Siber Çatışmalar: KODLARIN SİLAHLAŞTIRILMASI

> Günümüzde büyük bir ironi olarak nükleer silahlara sahip olan ülke sayısı 10'u geçmiyorken, siber silahlara sahip ülke sayısı kesin olarak bilinmemekte ve siber silahlara sahip olan ülke sayısının nükleer silahlara sahip olan ülke sayısından çok daha fazla olduğu ileri sürülmektedir.

Emine Çelik
Necmettin Erbakan Üniversitesi
Doktora Öğrencisi

Ekim 1962'de Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) ve Amerika Birleşik Devletleri (ABD) arasında yaşanan Küba Krizi, tüm dünyanın küresel ölçekte nükleer çatışmayı yakinen hissettiği önemli olaylardan biridir. Ortaya çıkan bu nükleer tehditle birlikte ABD'deki kurumlar olası bir saldırıda iletişimin nasıl sağlanacağına, komuta ve kontrol ağının nasıl ayakta kalacağına dair fikirler yürütmeye başlamışlardır. Bu bağlamda da bilgisayar bilimcileri olan J.C.R. Licklider, Leo Beranek, Richard Bolt ve Pobert Newman, merkezi ve bağlı olmayan bir iletişim ağının oluşturulması fikrini geliştirmişlerdir. Akabinde de World Wide Web'in (www) temelleri atılmıştır.

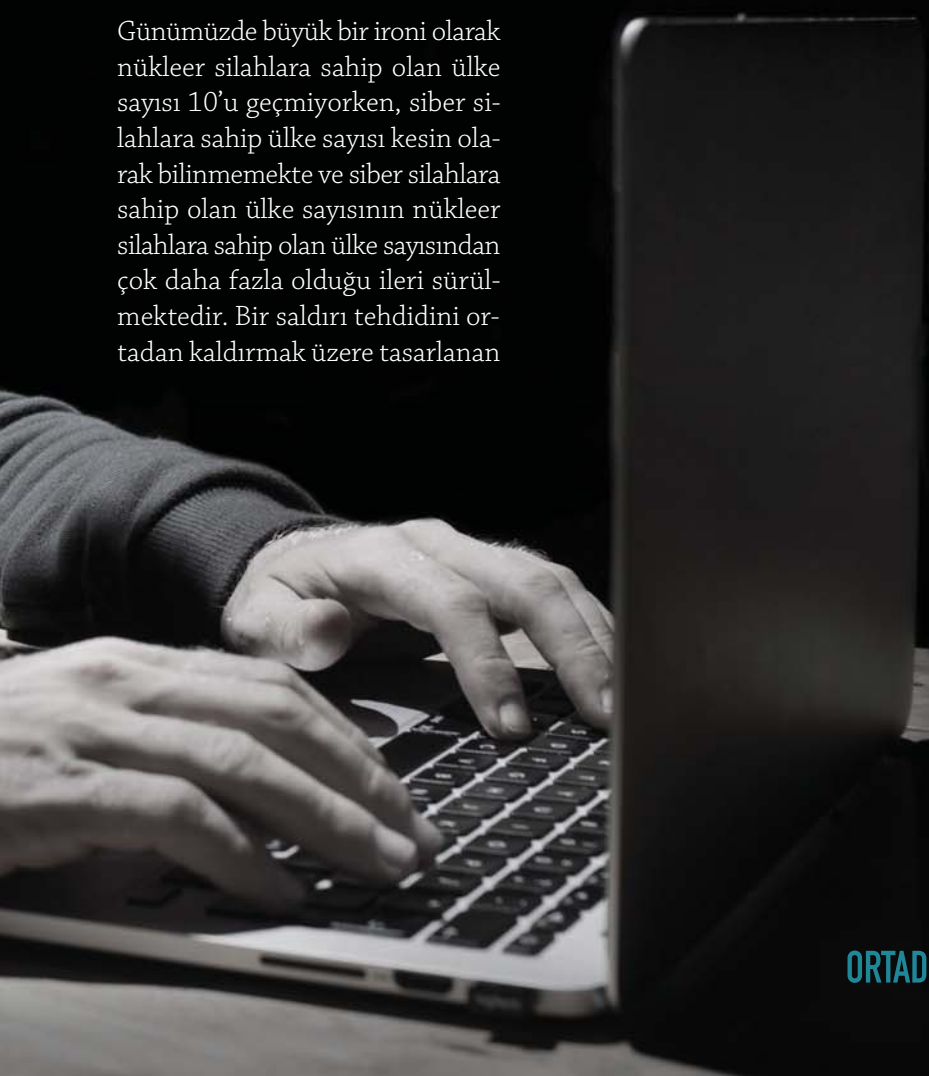
Günümüzde büyük bir ironi olarak nükleer silahlara sahip olan ülke sayısı 10'u geçmiyorken, siber silahlara sahip ülke sayısı kesin olarak bilinmemekte ve siber silahlara sahip olan ülke sayısının nükleer silahlara sahip olan ülke sayısından çok daha fazla olduğu ileri sürülmektedir. Bir saldırı tehdidini ortadan kaldırmak üzere tasarlanan sistem, yeni bir saldırı türünün ortaya çıkmasına zemin hazırlamıştır.

