Atıf - Reference: Holat, Olcay (2021) Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelenmesi. *Abant Kültürel Araştırmalar Dergisi*, 6(11): 105-125.

Araştırma makalesi / Research article

Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelenmesi [i]

Olcay Holat[*]

Öz

Zaman ve mekân sınırlarını bulanıklaştıran yeni medya, günümüz bilişim dünyasını da hızla değiştirmektedir. İnternet ile birlikte gelişen etkileşim ağı, kurumsal ve bireysel düzeyde riskleri ve olası tehditleri de ortaya çıkarmaktadır. Tehditlerin yaygınlığının ve türlerinin artması, yapılarının ve yönlerinin değişmesi, ulusal ve küresel çapta birçok önemli kuruma ait kritik alt yapıların ve gizli bilgilerin hedef haline gelmesi, karar alıcıların karşısına yeni bir mücadele ve savaş alanı çıkarmıştır. Bu çalışma, gelişen iletişim teknolojilerine paralel olarak siber saldırılardaki gelişimi, Stuxnet saldırısı üzerinden incelemektedir. Araştırmada örnek olay analizi yöntemi kullanılmaktadır. Çalışma kapsamında incelenen Stuxnet saldırısında, devlete ait kritik altyapıların hedef alınabileceği ve ulusal güvenliğin tehdit altında olabileceği görülmüştür. Bu çerçevede, ağların güvenliğine yönelik etkili mücadele yöntemlerinin geliştirilebilmesi için uluslararası bir iş birliği ve dayanışmanın giderek önem kazandığı vurgulanmaktadır.

Anahtar kelimeler: Yeni medya, siber ortam, siber savaş, siber güvenlik, Stuxnet Saldırısı

Investigation of Stuxnet attack example in the context of new media and cyber war concepts

Abstract

New media, which blurs the boundaries of time and space, is also rapidly changing today's IT world. The network of interaction that develops together with the Internet also reveals risks and possible threats at the corporate and individual levels. The increase in the prevalence and types of threats, the change in their structures and directions, and the targeting of critical infrastructures and confidential information of many important institutions on a national and global scale have created a new fight and battlefield for decision-makers. This study examines the evolution of cyber-attacks in parallel with developing communication technologies through the Stuxnet attack. The case study analysis method is used in the research. The Stuxnet attack, which was examined as part of the study, showed that critical state-owned infrastructure could be targeted, and national security could be threatened. In this context, it is emphasized that international cooperation and solidarity are becoming increasingly important to develop effective methods of combating the security of networks.

Keywords: New media, cyber environment, cyber war, cyber security, Stuxnet attack

[*] Öğr. Gör., Ege Üniversitesi Uzaktan Eğitim Uygulama ve Araştırma Merkezi, olcayholat@gmail.com, ORCID: 0000-0002-8242-1719

Geliş tarihi - Date of reception: 22.06.2020
Kabul tarihi - Date of acceptence: 10.03.2021

Giriş

Bilgisayar teknolojilerinin uzantısı ve geliştiricisi olarak internet olgusu, dünya üzerinde insanoğlunun kurduğu en büyük ağ (network) olma özelliğini göstermektedir. Bu küresel ağın eski teknolojilerden ayrıldığı noktalardan biri, birbirinden kilometrelerce uzaklıktaki bilgisayarların, birbirine bağlı olması koşulunu yerine getirmesidir. Dolayısıyla uzamsal farklılıkları aşan kullanıcı; dâhil olan, etkileyen ve her daim etkiye açık olan yeni bir bireyin ve bu birey etrafında şekillenen çevrim içi toplumsal yapılanmanın doğmasına neden olmuştur. "Sanallığa dayalı bu toplum modeli, bugüne kadar görülmemiş bir düzeyde yayılma ve örgütlenme imkânı sunarak, bir anda birçok insanın 'çevrim içi bir arada' bulunmasını sağlayabilmektedir" (Göker ve Doğan, 2011: 177).

21. yüzyılda gelişen iletişim teknolojileri karşısında, geleneksel medya kadar yeni medya araçları da güç kazanmıştır. Yeni medya ile birlikte tüm dünyada kitleler, birbirlerine iletişim araçlarıyla bağlanmaktadır. Bu noktada, teknolojik gelişmişlik seviyesi yükseldikçe, ülkelerin ekonomik yaşamları, ulusal ya da uluslararası altyapıları ve toplumsal yaşamları daha çok dijitalleşmiştir. Bu bağlamda, teknolojik gelişmelerin yeni bir bakış açısı getirdiği alan ise terör ve savaşlardır. Günümüzde siber ortamın kendisi de beşinci boyutta bir savaş alanı haline gelmiştir.

Yeni medyaya yönelik kavramsal çerçeve

Yeni medya kavramı ilk olarak 1970'li yıllarda enformasyon ve iletişim alanlarında kullanılan ve ortaya atılan bir kavramdır. Yeni medya; bilgisayar, elektronik posta, sanal gerçeklik, multimedya, yazılım, web siteleri, sosyal medya, podcast, video blog (vlog) vb. gibi gittikçe gelişen ve değişen birçok iletişim aracını bünyesinde barındırmaktadır. Yeni medyanın özellikleri arasında sesin, verinin, metnin ve görüntünün tek bir altyapı üzerinden aktarılabilmesine, saklanabilmesine, toplanabilmesine ve işleme tabii tutulabilmesine imkân tanıyan sayısallaştırma bulunmaktadır. Sayısallaştırma, enformasyonun içerisinde bulunduğu doğal yani analog halinden bilgisayarlar tarafından okunabilir bir formata dönüştürülmesidir. Sayısallaştırmanın yeni medyaya sunduğu en büyük avantaj ise sayısallaşmış enformasyonun elektriksel değerler şeklinde ifade edilmesinden dolayı elektronik cihazlar tarafından kullanılabilmesi, birbirine dönüştürülebilmesi ve kolayca bir ortamdan diğer bir ortama aktarılabilir olmasıdır (Manovich'den aktaran Aktaş, 2007: 2). Sayısallaştırma, teknolojinin gelişimine bağlı olarak iletişim teknolojilerini de büyük ölçüde dönüşüme uğratmıştır.

Küreselleşme, teknolojinin ve onları bağlayan iletişim ağlarının hızlı bir şekilde gelişmesiyle işlevsel anlamda etkili olmaya başlamıştır. Bu sürece işlevsellik ve hız katan, internet ve yeni medyadır. Küreselleşmenin sosyal, ekonomik, politik alanlardaki ilerlemesi, bu iletişim araçlarındaki kullanım gücüyle gerçekleşmektedir. Dolayısıyla, küreselleşmenin daha yaygın ve geçerli olabilmesi için, tüm dünyanın iletişim ağlarıyla birbirlerine bağlanması ve etkileşim içinde olması en önemli koşullardan biridir. Zaman ve mekânın sınırlarını ortadan kaldıran yeni medya olanakları, kültürel ve coğrafi olarak sınırları aşarak, küreselleşmenin yaygınlaşmasında önemli bir rol oynamıştır. Zira ülkeler arası sınırların kaldırılmasıyla birlikte, kültürler arasında etkileşimin hızı ve kapsamı da artmıştır.

M. McLuhan, 1960'lı yıllarda öngördüğü "küresel köy" yaklaşımında, kitle iletişim araçlarının kullanımının yaygınlaşması ile dünyanın küresel bir köye dönüşeceğini savunmaktadır. McLuhan köy kavramını, bilinen kırsal kesim yerleşim alanı olarak değil

teknolojinin yönlendirdiği, insanların evlerine kapanıp ekranlar aracılığıyla iletişim kurdukları yeni nesil elektronik bir yaşam formu olarak tanımlamıştır. Günümüzde internet ve yeni enformasyon teknolojileri aracılığı ile sanal ağlarda yaşayan insanlar, iletişim teknolojilerinin sunmuş olduğu olanaklar sayesinde, her türlü enformasyona kolayca ulaşabilmektedir. Bu bağlamda, dünyanın küresel bir köye dönüşmesi ile birlikte fiziki sınırlar ortadan kalkarak, bilgi akışının çok daha hızlı bir şekilde ilerlediği yeni bir dünya düzeni ortaya çıkmıştır (McLuhan, 2001). Özellikle, internetin istenilen her veriyi eşit hızda, istenilen her yere ulaştırma özelliği ise bir anlamda McLuhan'ın küresel köy kavramının karşılık bulması için en önemli aktörün, internet teknolojisi olduğu gerçeğini de ortaya çıkarmıştır.

McLuhan (2001: 157); "yeni teknolojik insan, bütüncüllüğüne ve kapsamlılığına doğru yarışırken, eski zamanlarda olduğu gibi bir vahşi doğa deneyimine sahip olmayacak. Teması kaybedecektir" demektedir. Bu bağlamda, McLuhan doğa deneyimi ile teknolojik deneyim arasındaki farka dikkat çekerek, temasın kaybedildiği yeni bir sanal evrenden söz etmektedir. Zira bireylerin zihinlerindeki gerçek ve kurgusal dünya yer değiştirerek, algılamalarının boyutu değişecektir. Mekânsal ve zamansal anlamda bedeni sanal evren içerisinde olan birey, tehlikeli olabilecek şekilde enformasyona maruz kalabilmektedir. McLuhan'a göre:

> İster evde, ister iş yerinde olsun, enformasyon odasında oturup dünyanın her bölgesinden gelen verileri anormal hızlarla almanın -imajlar, ses ya da dokunma halinde- sonuçları, tehlike yaratacak kadar şişirici ya da şizofrenik olabilir. Bedeni bir yerde olacak, ama zihni veri bankasının her yerinde tek bir anda olmak üzere elektronik bir boşluk içinde yüzecektir (McLuhan, 2001: 207-208).

