Alternatif Bir Kavram Olarak Siber Barış'ın Değerlendirilmesi. *TURAN-SAM,* 9(35), 2017, 287-297.

Krajnyk, R. (2024, Mart 10). *# 1 - The World's Worst Computer Virus: The I Love You Virus - ZOO Repairs x* [Blog]. Zoo Computer Repairs. https://www.zoorepairs.com.au/worlds-worst-computer-virus/

Lachow, I. (2011). The Stuxnet Enigma: Implications for the Future of Cybersecurity. *Georgetown Journal of International Affairs*, 118-126.

Landler, M., & Markoff, J. (2007, Mayıs 29). Digital Fears Emerge After Data Siege in Estonia. *The New York Times*. https://www.nytimes.com/2007/05/29/technology/29estonia.html

Laughland, O., Rushe, D. (2014, Aralık 19). Sony cyber attack linked to North Korean government hackers, FBI says. *The Guardian*. https://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official

Li, S. (2023, Eylül 27). How to Prevent Email-Borne Malware: Lessons from I-LOVE-YOU Virus. *Cybersecurity Solutions | Email & Network Security*. https://abusix.com/blog/email-security/how-to-prevent-email-borne-malware-lessons-from-i-love-you-virus/

Makovsky, D. (2012, Eylül 10). *The Silent Strike | The New Yorker* [Newspaper]. The New Yorker. https://www.newyorker.com/magazine/2012/09/17/the-silent-strike

Nakashima, E. (2016, Haziran 14). Russian government hackers penetrated DNC, stole opposition research on Trump. *Washington Post*. https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html

Proofpoint. (2023, Temmuz 10). *What Is Privilege Escalation? - Definition, Types, Examples | Proofpoint US*. Proofpoint. https://www.proofpoint.com/us/threat-reference/privilege-escalation

Ranger, S. (2018, Aralık 4). *What is cyberwar? Everything you need to know about the frightening future of digital conflict | ZDNET*. ZDnet. https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

Rid, T. (2016, Ekim 20). *How Russia Pulled Off the Biggest Election Hack in U.S. History*. Esquire. https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/

Roberts, D., Jacobs, B., Yuhas, A. (2016, Temmuz 25). Debbie Wasserman Schultz to resign as DNC chair as email scandal rocks Democrats. *The Guardian*. https://www.theguardian.com/us-news/2016/jul/24/debbie-wasserman-schultz-resigns-dnc-chair-emails-sanders

Robinson, M., Jones, K., Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, (49), 2015, 70-94. https://doi.org/10.1016/j.cose.2014.11.007

Schwarz, E. (2024, Şubat 12). *Unraveling the I Love You Computer Virus on Valentine's Day—TriLeafTech*. https://trileaftech.com/i-love-you-virus-cybersecurity-lessons/

Segal, A. (2017). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age* (Second edition). PublicAffairs.

Shakarian, P., Shakarian, J., Ruef, A. (2013). Introduction to cyber-warfare: a multidisciplinary approach. Amsterdam: Morgan Kaufmann Publishers – Elsevier. s. 2.

Stark, H. (2009, Kasım 2). *The Story of "Operation Orchard": How Israel Destroyed Syria's Al Kibar Nuclear Reactor—DER SPIEGEL* [Newspaper]. Der Spiegel. https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

The UK National Cyber Security Centre. (2018, Ekim 4). *UK exposes Russian cyber attacks*. GOV.UK. https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks

The White House. (2016, Aralık 29). *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment*. Whitehouse.Gov. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

Thornburgh, N. (2005, Ağustos 29). *The Invasion of the Chinese Cyberspies*. TIME. https://time.com/archive/6674509/the-invasion-of-the-chinese-cyberspies/

Traynor, I. (2007, Mayıs 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*. https://www.theguardian.com/world/2007/may/17/topstories3.russia

Vaishnav, C., Choucri, N., Clark, D. (2013). Cyber international relations as an integrated system. *Environment Systems and Decisions*, 33(4), 2015, 561-576. https://doi.org/10.1007/s10669-013-9480-3

Yayla, M. (2013). Hukuki bir terim olarak siber savaş. *Türkiye Barolar Birliği Dergisi,* 104, 2013, 177-202.

Walker, C. (2017, Temmuz 18). *Red Alert: Russian Hackers Hit Colorado in "Moonlight Maze" Invasion*. Westword. https://www.westword.com/news/russian-cyberattacks-invaded-colorado-in-moonlight-maze-campaign-9269380

Weinberger, S. (2007, Ekim 4). How Israel Spoofed Syria's Air Defense System. *Wired*. https://www.wired.com/2007/10/how-israel-spoo/

Wikileaks. (2016). *WikiLeaks—The Podesta Emails* [Wiki]. Wikileaks. https://www.wikileaks.org/podesta-emails/

Zetter, K. (2017, Nisan 4). New Evidence Links a 20-Year-Old Hack on the US Government to a Modern Attack Group. *VICE*. https://www.vice.com/en/article/moonlight-maze-turla-link/