> **Nükleer silahların etki alanı halen ilk sırada yer alıyor olsa da siber saldırıların yeni caydırıcılık unsuru olarak kullanılması siber silahların önemini arttırmıştır.**

Annegret Dendiek ve Tobias Metzger'in de "Siber Yüzyılda Caydırıcılık Teorisi" (Deterrence Theory in The Cyber-Century) isimli çalışmalarında "Tırmanma Modeli" olarak ortaya koydukları şekilde siber silahların neden olduğu saldırıların küresel anlamda ne denli etkin olduğunu göstermektedir. Nükleer silahların etki alanı halen ilk sırada yer alıyor olsa da siber saldırıların yeni caydırıcılık unsuru olarak kullanılması siber silahların önemini arttırmıştır. Bu bağlamda, siber silahların kullanımının nükleer silahlardan sonra giderek artan bir küresel soruna dönüşmektedir.

Siber dünyanın giderek genişlemesi ve dijitalleşmenin devletler, uluslararası örgütlerin yanı sıra günlük hayatın her alanına yayılması bireysel ve sistemsel düzeyde güvenlik zafiyetlerinin ortaya çıkmasını sağlamıştır. Toplumların, "dijital toplum" haline dönüşmesi neticesinde de yapılan siber saldırılara daha açık hale geldikleri görülmektedir. Dijitalleşen toplumlarda ortaya çıkan güvenlik açıkları ise hiç şüphesiz devletler ve uluslararası aktörler tarafından bu toplumların giderek daha fazla istismar edilmelerine yol açmaktadır.

Ortaya çıkan siber saldırılarla birlikte DDoS Saldırıları (Dağıtılmış Hizmet Reddi), Dos Saldırıları (DNS Hizmet Engelleme Saldırıları) ile trojan, virüs ve worm'u kapsayan malware yazılımlar (kötü amaçlı yazılımlar) gibi terimler giderek yaygınlaşmıştır. "Siber Si-



lahlar" olarak isimlendirilen bu kavramların neden oldukları yaygın etkileri ve gelecekte nelere yol açabilecekleri ise siber silahlarla ilgili tartışmaların odak noktası haline dönüşmüştür. Tartışmalara yol açan önemli nedenlerin ilki genel olarak asimetrik savaş silahı olarak sınıflandırılan siber silahların devletler, devlet dışı aktörler, terör örgütleri ya da bireysel yapılan siber saldırılarda kullanılmasından kaynaklandığı söylenebilmektedir. Bunun yanı sıra ikinci olarak ise siber silahların kullanılmasından sonra ortaya çıkacak olan ekonomik, siyasi ve toplumsal yıkımın öngörülememesi bir diğer nedendir.

"Dijitalleşmenin önde gelen ülkelerinden olan Estonya, 2004 yılında NATO'ya siber savunma konseptini önermiştir. 2006 yılında NATO Müttefik Dönüşüm Komutanlığı (NATO Supreme Allied Command Transformation) tarafından onaylanan konsept işlevsellik kazanamadan Estonya'da gerçekleşen siber saldırı, NATO üyesi diğer ülkeleri de harekete geçirmiştir."