İletişim teknolojilerinin geldiği bu noktada, M. Castells'in "ağ toplumu" kavramı önemli görülmektedir. Castells'e (2005) göre; "bireyler artık küresel ve yerel olarak örülmüş, birbirleriyle bağlantılı ağlar içinde yaşamaktadır." Günümüzde internet teknolojisinin gelişmesiyle birlikte, dünya üzerinde internet ağı ile bağlanan insanların iletişim ve etkileşim süreçleri de ağ toplumu kavramının yaygınlaşmasında etkili olmuştur. Castells'e göre ağ toplumunun en belirgin karakteristik özellikleri zaman ve mekân kavramlarında ortaya çıkmaktadır. Ağ toplumunda zaman dışı zaman ve akışlar uzamı vardır (Castells, 2000: 13):

> Ağ toplumunun en belirgin özelliği zaman ve mekân kavramlarındaki değişimdir. Zaman kavramının genişletilmiş ve yok sayılabilen özelliğine göndermede bulunurken, mekânın da coğrafi sınırlardan ve uzaklıklardan arındırılarak teknolojik imkânlarla aşıldığını anlatmaktadır. Zira enformasyon teknolojileri sayesinde yeni bir zaman ve uzam algısı yaratılmış olmaktadır. Bu nokta da bir önemli kavramda ağ toplumunda etkileşimin varlığıdır (Göker ve Doğan, 2011: 178-179).

İnteraktif bilgisayar ağları, yeni iletişim biçimleri ve kanalları yaratarak, hayatı şekillendirmeye devam etmektedir. İki yönlü iletişime bağlı süreç içerisinde, özellikle bireyler sosyal medya araçlarıyla birbirleriyle etkileşim içerisindedir. Castells; "artık kimliklerimizi geçmişimizden almıyoruz; kimliklerimizi başkaları ile etkileşime girerek yaratmak zorundayız" demektedir. Toplumlarımız giderek ağ ile benlik arasındaki çift kutuplu bir karşıtlık etrafında yapılandırılmaktadır (Castells, 2005: 2-4). Dijitalleşen dünyada etkileşimin, kimlik yaratma sürecinde önemli bir etken haline geldiği ve kimlik temsillerinde baskın bir rolü olduğu görülmektedir. Bu bağlamda, ağ toplumunda yaratılan yeni kimliklerimiz, küresel bir etkileşimi de beraberinde getirmektedir. Özellikle birbirleriyle bağlantılı ağlar içerisinde yaşayan toplumların, ulusötesi bir

boyutta bir etkileşim içerisinde olması, ağ toplumunun önemli özellikleri içerisinde yer almaktadır.

Ses, görüntü, veri ve bilgi dolaşımı, internet ve sayısal teknolojilerle birlikte giderek hızlanmıştır. Yeni medya çağının oluşumunu sağlayan siber iletişim araçları yaşamsal nitelikleri de değiştirmeye başlamıştır. Yaşamın her alanı dijital teknolojiye bağlı olarak gelişen, dijital iletişim biçimleriyle değişmektedir. 2000'li yılların "yeni medya çağı" adını almasının en önemli nedenleri arasında, teknolojik gelişmelerin kitleleri yönlendiriyor olması yatmaktadır. Küreselleşmenin etkisi ve büyük ölçekli uluslararası şirketlerin güç kazanması yeni medya çağının oluşumunu hızlandıran diğer önemli faktörlerdir (Baudrillard, 2004: 19). Zira yeni medya çağında teknolojik gelişmelere bağlı olarak toplumsal yapıda dönüşüme uğramaktadır.

Teknolojik gelişmelerin toplumsal yapı üzerindeki etkisine vurgu yapan Castells (2005: 8-9), toplumların stratejik açıdan belirleyici olan bazı teknolojik kabiliyet özellikleri onların kaderlerini doğrudan etkilemektedir. Var olan teknolojinin ya da yoksunluğunun ortaya çıkardığı kabullenme ve uygulama sürecinde, oluşan kullanım tarzları ve toplumların bu süreçte kendilerini dönüştürme biçimlerinin, tarihsel evrim ve toplumsal değişim üzerinde belirleyici bir role büründüğü görülmektedir.

Yeni medya çağında riskler ve tehditler

Bilgi ve iletişim teknolojilerinde yaşanan gelişmelerle ile birlikte ortaya çıkan küreselleşme sürecinde yeni bir sosyal, siyasal, ekonomik ve kültürel değişim yaşanmaktadır. Gelişen teknolojilerin insanlığa sunduğu olanaklar beraberinde birçok riskleri de getirmiştir. Teknolojideki bu gelişmeleri yakından takip eden organize suç ve terör örgütleri, hem siyasi ve ekonomik kazanımlarını arttırmakta hem de geleneksel terör ve savaş türlerinin dışında yeni saldırı teknikleri geliştirmektedir. Virüs kavramının vücudumuzun dışına çıkarılarak sanal mikroplar haline dönüştürülmesi, bilgisayarlara, iletişim ve telekomünikasyon hizmetlerine bulaştırılarak sosyal hayatın felce uğratılması gibi birçok yeni risk ve tehdit türleri ortaya çıkmıştır (Kara vd., 2006: 2). Bu bağlamda, özellikle yeni medya araçlarıyla birlikte kullanıcıların çevrim içi hale geldiği ve tüm kimlik, güvenlik vb. bilgilerinin siber ortama aktarıldığı bir dönemde, teknoloji artık bir korku ve tehdit unsuru da olmaya başlamıştır.

Modernite sonrası risk ve tehdit unsuru değişmiştir. U. Beck, modern sonrası dönemi "risk toplumu" olarak ele almaktadır. Beck'e göre riskler, bireyin hayatının her alanına yayılmıştır. Riskler, önceden bilinemeyen, öngörülemeyen ve tanımlanamaz bir yapıdadır. Doğal olarak risklere karşı tedbir almak zordur. Riskler belirli coğrafyalarda ortaya çıksa da, tüm dünyaya yayılarak evrenselleşmektedir (Koçak ve Memiş, 2017: 257). Beck, modernleşme ile meydana gelen risk toplumunu, yaşanması gereken ve kaçışı olmayan bir süreç olarak görmektedir. Bu nedenle, bireyler ve toplumlar bilinçli ya da bilinçsiz birçok risk ve tehlikelerle yüz yüzedir. Risk ve tehlikelerin yönetilmesi zorlaşmaktadır (Beck, 1992: 42). Gelinen risk toplumunda, öteden beri var olan risklerin çok daha farklı şekillerde ortaya çıkıp bütün toplumu kuşattığı ve tehdit ettiği görülmektedir. Bu konu hakkında Beck, küreselleşen risklerin, sosyal medya yoluyla risk algısı yaratılarak varlığını sürdürdüğünü söylemektedir (Beck, 2009: 39). Özellikle siber ortamda yaratılan risk algısı, Beck'in öngördüğü risk toplumunun da bir uzantısıdır.

Castells *İsyan ve Umut Ağları İnternet Çağında Toplumsal Hareketler* (Networks of Outrage and Hope: Social Movements in the İnternet Age-2013) adlı kitabında, günümüzdeki toplumsal hareketlerin değişimi ve ortaya çıkışları üzerine incelemeler

yapmıştır. Özellikle ağ toplumunda, insanların toplumsal değişim için hareket süreçlerinde, ortak noktanın internet olduğunu söylemektedir. İnternet, devlet ve sermaye kontrolü dışında bir özgürlük alanı olarak görülmektedir. Bu çerçevede, analizlerinde örneklem olarak kullandığı Tunus ve İzlanda toplumsal hareketlerinde, farklı coğrafyalarda siber uzam ağları ile kent uzamı arasındaki geçişlerin benzer nitelikte olduğunu gözlemlemiştir. Göstericiler oluşturdukları hashtag ile "devrimin bir etiketini" ortaya çıkarmış ve her iki ülkede sembolik kamusal meydanların işgal edilmesi ile birlikte hareket, siber uzamdan kent uzamına geçiş yapmıştır (Castells, 2013). Tunus'ta yaşanan toplumsal olaylar ve teknoloji arasında bir ilişki vardır. Buna göre Tunus'ta yaşanan olaylar sırasında "olayların ve koordinasyon eylemlerinin tartışılmasında" Twitter önemli bir rol oynamaktadır. Castells bu noktada Tunus'un Arap Dünyasında internetin ve cep telefonlarının yaygınlık oranının en yüksek ülkelerden biri olduğunun altını çizer. İzlanda örneğinde Castells ülkenin ekonomisine ilişkin değerlendirmelerde bulunur. Burada başlayan ve yine internet üzerinden yayılan olayların sonuçlarına odaklanır (Castells, 2013: 41-52). Kitleler çoğunlukla siber uzamda örgütlenerek, kent uzamında toplumsal harekete başvurarak, değişim için çare aramaktadır. Castells, Tunus ve İzlanda'da gerçekleşen toplumsal olayları şu şekilde açıklar:

> Tunus ve İzlanda'nın ortak özellikleri nedir? Buna göre her iki ülkedeki hareketleri başlatan ciddi olaylar olmuştur. İzlanda'da yaşanan finansal kriz ve Tunus'ta Buazizi'nin kendisini yakması bu olayların başlangıç referansları olarak sayılabilir. Her iki ülkede gelişen olaylarda cep telefonları ve internetteki sosyal ağlar tartışmadan eyleme kadarki süreçte etkili olmuştur. Ayrıca her iki ülkede sembolik kamusal meydanların işgal edilmesi ile birlikte hareket siber uzamdan kent uzamına taşınmıştır (Castells, 2013: 53).

Yeni medya çağında temel sorunsallardan biri, "interneti kim yönetiyor?" sorusudur. V. Dijk (2012), internetin yönetimi için birbiri ile yarışan dört tarafın; hükümetler, internet toplulukları, şirketler, yazılımı ve güvenliği tasarlayan kişiler olarak belirlemiştir. Özellikle üretimin ve dağıtımın paydaşlarının, internet üzerindeki kontrol mücadelesinde baskın bir rolde olduklarını vurgulamıştır. Bu mücadelenin tarafları olan "Microsoft, Apple, Google, Facebook, Twitter vb." gibi monopol şirketlerin karşısında, tüketicilerinde etkin bir role sahip olduğuna değinmiştir. Ancak internet, pozitif anlamda kullanıldığı kadar, çeşitli amaçlar için kötüye kullanılma riskini de taşımaktadır. Bu bağlamda, kendi çıkarları amacıyla interneti ve yeni medya araçlarını kullanabilecek terör örgütü mensupları, gelecek yüzyıllarda siber ortam için en büyük tehlikelerden biri olacaktır.

Bilişim teknolojilerinin günden güne gelişmesi, internetin sunduğu avantajların yanında bazı tehlikeleri ortaya çıkardığı görülmektedir. Bu risk ve tehditler çevrim içi gizlilik kavramının gündeme gelmesini beraberinde getirmiştir.

> Çevrim içi gizlilik kavramı; internet üzerinde istemli ya da istemsiz bir şekilde paylaşılan kişisel bilgilerin mahremiyeti ve güvenlik seviyesi ile alakalı bir kavramdır. Örneğin, bir e-ticaret sitesinden alışveriş yaptığımızda girdiğimiz kredi kartı bilgileri veya herhangi bir internet sitesine ya da sosyal ağa üye olurken girdiğimiz kişisel verilerin güvenliği; bu verilerin kötü amaçlar için üçüncü şahısların eline geçmesi ya da çalınması vb. kaygıları tanımlayan bir kavramdır. Çevrim içi gizlilik konusu, internet üzerinde yapılacak birçok aktivite ve atılacak birçok adımda kaygılara sebep olmaktadır. İnternette bir faaliyet içinde yer almadan önce düşünmemize sebep olmaktadır (Techopedia, 2018).

Günümüzde devletlerin birer e-devlet halini aldığı, bankacılık işlemlerinin internet bankacılığı sistemleri aracılığıyla web tabanlı ya da mobil uygulamalar aracılığıyla yapıldığı bir dönem yaşanmaktadır. Sağlık bilgilerimizin tamamı web ortamlarında saklanabilirken, kişisel kredi kartı bilgileri de çalınabilme tehlikesiyle karşı karşıya

kalmaktadır. Nüfus cüzdanı bilgileri, ehliyet ve pasaport bilgileri, iş yeri ve konum bilgileri, kurum ya da maaş (e-bordro) bilgileri gibi paylaşılması risk taşıyan bilgiler çevrim içi gizlilik konusunu gündeme taşımaktadır. Bu bağlamda, siber ortam güvenliliğinin sadece devletler açısından değil, bireysel yaşamda insan yaşamını tehdit edebilecek birçok boyutu olduğu görülmektedir. Kişisel verilerin güvenliği sorunsalının gelecek yıllarda siber ortam güvenliğinin en temel konularından biri olacağı öngörülmektedir.

Siber ortamın bir risk ve tehdit olabileceği gerçeği, yeni yüzyılda terörizmin yeni bir yüzü olarak yansımasına neden olabilmektedir. Teröristlerin elektronik bir saldırı yaparak; bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, elektrik ve doğalgazı kapatabilecekleri ihtimalleri bulunmaktadır. Özellikle siber terör ile elektrik santrallerinin devre dışı bırakılması ya da nükleer santrallerin kontrollerinin ele geçirilerek potansiyel bir atom bombasına dönüştürülmesi gibi toplumsal yaşamı önemli ölçüde etkileyebilecek teknolojik saldırılar düzenlenebilmektedir. Zira tüm bu koşullar altında siber savaş ve terör konularının araştırılmasına yönelik gereklilik doğmaktadır.

Siber savaş kavramı

İnsanoğlu ilk zamanlarda “kara” ve “deniz” olmak üzere bir birinden çok farklı özellikler gösteren iki alanda savaşmıştır. Hava teknolojisinin gelişmesi ile birlikte üçüncü savaş ortamı “gökyüzü” olmuştur. 20. yüzyılın ikinci çeyreğinde dördüncü savaş ortamı “uzay” olarak kabul edilmiştir. Bu dört savaş ortamının da kendine has özellikleri ve gereklilikleri bulunmaktadır (Yayla, 2013: 183). 21.yüzyılda teknolojik gelişmeler sonucunda güvenlik parametreleri değişmiş; kara, deniz, hava ve uzay yanında beşinci bir savaş ortamı “siber ortam” olarak kabul edilmiştir. Siber ortam diğer boyutlardan radikal biçimde farklılaşan karakteristik özelliklere sahiptir. En önemli özelliği dört fiziksel boyutun yanında karmaşık ilişkiler ağına sahip olmasıdır. Öte yandan sınırları çizilemeyen, tanımlanması zor bir alandır. Siber ortamda yapılan saldırılara karşı mücadeleler oldukça güç olup, tek bir devletin kapasitesini aşmakta ve ortak mücadeleyi zorunlu kılmaktadır (Polat, 2020: 135). Bu süreçte küresel bir iş birliği, risklere ve tehditlere karşı önemli görülmektedir. Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization-NATO) 15 Haziran 2016'da siber savaş ortamını savaşın operasyonel bir alanı olarak resmen tanımıştır. NATO siber savaş ortamına yönelik mücadele stratejileri ve planları yapmak için çalışmalar yürütmektedir.

Siber savaş; bilişim sistemleri doğrultusunda, elektronik araçların, bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla, ulusal denge ve çıkarların tahrip edilmesini amaçlayan, kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinlikler olarak tanımlanabilmektedir (Kara vd., 2006: 2). Siber savaş, kuralsız bir şekilde siber silahlar kullanılarak yürütülen asimetrik veya hibrit yaklaşımların kullanıldığı savaş şeklidir. Askeri yapıların tek başına değil sivil altyapılar ile bağlantılı olması nedeniyle siber uzaydaki bu saldırıların, askeri yapılarla sınırlı kalmadığı da bir gerçektir (Ottis, 2011: 178). Siber savaş nedeni sayılabilecek saldırının gerisindeki saldırgan devlet, örgüt ya da bilgisayar korsanı (hacker) genellikle tespit edilememektedir. Siber dünyanın bazı karakteristik özellikleri, siber eylemlerin bir devlete isnat edilebilirliğini oldukça güçleştirmektedir. Siber harekâtların anonim olarak farklı ülkelerden, farklı bilgisayarlar kullanılarak gerçekleşmesi eylemlerin arkasındaki esas gücün tespitini oldukça zorlaştırmaktadır. Saldırının kaynağının yani kullanılan

bilgisayarın hatta onu kullanan kişinin tespit edilmesi, saldırıyı bir devlete isnat etmek için yeterli olmamaktadır (Gümüşbaş, 2016: 188). Siber ortam üzerinden yapılan saldırılar için siber savaş ya da terör tanımlaması yapılabilmektedir. Her iki kavram da literatürde birbiri yerine kullanılabilmektedir.

Siber savaş ile siber terör kavramlarını birbirinden ayırmak oldukça zordur. Geleneksel uluslararası hukuka göre savaş kavramının tanımlanabilmesi için şu kriterler aranmaktadır: a) iki veya daha fazla devlet arasında gerçekleşmesi, b) ilan edilmesi, c) tarafların amacı ve niyetinin ortaya konulması, d) çatışmaların süresi ve yoğunluğu. Savaşan tarafların niyeti ne olursa olsun, savaş ilan edilsin ya da edilmesin, eğer çatışma varsa, uzun süredir devam ediyorsa ve yoğunluğu buna uygunsa bir çatışmanın savaş olarak kabul edilebileceği ileri sürülmüştür. Kısaca savaş, silahlı güçler tarafından yürütülen bir çatışmadır ve taraflar arasında bir silahlı çatışmanın bulunması şarttır (Keskin, 1998: 68). Terör ise siyasi amaçlar için örgütlü olarak sistemli ve devamlı terör kullanmayı metot olarak kullanan ve bir strateji anlayışı olarak ya da insanları yıldırmak sindirmek yoluyla onlara belli düşünceleri benimsetmek için zor kullanma ya da tehdit eylemi olarak tanımlanmaktadır (Bozdemir, 1982: 526). Savaşlar çoğunlukla tanımlanmış ve resmi devletler arasında gerçekleşirken, terör eylemleri yasa dışı veya terör örgütleri tarafından gerçekleştirilmektedir.