Yaygın etkilerinin neler olabileceğine dair yürütülen tartışmaların devam ettiği bir süreçte, 2007 yılında Rusya'nın Estonya'ya düzenlemiş olduğu siber saldırı tüm dünyanın dikkatini buraya yöneltmiştir. 2006 ile 2016 yılları arasında Estonya Cumhurbaşkanlığı

yapan Toomas Hendrik Ilves'ın Ukraine World'e verdiği demeçte, 1998'den itibaren okullarda başlayan çevrimiçi hizmetlerin akabinde vatandaşların; dijital kimliklere, çevrimiçi oy kullanma haklarına, internet üzerinden gerçekleştirilen sağlık hizmetlerine sahip olduğunu ve ayrıca vergi işlemleri gibi birçok aksiyonun da dijital olarak gerçekleştirildiğini belirtmiştir. Ayrıca Estonyalıların %95'inin de dijital bankacılığı aktif şekilde kullandığı bilinmektedir.

Dijitalleşmenin önde gelen ülkelerinden olan Estonya'ya düzenlenen saldırının arka planında ise tarihsel bir yüzleşme yatmaktadır. İkinci dünya savaşı sonrasında Sovyet Sosyalist Cumhuriyet Birliği (SSCB) tarafından temsili bir Sovyet askerinin bronz heykeli Estonya'nın başkenti Tallinn'de anıtlaştırılmıştır. 2007 yılında ise Estonya hükümeti tarafından söz konusu heykelin şehir merkezinden kaldırılacağının duyurulması, Estonya'da azınlık olarak bulunan Rusların ve dolayısıyla da Rusya'nın tepkisine neden olmuştur. Ülkede bulunan Ruslar sokaklara inerek 26 Nisan 2007 tarihinde eylemlere başlamış, akabinde binlerce kişi gözaltına alınmış, yüzlerce kişi ise yaralanmıştır. Hükümetin müdahalesinin sonrasında ise 27 Nisan'da gecesinde dünyadaki en teknolojik ülkelerden biri olan Estonya DDoS saldırısı başta olmak üzere birçok Malware'in kullanıldığı siber saldırıyla yüzleşmiştir. Rusya üzerinden gelen siber saldırı atağının hükümet yetkilileri tarafından 24 saat sonra fark edilmesi ise DDoS saldırılarının ve Malware'lerin etkisinin artmasına neden olmuştur. İlk olarak Estonya parlamentosunun e-posta sunucusu çökmüş, ülkedeki haber siteleri siber saldırıyla hükümet karşıtı haberlerle doldurulmuş, üniversitelerin web sitelerinin formatları değiştirilmiş ya da kapatılmış, banka ATMleri hizmet dışı kalmıştır. 22 gün süren siber saldırılar neticesinde Estonya siber güvenliği tam olarak sağlayamadan dijitalleşmesinin bedelini ağır ödemek zorunda kalmıştır.