Siber savaş, kendi içinde birçok yöntem ve teknik barındırmaktadır. Siber savaşta kullanılabilecek çalışma alanları vardır. Casusluk, manipülasyon, propaganda, iletişimin kontrol altına alınması, virüs ve Truva atlarıyla sistemlerin bozulması, siber bombalarla sabotaj, sistem kilitleme, dolandırıcılık, bilgi kirliliği gibi birçok alan siber savaşın oluşumuna katkı sağlamaktadır (Kara, 2013: 40). Çeşitli amaçlarla kontrolü ele geçirmek için bilgileri çalmak, değiştirmek, içine sızmak bu sürecin günümüzde en etkin mekânizmaları arasında yer almaktadır.

Siber saldırılar çeşitli kategorilere ayrılmaktadır. Siber saldırı ataklarının birinci kategorisi, "basit ve yapılandırılmamış" olanlardır. Genelde hedef ayrımı yapmayan, çok hızlı ve etkili yayılarak büyük zararlar veren solucan *(worm)* virüsler, bu kategori altında toplanmaktadır. Son yıllarda bu virüslerin birçok saldırıda kullanıldığı görülmektedir. İkincisi, çoklu sistemlere karşı, daha karmaşık atakları içeren "ileri düzeyde yapılandırılmış" olanlardır. Bu kategorideki saldırılar önceden planlanarak, uzun çalışmaların ürünü olarak gerçekleşmektedir. Üçüncü olarak ise, "karmaşık koordinasyona sahip ataklar" söz konusudur. Bu ataklar, çok ileri düzeyde yapılmış hedef analizlerine, üstün zekâ ve denetime sahiptir (Atıcı ve Gümüş, 2003: 58). Kendi içerisinde özelliklerine göre kategorileştirilen bu saldırı türleri, teknolojinin gelişimine bağlı olarak değişmekte ve gelişmektedir.

Geleneksel savaş ile siber savaş arasında önemli farklılıklar bulunmaktadır. Siber savaş sürecinde herhangi bir yaşamsal riski olmadan (şu ana kadar bilinen saldırılar doğrultusunda) etkili bir saldırı gerçekleştirilebilmektedir. Top, tüfek, silah, bomba ile gerçekleştirilen savaşlar kadar düşmanın silahı; virüsler, yazılımlar ve bilişim teknolojilerindeki hâkimiyeti olabilmektedir (Kara vd., 2006: 2). Özellikle devletlerin teknolojik gelişmişliği ve yeni medya araçlarını kullanabilme becerisi, siber ortam üzerindeki savaşma kabiliyetindeki gücünü belirleyecektir.

Dünyada siber savaş örnekleri ve ulaştığı boyutlar

Günümüzde bütün devletlerin, şirketlerin ve bireylerin yüksek teknolojili bilgisayar sistemlerine bağlı hale gelmesi, siber savaşların hızlı bir şekilde yayılmasına neden

olmuştur. Bu hızlı gelişmeler karşısında devletler, sanal dünyayı kontrol etmeleri ve izlemeleri için yeni tedbirler alarak, çeşitli stratejiler geliştirmektedir. Bu tehditler ve riskler sadece devletler için değil, bireysel düzeyde dahi insan yaşamını etkiler hale gelmektedir. Siber alandaki bu yeni güvenlik riskleri gün geçtikçe farklı boyutlarda karşımıza çıkmaktadır.

Dünyada siber saldırıların başlangıcına yönelik farklı görüşler bulunmaktadır. Soğuk Savaş döneminde Amerika Birleşik Devletleri (ABD) ve Sovyetler Birliği arasında gizli olarak yürütüldüğü düşünülen faaliyetlerin çoğunluğu siber savaşın başlangıç yılları olarak anılmaktadır. Özellikle Soğuk Savaş'tan sonra değişen güvenlik algılamalarındaki farklılık, risk ve tehditler açısından parametrelerin değişiklik göstermesine neden olmuştur. Bu dönemde gerçekleşen bir siber saldırı örneği ise, Sovyetler Birliği 1982 yılında, Kanada'daki bir şirketten doğal gaz boru hatlarını kontrol etmek için kullanılan bir yazılımı çalmaya çalışmıştır. Kanada'dan gizlice çalınan yazılım aslında ABD tarafından Merkezî İstihbarat Teşkilatı (Central Intelligence Agency-CIA) tuzağı ile virüslü bir yazılımdır. ABD yazılımın içine Truva atı virüsü yüklemiştir (Markoff, 2009). Aynı yıl Sibirya'da yaşanan patlama, tarihte siber teknoloji kullanılarak gerçekleştirilen ilk siber saldırı örneği olma özelliği taşımaktadır. Bu saldırı, tarihte nükleer olmayan en büyük patlamadır (Kara, 2013: 40). Patlamanın nedenlerinin arasında CIA tarafından gizlice koyulan Truva atı virüsü olduğu öne sürülmektedir.

ABD'de 11 Eylül 2001 yılında gerçekleşen ve "İkiz Kuleler" olarak bilinen "Dünya Ticaret Merkezi" saldırısıyla birlikte, dünyada siber ortamın güvenliğinin de önemi artmıştır. 11 Eylül saldırıları bir siber saldırı olayı olarak nitelendirilmese de, Pentagon'un kırılmaz denilen güvenlik şifrelerinin kırılması, hava radar sistemlerinin devre dışı bırakılması ve düşen uçakların pilotlarından kaçırılma sinyalleri alınmaması gibi unsurlar bu saldırıların önlenmesinde teknolojik sistemlerin ne kadar önemli olduğunu açıkça ortaya koymaktadır. 11 Eylül saldırısı için teknoloji yoğunluklu bir terör olayı demek mümkündür (Keçeci, 2016: 8). 11 Eylül saldırıları sonrasında terörizm ve güvenlik söylemlerinin yanında siber terörizm endişeleri de gündeme gelmiştir. Bilişim teknolojilerine ve siber ortama karşı güvensizlik ve endişe duyguları siber terörizm korkularını yaratmıştır. Soğuk Savaş sonrası ortaya çıkan Amerikan hegemonyasının, ele geçirilemez denilen güvenlik ağlarının kırılganlığı bu saldırılarla birlikte ön plana çıkmıştır.

Siber saldırıların bir başka örneği ise 2007 yılında Estonya'da gerçekleşmiştir. "Estonya Siber Savaşı" olarak da anılan bu saldırı, küresel ağ internet aracılığıyla gerçekleştirilen en güçlü saldırılardan birisidir. Rus Kızıl Ordusu'nun 2. Dünya Savaşı anısına dikilen "Tallin'in Bronz Heykeli" anıtının yer değiştirilmesi olayında, karşı grubun internet erişimini durdurması vakasıdır. Saldırı sonrası NATO ve Avrupa Birliği (AB)'den birçok yetkili Estonya'ya saldırının nedeni üzerine araştırma yapmak için gönderilmiştir (Özcan, 2004: 39). O zamana kadar, hiçbir ülkede görülmeyen boyutta bir dijital saldırıya maruz kalan Estonya'da kurumlarının neredeyse tamamının dijitalleşmiş olması ve vatandaşların gündelik birçok işini, internet üzerinden gerçekleştirmesi, yaşanan bu saldırı sonucunda altyapının çökmesine sebep olmuştur (Polat, 2020: 146). Estonya'da yapılan siber saldırılar sonucunda, dünyada uluslararası güvenlik açısından bir milat olmuştur. Devlete ait kritik alt yapılara ve önemli bilgilere yönelik yapılan bu saldırı, siber güvenlik politikalarının tartışılmasına neden olmuştur.

Estonya Siber Savaşı sonrasında benzer bir olay ise Ağustos 2007'de, Almanya'da gerçekleşmiştir. Almanya'daki stratejik kurumların veri tabanlarına girilmiş, birçok belge kopyalanmıştır. Siber terör kavramı, 2009 yılının Nisan ayında İngiltere'de bir bakanlığın

web sitesinde yaşanan olay üzerine tüm dikkatleri üzerine çekmiştir. Söz konusu bakanlığın web sitesi şifre kırıcılar tarafından ele geçirilmiş ve siteye dikkat çekmek istedikleri konu ile ilgili bir web sitesini yönlendirmiştir. Benzer bir olay, aynı yılın Şubat ayında Fransız Savunma Bakanlığı'nda yaşanmıştır. Öyle ki; söz konusu siber saldırı sonucunda bilgisayar virüsü nedeni ile birçok uçak Villacoublay Hava Üssü'nden havalanamamıştır (Özkan, 2006: 83).

ABD siber savaşlar açısından en fazla saldırıya uğrayan ülkelerden biridir. 24 Nisan 2013 tarihinde bilinmeyen bir bilgisayar korsan grubu (hacker) tarafından gerçekleştirilen siber saldırıda, Uluslararası Haber Ajansı Associated Press'in (AP) Twitter hesabı hacklenmiştir. Bu hesaptan gönderilen bir sahte Tweet ile *"Flaş Haber: Beyaz Saray'da iki patlama oldu. Başkan Obama yaralandı"* yazılmıştır. 10 milyondan fazla takipçisi olan AP'nin sahte Tweet'inin ardından, ABD borsası 3 dakikalık bir düşüş yaşamış ve ABD ekonomisi 136 milyar dolarlık bir değer kaybına uğramıştır (Özdemiroğlu, 2013). Siber savaşlar içerisinde en etkili saldırılardan biri olan bu olayda, bir ülkenin ekonomisine de zarar verebileceği gerçeği ortaya çıkmıştır.

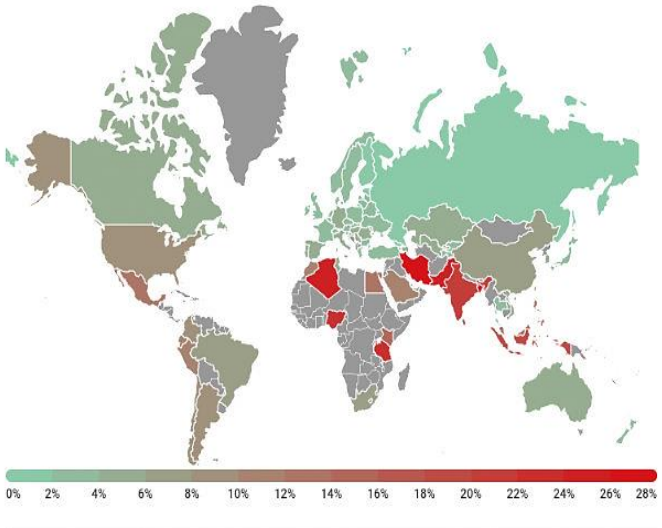
Kamu ve özel sektördeki bilişim teknolojilerinin gelişimine bağlı olarak yüksek düzeydeki gizli bilgiler, kişisel veriler, devlet kaynaklı bilgilerin depolanmasına paralel olarak bu bilgilerin güvenliği sorunu ortaya çıkmıştır. Bilgisayar korsan grupları tarafından yapılan saldırılar sonucunda güvenlik zafiyetleri oluşmakta ve devlete ait önemli bilgiler ifşa edilebilmektedir. Siber saldırılar içerisinde devlet kaynaklı gizli bilgilerin ifşa edilmesine önemli bir örnek ise Wikileaks bilgilerinin yayınlanmasıdır. Irak operasyonunda görev yapmış ABD kıdemli eri Bradley Manning, 1966-2010 tarihleri arasında ABD Dış İşleri Bakanlığı'nca yapılan gizli yazışmaları, ordu veri tabanından indirdiği doküman ve görüntüleri, 2010 yılı Kasım ayında Wikileaks sitesine sızdırmıştır. Yayınlanan görüntüler içerisinde, Cenevre Sözleşmesine göre sivil hedeflerin bombalanamayacağı kuralını ihlal eden görüntüler yer almaktadır. Pentagon'u rahatsız eden ve ABD'nin yönetimini sıkıntıya düşürecek bilgiler ifşa edilmiştir (Kara, 2013). Siber tehditler finans ya da itibar kaybıyla sınırlı kalmamakta devlet kurumlarındaki güvenlik zafiyetleri nedeniyle ulusal güvenlik bile tehlikeye düşebilmektedir. Küresel düzeyde siyasi sonuçları olduğu için, siber ortam güvenliği gün geçtikçe üzerinde durulması gereken en temel sorunlardan biri haline gelmiştir.

Wikileaks belgelerinin sızdırılması sonrasında, "Panama Belgeleri" adı altında ifşa edilen belgeler, siber ortamın güvenliğinin önemini bir kez daha gündeme taşımıştır. Panama merkezli, dünyanın dördüncü büyük offshore firması[ii] olan Mossack Fonseca'ya ait veri tabanından sızdırılan 11.5 milyon belge, Uluslararası Araştırmacı Gazeteciler Konsorsiyumu (International Consortium of Investigative Journalists-ICIJ) tarafından 2016 yılında tüm dünyaya servis edilmiştir. Belgelerde dünya liderleri, bürokratlar, iş adamları ve ünlülerin dâhil olduğu uluslararası düzeydeki para aklama ve vergi kaçırma gibi yasa dışı faaliyetleri ortaya çıkarmıştır. On iki ulusal lider, denizaşırı vergi cennetlerini kullandığı bilinen 143 siyasetçi, bunların aileleri ve dünyadaki yakın ortakları belgelerde yer almaktadır (Erdurucan, 2017: 23-24). Sıradan okuyucu için pek anlam ifade etmeyecek verilerden oluşan Panama Belgeleri, gazetecilerin analizleri sayesinde önemli ve çarpıcı haberlere dönüşmüştür. Panama Belgeleri'nin yayımlanması, siyasal ve yasal alanda önemli etkilere sahip olmasının yanında, gazetecilik açısından son derece önemli bir gelişmedir. Yeni medyanın olanaklarından faydalanarak çok kapsamlı bir iş birliği ile gerçekleştirilen bir araştırmacı gazetecilik örneğidir (Atalay, 2018: 143). Şimdiye kadar görülen en büyük veri sızıntısı sonucunda siyasal ve finansal anlamda birçok olumsuz sonuca neden olmuştur. Hem Wikileaks hem de Panama Belgeleri

örneklerinde varılan sonuçlardan biri, uluslararası siyaseti belirleyen ve süreçlere yön veren siber ortam güvenliği meselesi uluslararası siyasetin de en önemli gündemlerinden biri haline gelmiştir.

Yeni terörün hızlı bir şekilde ilerlemesi sonucunda, NATO savaş doktrini oluşturma konusunda çalışmalarını hızlandırarak, 2011 Haziran ayında bir siber savaş doktrini açıklamıştır. Siber saldırıyı, silahlı bir saldırı ile eş tutacağını ve gerekirse bu türdeki siber saldırılara silahla karşılık verileceğini söylemektedir. NATO'nun yeni siber savaş doktrinini açıklamasıyla birlikte, çeşitli ülkeler siber ordularını kurmaya başlamıştır. Örneğin Çin, 30 siber savaşçıdan oluşan bir siber ordu kuracağını 2011 yılında açıklamıştır (Ege, 2012). Çin, önemli siber saldırı kapasitesine ve gelişmiş istihbarat alt yapısına sahip bir devlet olarak, 2050 yılına kadar elektronik egemenliği hedefleyen ve düşman ülkelerin siber ortamdaki altyapılarını etkisiz hale getirecek bir siber doktrin benimsemiştir. Çin Halk Özgürlük Ordusu siber savaşın kara, deniz ve hava savaşlarıyla aynı öneme sahip olduğunu ve bunun içinde bir siber ordunun her devlet için gerekli bir nitelik olduğunu ileri sürmektedir (Coleman, 2008: 132).

Türkiye'de Ulusal Siber Olaylara Müdahale (USOM), 2013-2014 yılında Stratejisi ve Eylem Planı kapsamında, ulusal ve uluslararası koordinasyonun sağlanması için kurulmuştur. USOM, hem ulusal ve uluslararası koordinasyon görevini yürütmekte hem de internet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişimi gerçekleştirmektedir. Siber Olaylara Müdahale Ekibi (SOME) ise ülkemizde USOM ile iş birliği içerisinde çalışan, kurum ve kuruluşların sorumluluğunu yürüten birim, bir siber saldırının tespit edilmesi, tespitin USOM'a bildirilmesi, USOM'dan gelen uyarıların veya bildirimlerin yerine getirilmesi ya da giderilmesi için atılması gereken adımları atan bir kurumdaki yetişmiş uzmanları tanımlar. Dolayısıyla, ulusal strateji dokümanı kapsamında meydana gelen siber olayların önlenmesi, zararlarının azaltılması, kurum bilgi teknoloji sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda ilgili birimlere öneriler sunabilmektedirler (Sağıroğlu, 2018: 30). Bu gelişmeler sonucunda birçok devlet gibi Türkiye'de siber ortam güvenliği için etkili çalışmalar yürütmektedir.



Grafik 1. Mobil Kötü Amaçlı Yazılıma Bağlı Ülkelerin Küresel Etkilenme Oranları (Kaynak: Kaspersky, 2019)

Yeni medya ortamlarının sağladığı birçok özelliği bünyesinde barındıran ve gündelik hayatın her alanına nüfuz etmiş olan mobil teknolojiler, siber savaş alanının da içerisinde yer almaktadır. Dijitalleşme ve etkileşimliliğin etkili olduğu araçlar olan mobil teknolojiler, kaynağı bilinmeyen bilgisayar korsan grupları (hacker) tarafından küresel ölçekte saldırı altındadır. Grafik 1'de 2019 yılı verilerine göre[iii], mobil kötü amaçlı yazılım bulaşma girişimlerinin coğrafyası ve ülkelerin etkilenme oranları verilmiştir. Kaspersky Lab verilerine göre (2019); İran %28.31 ile birinci sırada yer almaktadır. Bangladeş %28.10 ikinci sırada, Cezayir %24.77 ise üçüncü sırada yer alan ülke olarak etkilenme payı ölçümleri verilmiştir. Türkiye ise diğer ülkelere göre oldukça düşük bir etkilenme payına sahiptir. Siber tehditlerin farklı fiziki araçlarla etkinlik gösterdiği, bunlardan birinin de mobil kötü amaçlı yazılım bulaşma girişimleri olduğu açıkça görülmektedir. Siber saldırıların küresel ölçekte ciddi bir tehdit olduğu, bu haritalanma aracılığıyla ön plana çıkmaktadır.