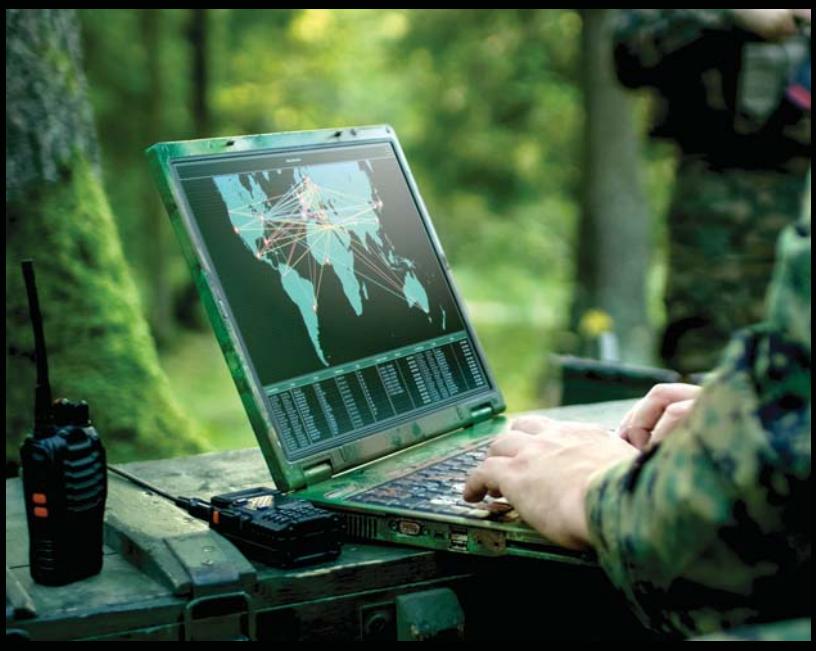
Dijitalleşmenin önde gelen ülke-

lerinden olan Estonya, 2004 yılında NATO'ya siber savunma konseptini önermiştir. 2006 yılında NATO Müttefik Dönüşüm Komutanlığı (NATO Supreme Allied Command Transformation) tarafından onaylanan konsept işlevsellik kazanamadan Estonya'da gerçekleşen siber saldırı, NATO üyesi diğer ülkeleri de harekete geçirmiştir. Bu bağlamda da 14 Mayıs 2008 tarihinde Estonya'nın girişimleri neticesinde ve NATO önderliğinde Almanya, İtalya, Letonya, Litvanya, Slovakya Cumhuriyeti ve İspanya'nın aralarında bulunduğu 6 ülkeyle birlikte Kooperatif Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence/CCDCOE) kurulmuştur. CCDCOE içerisinde günümüzde de hem NATO Müttefiki hem de ittifak dışı 21 ülke yer almaktadır.

2010 yılına gelindiğindeyse İran'a düzenlenen siber saldırıda kullanılan Stuxnet Solucanı, Estonya saldırılarından farklı olarak hizmet aksatma, erişim kısıtlama gibi siber dünya içerisinde kalan saldırıların dışına çıkmış ve siber dünyada var olması gereken bir kod parçasının fiziksel ekipmanları etkileyebilecek kapasitede olması da siber silahların tehlike düzeyini açığa çıkarmıştır.

CCDCOE bünyesinde hazırlanan "Estonya'ya Yönelik 2007 Siber Saldırılarının Bilgi Savaşı Açısından Analizi" (Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective) isimli raporda saldırının gerçekleştirildiği tarihlerde 1,3 milyonluk nüfusa sahip olan Estonya'ya dünyanın çeşitli ülkelerinde bulunan 1 milyondan fazla zombileştirilmiş bilgisayarla saldırılar düzenlenmiştir. Hackerlar saldırıların adreslerini anonim hale getirmek ve gerçekleştirecekleri saldırıların etkilerini arttırmak adına korunmasız bilgisayarlara spam e-posta ya da güvenliksiz web sitelerinden bulaştırdıkları Malware yazılımlarla bilgisayarları zombileştirmişlerdir. Bu veri göz önüne alındığında siber saldırıların gerçekleştirme şeklinin ne kadar komplike olduğu açıktır.

2010 yılına gelindiğindeyse İran'a düzenlenen siber saldırıda kullanılan Stuxnet Solucanı, Estonya saldırılarından farklı olarak hizmet aksatma, erişim kısıtlama gibi siber dünya içerisinde kalan saldırıların dışına çıkmış ve siber dünyada var olması gereken bir kod parçasının fiziksel ekipmanları etkileyebilecek kapasitede olması da siber silahların tehlike düzeyini açığa çıkarmıştır. Haziran 2010 tarihinde düzenlenen 'Stuxnet Saldırısı' siber silahların popülerliğini arttıracak bir zeminin oluşmasını sağlamıştır. Stuxnet Solucanı adı verilen 500 kilobaytlık bir Malware yazılımının kim tarafından tasarlandığı ilk dönemlerde kesinleştirilemese bile 2013 yılında ABD ve İsrail ortaklığında geliştirildiği eski NSA (National Security Agency) çalışanı Edward Snowden tarafından sızdırılmıştır. Nitekim İsrail ve ABD ortaklığında İran'a düzenlenen siber saldırıda Stuxnet Solucanı kullanıldığı ve İran'da on binleri aşan sanayi tesisinin zarar gördüğü uluslararası arenada da kabul görmüştür. Gerçekleştirilen siber saldırı İran'daki birçok sanayi tesisini etkilenmiş olsa bile Stuxnet'in asıl hedefi olan Natanz nükleer tesisi en büyük yıkımı yaşamıştır. İleri