Devletler, güvenli bir siber ortam sağlayabilme yolunda, siber ortamın parçası olan bileşenleri siber saldırılara karşı korumak, yapılan saldırılara müdahale etmek, saldıranları cezalandırmak, gerekli yasal mevzuatı oluşturmak ve bütün faaliyetleri yerine getirecek yapıları tesis etmek üzere siber ortama yönelik politika ve stratejiler geliştirmiş ve geliştirmeye devam etmektedir (Çiftçi, 2013). Siber ortam güvenliği sorunlarıyla mücadele etmek için uluslararası bir işbirliğinin gerekliliği vurgulanmaktadır. Uluslararası aktörlerin ve devletlerin bilişim sistemleri üzerine kendi bilgi ve deneyimlerini ortaya koyduğu kolektif bir iş birliği, siber ortam güvenliği açısından önemli görülmektedir. Amerika Birleşik Devletleri'ne yönelik yapılacak bir siber saldırı sonucunda İtalya, Almanya ya da Türkiye dahi etkilenebilmektedir. Bu bağlamda, teknolojik gelişmelerin ilerlemesine bağlı olarak saldırı potansiyellerinin artması, devletlerin siber kabiliyetlerini ve stratejilerini geliştirmeleri açısından küresel bir iş birliğini ve dayanışmayı zorunlu hale getirmiştir.

Örnek olay analizi: Stuxnet Saldırısı

21. yüzyılın en ciddi siber saldırısı olarak değerlendirilen Stuxnet saldırısı, İran'ın nükleer santrallerini hedef almıştır. İnsanlık tarihinde sabotaj için geliştirilmiş ilk süper bilgisayar virüsü olma özelliğini taşımaktadır. Kötü amaçlı yazılım programlarının en gelişmiş ve karmaşık versiyonunu oluşturan Stuxnet adındaki solucan (worm) virüsü[iv] 2010 yılında tespit edilmiştir. Stuxnet'in en belirgin özelliği kendi kendini kopyalayabilmesidir. Böylece içine yerleştiği ağı kullanılamaz hale getirene kadar yayılabilen bir tür yazılım bombası işlevi görmektedir. Özellikle Stuxnet saldırısı, uzaktaki bir bilgisayar sistemine yönelik yapılan ilk büyük saldırı olmasıyla da büyük önem taşımaktadır. Süper bilgisayar virüsleri çağını başlatan Stuxnet Saldırısı, siber terör düzenin ve kurallarının büyük ölçüde değişimine neden olmuştur.

Kullanılan virüsün adıyla "Stuxnet" olarak bilinen bu saldırının, 2009'da ABD tarafından İran'ın Natanz nükleer yakıt zenginleştirme tesislerine karşı düzenlendiği öne sürülmektedir. Bulgulara göre, İran'ın Natanz nükleer yakıt zenginleştirme tesislerindeki bilgisayar ağına karşı düzenlenen virüs saldırısı, iki ayrı tarihte gerçekleştirilmiş olup; birinci saldırı 22 Haziran 2009'da yerel saatle 16.30'da, ikinci saldırı ise 7 Temmuz 2009 tarihinde yerel saatle 17.00'de meydana gelmiştir (Kara ve Çelikkol, 2011: 145). Özellikle SCADA (Supervisory Control And Data Acquisition)[v] sistemlerine saldırmak üzere yazılmış, bilinen ilk ve karmaşık yazılımdır. Nükleer enerji tesislerinde SCADA

sistemleri, tüm sahaları kontrol eden ve izleyen merkezi sistemleri kapsadığından dolayı konunun önemi dikkat çekmektedir.

İran nükleer tesisinden içeri girmeyi başaran Stuxnet virüsü, yavaş ve emin adımlarla zarar vermeye başlamıştır. Santrifüjler uranyum zenginleştirmede kullanılan ve son derece hızlı dönen makinelerdir. Virüsün amacı, Santrifüjlerin kontrolünde kullanılan "Programlanabilir Mantık Denetleyicisi" (PLC: Programmable Logic Controller) kontrol devrelerini hedef alarak kontrolü ele geçirmektir. Stuxnet'in virüs bulaştırılmış bir USB vasıtasıyla, yerel ağdaki bir Programlanabilir Mantıksal Kontrol Aygıtı'na bulaştırıldığı tespit edilmiştir. Bir USB sürücüsü vasıtasıyla sisteme bulaştırılan bu kötücül yazılım, komuta kontrol servis sağlayıcısına bağlanmak üzere programlanmıştır. Stuxnet, bu sayede saldırıyı düzenleyene hareket serbestliği kazandırmakta ve bulaştırılan bilgisayar vasıtasıyla sisteme daha fazla kötücül kod yüklemesi yapılabilmektedir (Bıçakçı, 2016: 116).

Kontrolör yazılımı bozulmaya başlayınca hızla dönen makinelerin dönme hızı kontrolden çıkıp, makineler parçalanmaya başlamıştır. Sistemi ele geçirerek içten içe zarar veren virüsün en karmaşık yanı ise merkez bilgisayarlarına her şeyi normal göstermesidir. Bu nedenle içten içe verilen zarar uzun zaman sonra anlaşılabilmiştir (Kara ve Çelikol, 2011: 34). Stuxnet, saldırdığı sistemlere her 100 milisaniyede sisteme bir komut göndererek olağanüstü bir hızda frekans değiştirme işlemi yapmıştır. Bu işlevi göz önüne alındığında, virüsün uranyum zenginleştirme sürecini veya tesislerini bütünüyle sabote etmek değil, tesislerdeki çalışmaları sekteye uğratmak maksadıyla da geliştirildiği ve sisteme yüklendiği anlaşılmaktadır (Çelik, 2013: 148).

2010 yılının Haziran ayında Ukrayna'daki küçük bir firma olan VirusBlokAda tarafından bu virüsün varlığı tespit edilmiştir. Programın o güne kadar rastlanılan tüm zararlı yazılımlardan daha karmaşık yapıya sahip olduğunun fark edilmesiyle, anti virüs program yazılım şirketi Kaspersky ve yazılım şirketi Microsoft ile birlikte virüsün kaynağını bulmak üzere ortak bir araştırma başlatmış, araştırmaya daha sonra Amerikan bilişim şirketi Symantec dâhil olmuştur (Çelik, 2013: 145). İncelemeler sonucunda yazılımın karışık yapısı, basit bir solucan virüsü olmadığını göstermiştir. Farklı alanlarda uzmanların uzun zaman ve büyük bir bütçe harcayarak gerçekleştirilebileceği bir yazılım olduğu anlaşılmıştır.

Tüm saldırılar sonucunda Stuxnet virüsü, Natanz nükleer tesisindeki çalışmaların uzaktan takibine olanak sağlamakla birlikte santralde bulunan santrifüjlerden yaklaşık 1000 tanesini uğrattığı zarar neticesinde durdurmuştur. Uranyum zenginleştirme faaliyetlerinin parçası olan bu nükleer tesisin yaklaşık beşte biri işlemez hale gelmiştir. Santrifüjleri kontrol eden SCADA, sisteminin işleyişi bozarak verim kaybına neden olmuştur. Tamiri aylar sürecek bir hasara sebep olan bu operasyonun geçici surette olsa dahi fiziksel bir zarara sebebiyet verdiği açıktır (Gümüşbaş, 2016: 185). Stuxnet saldırısından sonra parçalanan makinelerin yenilenmesi ve kalan makinelerin zararlı yazılımlardan temizlenmesi, yeniden yüklemelerinin yapılması, çalışmaları uzun süre aksatmıştır. Stuxnet virüsünün, İran'ın nükleer çalışmalarını iki yıl geriye götürdüğü bilinmektedir. Dünya genelinde virüsün %60'ı aşan bir oranda İran'ı etkilemesi ise bu virüsün özellikle İran nükleer tesisini kontrol altına almak ve çökertmek için geliştirildiği düşüncesini arttırmıştır. Gerçek hedefi olan İran'daki Natanz uranyum zenginleştirme tesisine ulaşana kadar Stuxnet'in 100 binden fazla sisteme bulaştığı bilinmektedir (Kara, 2013: 34). Saldırılardan zarar gören ülkeler arasında İran (%58.85) ve Endonezya (%18.22) ilk sıraları alırken, Hindistan (%8.31), Azerbaycan (%2.57), Amerika Birleşik Devletleri (%1.56), Pakistan (%1.28) da listede etkilenme oranlarıyla birlikte yer almıştır

(Wikipedia, 2020). Stuxnet saldırısı sonrasında aslında sadece bir ülkenin değil, birçok ülkenin de bu saldırıdan etkilendiği görülmektedir. Siber ortam güvenliğine yönelik küresel çapta işbirliğinin gerekliliği bu örnek aracılığıyla da dikkat çekmektedir.

Siber saldırı sonucunda meydana gelebilecek olan fiziki zararın, geleneksel silahlarla yapılan saldırı sonucunda meydana gelecek zarar eşiğine ulaşma olasılığı azımsanamayacak derecede yüksektir. Stuxnet saldırısından sonra Natanz'da can veya mal kaybına neden olan fiziksel bir etki gözlemlenmemişse de yaratabileceği etkileri açısından bu yargıyı doğrulamaktadır. Saldırı sonrasında tesisin soğutma sisteminde meydana gelebilecek bir arızanın nükleer serpintiye neden olmayacağını garanti etmek mümkün değildir. Sebep olabileceği etkiler göz önüne alındığında, siber saldırının fiziksel bir zarara neden olmasının madde uyarınca bir saldırı fiili olarak yorumlanabileceği açıktır (Çelik, 2013: 159). Dolayısıyla saldırıların siber ortam üzerinden sadece bir zarar oluşturması dışında, insan yaşamına da etkileri olabileceği gerçeğini ortaya çıkarmıştır. Ağ toplumunda yaşadığı varsayılan toplumların, gelecek saldırılarda birçok can ve mal kayıplarına ulaşabileceği yorumu yapılabilmektedir.

ABD, söz konusu saldırıda bir rolü olduğuna dair herhangi bir resmi beyanda bulunmamıştır ancak bu virüsün yazılması ve saldırı amacıyla kullanılmasında bir rolü olduğunu da hiçbir zaman yalanlamamıştır. Ancak İran Sivil Savunma Kurumu, yaptığı açıklamada Stuxnet virüsünün nükleer santrallere ilişkin edindiği bilgileri nereye rapor ettiğinin izinin sürüldüğünü ve buranın ABD'nin Texas eyaletinde olduğunu tespit ettiklerini iddia etmiştir. Bunun yanında birçok bilişim uzmanı saldırının arkasında ABD ve İsrail'in olduğunu savunmuştur (Maness ve Valeriano, 2015: 151). Stuxnet saldırısı ile birlikte, teknolojik ve bilişim dünyasındaki hâkimiyetini kanıtlayan ABD, siber silahların geliştirilmesi adına önemli bir gelişmeye yol açmıştır.

Stuxnet virüsünden önce siber silahlar, bugüne kadar daha çok örgütlü olmayan, kurumsal kimlikten yoksun, hiyerarşik bir emir komuta düzeni içinde yer almayan ve genellikle politik muhalif-aktivist kimliğiyle hareket eden bireysel girişimlerin ürünü olmaktadır (Çelik, 2013: 141). Ancak Stuxnet tüm bu kuralları yıkarak, siber silahın geleneksel silahlar kadar etkili bir şekilde kullanılabileceğini göstermiştir. Geleneksel savaş stratejileri incelendiğinde ilk saldırının rakibin iletişim ve enerji kaynaklarını zayıflatmak ya da kesmek üzere yapıldığı bilinmektedir (Bıçakçı, 2019: 6). Bu geleneksel askeri stratejinin Stuxnet virüsü aracılığıyla siber ortam üzerinden kurulduğu görülmektedir.

2010'da yapılan çalışmalar sonucunda Stuxnet'in deşifre olmasıyla birlikte, siber savaş konusunda çalışmalarını hızlandıran NATO, siber savaş doktrinini 2011 Haziran'ında açıklamıştır. Zira Stuxnet saldırısı sonrasında, süper bilgisayar virüsleri çağı başlamıştır. Stuxnet saldırısı ardından ortaya çıkan, "Duqu, Flame, Mehdi ve Gauss[vi]" adlı süper bilgisayar virüsleri de kimliği belirsiz bilgisayar korsan grupları (hackers) tarafından oluşturulup, çoğunlukla Orta Doğu bölgesinde kullanılmış siber silahlardır. Ayrıca söz konusu süper virüslerde kullanılan yazılım mimarisinden yola çıkan Vitaly Kamluk; Stuxnet, Duqu, Flame ve Gauss'un aynı kadrolar tarafından geliştirildiğini öne sürmektedir. Siber güvenlik uzmanları Stuxnet, Flame ve Gauss tipindeki süper virüslerin ancak bir devlet tarafından organize edilen, geniş bir bilişimci kadrosuyla yazılmış olabileceğine dikkat çekmektedir (Börçetin, 2012: 19). Son yıllarda birbiri ardına ortaya çıkan ve gittikçe mücadele etmesi güçleşen süper bilgisayar virüsleri, internetin giderek artan bir hızla, savaş meydanı haline geldiğini gösteren önemli örneklerdir.

Sonuç

Günümüzde bilişim teknolojisinin gelişmesi ve yeni medya araçlarının tüm dünyayı küresel bir köye dönüştürmesi sonucunda, dünya üzerinde devletler, bireyler, kurum ve kuruluşlar ağlarla birbirlerine bağlanmaktadır. Devletlerin birer e-devlet haline geldiği ve elektrik santralleri, doğal gaz üretim sahaları ve bankacılık ağları gibi kritik altyapıların tamamıyla bilgisayar tabanlı ağlar aracılığıyla kontrollerinin sağlanıyor oluşu, siber ortam güvenliğinin önemini başka bir boyuta taşımıştır. Siber ortam üzerinden yapılan saldırılar sonucunda kişisel, kurumsal ya da ulusal verilere yönelik kayıp ve zararlar yaratabileceği gerçeği birçok siber savaş örneğinde (AP Twitter hacklenmesi olayı, Wikileaks, Panama Belgeleri vb.) tespit edilmiştir.

Bu çalışmada, insanlık tarihinde sabotaj için geliştirilmiş ilk süper bilgisayar virüsü olan ve siber savaşların etki boyutunu değiştiren Stuxnet saldırısı, örnek olay analizi yöntemiyle incelenmiştir. Stuxnet virüsünün ABD tarafından İran'ın nükleer yakıt zenginleştirme tesislerinin çalışmalarını engellemek ve nükleer çalışmaları aksatmak amacıyla üretildiği öne sürülmektedir. Çalışmada incelenen Stuxnet saldırısı, nükleer zenginleştirme programını hedefleyen ve endüstriyel SCADA sistemlerini hedef alarak kritik altyapıların kontrol edilmesi ve izlenmesini engellemek için kullanılmıştır. Uzaktaki bir bilgisayar sistemine yönelik yapılan ilk büyük saldırı olması ve solucan (worm) virüslerin birer sanal mikrop haline dönüşerek, terör amaçlı kullanılıyor oluşu, siber savaşlar tarihini büyük ölçüde etkilemiştir. Bir siber silah olarak Stuxnet, konvansiyonel saldırıların benzeri yöntemleri benimseyerek; hiyerarşik, emir-komuta düzeni içerisinde, örgütlü bir yapıda saldırı gerçekleştirmiştir. Stuxnet saldırısı, konvansiyonel askeri stratejilerine benzer şekilde, ilk olarak düşman ülkenin iletişim ve enerji kaynaklarını zayıflatmak ya da kesmek üzere yapıldığı amacını taşımaktadır. Siber alan üzerinden gerçekleştirilmiş bir saldırı olmasına rağmen, geleneksel saldırılara benzer şekilde fiziki zararlar yaratabilmiş, bir süper bilgisayar virüsü gerçek mekânı da etkileyebilmiştir. Bu saldırılar sonucunda nükleer tesislerin siber güvenliği konusu, küresel ölçekte ulusal güvenliğin en önemli sorunlarından biri haline gelmiştir. Zira Stuxnet saldırısı sonrası süper bilgisayar virüsleri çağı başlamış ve çoğunlukla Orta Doğu ülkelerine yönelik birçok saldırının (Duqu, Flame ve Gauss) yapıldığı tespit edilmiştir.

Devletlerin siber ortam üzerindeki hâkimiyeti, bilişim sistemlerindeki gücüne, yeni medya araçlarını yönetebilmesine ve teknolojik gelişmişliğine bağlı olarak değişebilmektedir. Bu hâkimiyet, devletlerin yaşamsal faaliyetlerini ve ülkelerin ulusal güvenliğini korumak açısından da önemli görülmektedir. Zira siber güvenlik stratejileri için etkili mücadele yöntemleri geliştirilmesi ve azami önemin bu alana yönlendirilmesi yorumu yapılabilmektedir.

---

[i] Bu araştırma, Galatasaray Üniversitesi İletişim Fakültesi Stratejik İletişim Yönetimi Konferansları-1-"21. Yüzyılın Krizleri: Yönetim, İletişim ve Etik" adlı konferansta 19 Aralık 2018 tarihinde *"Yeni Medya, Yeni Terör: Stuxnet Saldırısı"* adıyla sözlü bildiri olarak sunulmuştur.

[ii] Offshore: Kıyı bankacılığı olarak da adlandırılan, serbest bölgelerde faaliyet gösteren ve ulusal bankacılık sisteminin dışında tutulan ve buna göre de muafiyetler tanınan bir tür uluslararası bankacılıktır (Kaynak, Çeker, 2006).

[iii] Kaspersky Lab., *"IT threat evolution Q2 2019. Statistics"* verilerine göre, 2019 yılında *"geography of mobile malware infection attempts"* adlı ölçümlere göre bir haritalanma işlemi yapılmıştır. (Kaynak: https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/ Erişim Tarihi: 10.03.2020)

[iv] Solucan (Worm): Kurt da denmektedir; bağımsız, kendi kendine çoğalabilen, ağda bir bilgisayardan diğerine yayılma yollarını araştıran ve yayılan bir programdır. Saniyeler içinde milyonlarca bilgisayara ulaşabilir (Kaynak, Çiftçi, 2013: 150).