düzeyde akıllı bir kod parçası olarak tasarlanan Stuxnet, Windows tabanlı ve santrifüjler gibi ekipmanları çalıştıran, endüstriyel kontrol sistemlerini programlamak için kullanılan Siemens Step7'a ait yazılımın işlevini bozmak üzere programlanmıştır. Nitekim Uluslararası Atom Enerjisi Ajansı'nın (The International Atomic Energy Agency /IAEA)23 Kasım 2010'da hazırlamış olduğu raporda, Stuxnet'in, Natanz nükleer tesislerinde uranyum zenginleştirmesi için çalışan 5000 santrifüjden 1000 tanesini etkisiz hale getirerek İran'ın nükleer programında en az iki yıl geriye gitmesine neden olduğunu açıklamıştır. Fiziksel hasar bağlamında değerlendirildiğinde Stuxnet Solucanı siber alanda yürütülen savaşların yalnızca dijital bilgi ve iletişimi kesmek yerine fiziksel bir yıkım getirebileceğini gözler önüne sermiştir. Dolayısıyla da Stuxnet fiziksel olarak zarar verebilen dünyanın ilk siber silahı olmuştur. İran saldırısından sonra Stuxnet gibi tasarlanan gelişmiş virüslerin usb ile bilgisayarlara aktarılması ile internetsiz ortamda bile yayılabilecekleri gerçeği ortaya çıkmıştır.

"Akıllı siber silahların bir diğer örneği ise Triton Malware'i olarak bilinmektedir. Rusya ve İran ortaklığında kodlandığı iddia edilse bile Triton'un kim tarafından tasarlandığına dair hiçbir resmi raporda açıklama bulunmamaktadır."

Stuxnet Solucanı ile siber silahların gelişiminde 3 önemli aşamaya geçilmiştir. Yeni nesil siber silahlar;

- Malware yazılımları dağıtmak ve hedefleri belirlemek için siber dünyayı kullanabilmektedirler.
- Fiziksel zararlarda etkin olabilmek adına süreçleri kontrol etmek için ilgili katmanları kullanabilmektedirler (Natanz'da Siemens'in PLC bilgisayarları kullanması örneğinde olduğu gibi).
- Fiziksel katmanlara etki ederek, siber dünya dışında gerçek hayatta zarar verebilen bir kod parçası olarak kendilerini aktive edebilmektedirler.

Akıllı siber silahların bir diğer örneği ise Triton Malware'i olarak bilinmektedir. Rusya ve İran ortaklığında kodlandığı iddia edilse bile Triton'un kim tarafından tasarlandığına dair hiçbir resmi raporda açıklama bulunmamaktadır. Triton, dünyanın en büyük petrol şirketi olan Suudi Aramco'da endüstriyel felaketi önlemek üzere süspansiyon görevini üstlenen bilgisayar sistemine saldırmak üzere tasarlanmıştır. Ağustos 2017 tarihinde kritik altyapıyı koruyan güvenlik sistemine saldırı düzenlemeyi amaçlayan Triton yapısındaki bir kod hatası yüzünden başarıya ulaşamamıştır. FireEye güvenlik şirketinin verilerine göre Triton, Alman Shneider Electric firması tarafından üretilen, Triconex olarak bilinen ve dünyanın her yerinde kullanılan, acil durumlarda sistemi kapatma işlevi sağlayan bir güvenlik sistemine saldırmıştır. Bahsi geçen güvenlik sistemi, olası basınç farklılığı, sıcaklık artışı gibi Suudi Aramco'daki endüstriyel fabrikaların hayati fonksiyonlarının korunmasına yönelik kullanılmaktadır. Triton kodlarının aktif şekilde çalıştırılmasının akabinde de FireEye güvenlik şirketi petro-kimya ürünlerinin tesislerden sızdırılması ya da büyük bir patlamanın söz konusu olabileceği yönünde görüş bildirmişlerdir.