[v] Scada Sistemi: Tüm sahaları kontrol eden ve izleyen merkezi sistemleri ifade eder. Denetim kontrolü ve veri toplama (SCADA) altyapı işlemlerini (su arıtma, atık su arıtma, gaz boru hatları, rüzgâr santralleri, vb.), tesis tabanlı işlemleri (havaalanları, uzay istasyonları, gemiler, vb.) kontrol etmek için kullanılan ICS (Endüstriyel Kontrol Sistemleri) anlamına gelir. Genellikle endüstriyel işlemlerde (üretim, üretim, rafinaj, elektrik üretimi vb.) kullanılır (Kaynak: http://www.prowmes.com/blog/scada-sistemi-nedir/ Erişim Tarihi: 12.03.2020).

[vi] Stuxnet sadece önceden belirlenmiş bir konfigürasyona sahip bilgisayarlara ve endüstri sistemlerine zarar vermeyi amaçlarken, Stuxnet'ten sonra deşifre edilen Duqu'nun görevi Stuxnet için yeni hedefler seçmek (dolayısıyla bir nevi keşif virüsü olarak da sınıflandırılabilir). Flame ve Mehdi ise daha çok bilgi sızdırmaya yönelik virüsler. Görevleri içine sızdıkları sistemi tahrip etmekten ziyade kullanıcının elektronik postalarını okumak, gizli kalması gereken bilgilerini -örneğin şifrelerini- ele geçirmek, ekran görüntülerini almak, bilgisayarın mikrofonunu açarak konuşmaları kaydetmek, daha sonra da kaydettiği tüm bu bilgileri bilgisayarın "arka kapısını" kullanarak, dikkat çekmeden kendi sahiplerine göndermek. Gauss ise yine Kaspersky Lab uzmanları tarafından bu yılın Haziran ayında keşfedildi. Kaspersky uzmanlarından Vitaly Kamluk'un bildirdiğine göre, Gauss mimarları tarafından tahminen 2011'in Eylül ayında etkinleştirildi, görevi aralarında bu sefer Türkiye'nin de olduğu bazı Orta doğu ülkelerinde bulunan bankalardaki hesap hareketlerini gözlemlemekti (Kaynak, Börçetin, 2012: 19).

Kaynakça

Atalay, Esra Gül (2018) Enformasyon Anarşisi ve Gazeteciliğin Dönüşümü: Panama Belgeleri, *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi (ASEAD)*, 5 (5): 143-157.

Atıcı, Bünyamin ve Gümüş, Çetin (2003) Sanal Ortamda Gerçek Tehditler: Siber Terör, *Polis Dergisi*, 9 (37): 57-66.

Baudrillard, Jean (2004) *Tam Ekran*, Çev. Bahadır Gülmez, İstanbul: Yapı Kredi Yayınları.

Beck, Ulrich (1992) *Risk Society: Towards a New Modernity*, London: Sage Publications.

Beck, Ulrich (2009) *World And Risk*, Cambridge: Polity Press.

Bıçakçı, Salih (2016). Nükleer Tesislerin Siber Güvenliğine Giriş. *Türkiye'de Siber Güvenlik ve Nükleer Enerji*, Ed. Sinan Ülgen ve Grace Kim, ss.100-146, İstanbul: Ekonomi ve Dış Politika Araştırmalar Merkezi.

Bıçakçı, Salih (2019). Siber Güvenlik ve Savunma, *Güvenlik Yazıları Serisi,* Kasım 2019, https://trguvenlikportali.com/wpcontent/uploads/2019/11/SiberGuvenlik_SalihBicakci_v.1.pdf (Erişim Tarihi: 19 Ekim 2019).

Bozdemir, Mevlüt (1982).*Terör (mü) ve Terörizm (mi)?*, 100. Doğum Yılında Atatürk'e Armağan Dizisi, Cilt: VI, Ankara: SBF Basın ve Yayın Yüksek Okulu

Börçetin, Ege (2012) Siber Savaşlar, Bilişimin Karanlık Yüzü, *Bilim ve Teknik Dergisi*, Kasım 2012 Sayısı, ss.18-22, Ankara: Tübitak Yayınları.

Castells, Manuel (2000) Materials for an Exploratory Theory of the Network Society, *British Journal of Sociology*, 51 (1): 5-24.

Castells, Manuel (2005) *Ağ Toplumunun Yükselişi – Enformasyon Çağı: Ekonomi, Toplum ve Kültür*, Çev: Ebru Kılıç, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Castells, Manuel (2013) *İsyan ve Umut Ağları: İnternet Çağında Toplumsal Hareketler*, Çev: Ebru Kılıç, İstanbul: Koç Üniversitesi Yayınları.

Çeker, Mustafa (2006) Offshore Hesaplar ve Bankaların Sorumluluğu. *Çukurova Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 10 (2): 95-107.

Çelik, Şener (2013) Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme, *Dokuz Eylül Hukuk Fakültesi Dergisi*, 15 (1): 137-175.

Çiftçi, Hasan (2013). *Her Yönüyle Siber Savaş*, Ankara: Tübitak Bilim Kitapları

Dijk, Jan. Van (2012). *The Network Society*, London: Sage Publications.

Erdurucan, Salih (2017) *İnternet Medyasında Gizli Belge Yayıncılığının Teknik ve Elektronik Analizi: Wikileaks ve Panama Belgeleri*, Yayınlanmamış Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü.

Göker, Göksel ve Doğan, Adem (2011). Ağ Toplumunda Örgütlenme: Facebook'ta Çevrimiçi Tekel Eylemi, *Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 14 (25): 176-203.

Gümüşbaş, Ahmet (2016) Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları, *Türk-Arap İlişkileri: Çok Boyutlu Güvenlik İnşası*, Ed. Reyyan Akkaş, ss.181-194, İstanbul: Tasam Yayınları.

Kara, Oğuz, Aydın, Üzeyir ve Oğuz, Ahmet (2006) *Ağ Ekonomisinin Karanlık Yüzü: Siber Terör*, 5. Bilgi, Ekonomi ve Yönetim Kongresi, İstanbul.

Kara, Mehmet ve Çelikkol, Soner (2011) Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği, *Atılım Üniversitesi 4. Ağ ve Bilgi Güvenliği Sempozyumu*, Ankara: Atılım Üniversitesi.

Kara, Mahruze (2013) *Siber Saldırılar - Siber Savaşlar ve Etkileri*, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi.

Kaspersky (2019) "IT Threat Evolution Q2 2019 Statistics", https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/ (Erişim Tarihi: 10 Mart 2020)

Keçeci, Orhun (2016) Siber Suçlar ve Terörizm, Meb Resmi Sitesi, http://mebk12.meb.gov.tr/meb_iys_dosyalar/60/01/201260/dosyalar/2016_03/29105407_siber_suclar_ve_terorizm.pdf (Erişim Tarihi: 10 Kasım 2019)

Keskin, Funda (1998) *Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler.* Ankara: Mülkiyeliler Birliği.

Koçak, Hüseyin ve Memiş, Kamile (2017) Ulrich Beck'in Risk Toplum Teorisi Bağlamında Güvenlik ve Özgürlük İkilemi, *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, 19 (2): 251-265.

Markoff, John (26 Ekim 2009) Old Trick Threatens the Newest Weapons, *NY Times*, https://www.nytimes.com/2009/10/27/science/27trojan.html?_r=2&ref=science&pagewanted=all& (Erişim Tarihi: 02 Eylül 2019).

McLuhan, Marshall (2001). *Global Köy*, Çev: Bahar Öcal Düzgören, İstanbul: Scala Yayıncılık.

Ottis, Rain (2011) *A Systematic Approach to Offensive Volunteer Cyber Militia*. (Yayımlanmış Doktora Tezi). Tut Press: Tallinn University of Technology.

Özcan, Mehmet (2004) Yeni Milenyumda Yeni Tehdit: Siber Terör, *Türk Harb-İş Dergisi*, 210: 39-40.

Özdemiroğlu, Patrick (24 Nisan 2013) Sahte Tweet'ler Bizi Yıldıramaz, *Milliyet Gazetesi*, https://www.milliyet.com.tr/ekonomi/sahte-tweet-ler-bizi-yildiramaz-1698125 (Erişim Tarihi: 23 Ekim 2019).

Polat, Şafak Doğan (2020) Nato'nun Yeni Operasyon Alanı: Siber Uzay, *Güvenlik Bilimleri Dergisi,* UGK Özel Sayısı, Şubat 2020: 135-158.

Sağıroğlu, Şeref (2018) Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler, *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık*, Ed. Şeref Sağıroğlu ve Mustafa Alkan, ss.21-45, Ankara: Grafiker Yayınları.

Techopedia (26 Mart 2018) İnternet Privacy, http://www.techopedia.com/definition/24954/İnternet-privacy (Erişim Tarihi: 20 Mart 2020)

Valeriano Brandon ve Maness Ryan C. (2015). *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, United Kingdom: Oxford University Press.

Wikipedia "Stuxnet", "t.y." https://en.wikipedia.org/wiki/Stuxnet (Erişim Tarihi: 20 Mart 2020)

Yayla, Mehmet (2013) Hukuki Bir Terim Olarak: "Siber Savaş", *Türkiye Barolar Birliği Dergisi*, 104: 177-202.