The New York Times'da yayınlanan "Suudi Arabistan'daki Bir Siber Saldırının Ölümcül Bir Hedefi Vardı. Uzmanlar Başka Bir Denemeden Korkuyor" (A Cyberattack in Saudi Arabia Had a Deadly Goal.

Experts Fear Another Try)" isimli makalede Suudi Aramco tesisinde kullanılan Triconex'in dünya genelindeki 18 bin tesiste kullanıldığı vurgulanmıştır. Triton Malware'in Triconex kontrol cihazlarına saldırması için kodlanması ise dünyanın herhangi bir yerindeki petro-kimya tesislerinde ortaya çıkarabileceği tehlikeyi gözler önüne sermektedir.

Devletlerin, devlet dışı aktörlerin maruz kaldıkları siber saldırılar sonucunda yeni bir siber silah daha üreterek siber güvenliklerini arttırmak adına yaptıkları yatırımlara bakıldığında, savaşların alışılagelmiş şekliyle konvansiyonel savaş sahaları yerine asimetrik bir savaş şekli olarak, ülkelerin bankalarına, iletişimlerine, elektrik şebekelerine, doğalgaz boru hatlarına ve endüstriyel tesislerine yönelik yapılacak saldırılara doğru evirildiğini söylemek mümkündür.

24 Saat İçerisinde Gerçekleştirilen Siber Saldırılar

Stuxnet Solucanı'nın Natanz'da gerçekleştirmiş olduğu eylem, siber dünyada siber silahların tamamen farklı bir alana evirilmesine neden olmuştur. Öyle ki Stuxnet siber-fiziksel sistemleri hedef alarak siber silahların fiziksel dünyada nasıl hasar vereceğini göstermiştir. Bununla birlikte siber silahların kullanımıyla ilgili devletlerin ve devlet dışı aktörlerin GPS güdümlü füzeler, nükleer silahlar gibi gelişmiş silahların etkileşime geçirilmesi söz konusu olabileceği yaygın kanaatler arasında yerini almıştır. Dolayısıyla da ulus devletlerin, devlet dışı aktörlerin ve hatta siber suçluların ve teröristlerin siber-fiziksel dünyada ortaya çıkarabilecekleri siber tehditlerin ve savaşların kapısını aralamıştır.

> **"IP yanıltmaları ile başka ülkeler üzerinden gösterilmesi ya da saldırıların kaynaklarının birçoğunun anonim olarak kalması siber saldırıya maruz kalan ülkelerin muhatapsız kalmasıyla sonuçlanmaktadır."**

Son olarak uluslararası sistem içerisinde siber silahların kullanımının önlenmesine dair işbirliğinin gerçekleştirilememesi ise siber silahlanmanın artan bir ivme sergilemesine neden olduğu söylenmektedir. Ayrıca devletlerin konvansiyonel savaş yerine, anonim olarak birbirilerinin finansal sistemleri, endüstriyel tesisleri, elektrik şebekeleri, askeri yapıları, silah ve güvenlik sistemleri gibi hayati alanlarına zarar verebilmesi sıradan insanların hayatlarını da etkileyecek şekilde değişmiştir. Bununla birlikte yapılan siber saldırılarının kaynağının en basit yöntem olarak IP yanıltmaları ile başka ülkeler üzerinden gösterilmesi ya da saldırıların kaynaklarının birçoğunun anonim olarak kalması siber saldırıya maruz kalan ülkelerin muhatapsız kalmasıyla sonuçlanmaktadır. Saldırı kaynağının kesin olarak tespit edilememesi ulusların dost düşman kavramının değişime uğramasına neden olmakla birlikte ulusların siber silah edinmelerinin önünü açmakta ve aynı zamanda da siber silahların kullanımının durdurulamamasına, yenilerinin üretilmesinin önüne geçememektedir.