DERLEME

Geliş Tarihi: 15.01.2022
Kabul Tarihi: 08.02.2022

SİBER ORDULAR VE SİBER SAVAŞLAR

Cyber Armies And Cyber Wars

*Meryem ORAK

Özet

Gelişen dünya teknolojileri karşısında geleneksel ordular ve geleneksel silahların yanında siber ordu ve siber silahlar da devreye girmeye başlamıştır. Rekabet ve yarış sanal dünyada devam etmekte olup hem devlet hem de devlet dışı aktörler, kozlarını bu platformda da paylaşmaktadırlar. Genellikle ülkelerin resmi web sitelerine yapılan saldırılarla birlikte ayrıca o ülke adına faaliyet gösteren firmalar ya da o ülke vatandaşları da bizzat siber orduların hedefi olabilmektedir. Bu bakımdan yalnızca resmi aktörlerin değil ülke için önemli ticari firmaların ve vatandaşların da korunması önem arz etmektedir. Devletler bu bağlamda savunma sistemlerini yapılandırmakta ve siber bir dünyada daha etkili olabilmek adına ordularını bu çerçevede geliştirmektedirler. Bu çalışmada siber güvenlik ve siber ordu kavramlarına dair literatür incelenerek dünyada bu alanda atılım yapan devletlerden olan ABD, Rusya ve İran'daki durum ortaya konulmuştur. Son olarak da siber güvenlik alanında Türkiye'nin kurumsal ve altyapı girişimleri ele alınmıştır.

Anahtar Kelimeler: *Siber güvenlik, Siber ordu, Siber savaş*

Abstract

In the face of developing world technologies, besides traditional armies and traditional weapons, cyber army and cyber weapons have started to come into play. Competition and race continues in the virtual world, and both state and non-state actors share their trump cards on this platform. In addition to attacks on the official websites of countries, companies operating on behalf of that country or citizens of that country can also be the target of cyber armies. In this respect, it is important to protect not only official actors but also important commercial companies and citizens for the country. In this context, states are structuring their defense systems and developing their armies within this framework in order to be more effective in a cyber world. In this study, the literature on the concepts of cyber security and cyber army has been examined and the situation in the USA, Russia and Iran, which are among the states that have made a breakthrough in this field in the world, has been revealed. Finally, Turkey's institutional and infrastructure initiatives in the field of cyber security are discussed.

Keywords: *Cyber security, Cyber army, Cyber warfare*

Meryem ORAK, Yüksek Lisans Öğrencisi, Bartın Üniversitesi, meryem_orak@icloud.com

Giriş

Siber ordu kavramı ele alınmadan önce siber orduların temel iki bileşeni olarak bilişim sistemleri ile askeri kurumların ilişkisine değinilmesi gerekmektedir. Günümüze kadar geliştirilen pek çok teknoloji ve bunlarla bağlantılı cihazlar öncelikle askeri alanda kullanılmış olup ardından sivil alana yayılmıştır. Bunun başlıca örnekleri ise bilindiği üzere bilgisayar sistemleri ve internettir. Bilgisayar teknolojisine dair kavramların ortaya çıkışı 2. Dünya Savaşı yıllarına kadar götürülebilir. 2. Dünya Savaşı esnasında iletişim kurmak için Almanlar tarafından kullanılan ve Enigma ismi verilen bir makine bünyesinde barındırdığı kompleks sistemler ile bilgisayar teknolojisine benzer özellikler taşımaktaydı. Enigma'yı kısaca, 1. Dünya Savaşı sonlarında Alman bilim adamı Arthur Scherbius tarafından geliştirilen, düşman kuvvetlerinin iletilen mesajları okumasını engelleyecek şekilde şifreleme yöntemleri kullanan karmaşık bir makine olarak tanımlamak mümkündür.

2. Dünya Savaşı'nın başlarında bir takım mesajlar çözülmüş olsa da Enigma Almanlar tarafından sürekli geliştirilmiş ve bir Enigma'nın bir algoritması çözülene kadar yenisi oluşturulmuştur. Böylece istihbarat ve haberleşme gibi çok önemli iki alanda Almanya düşman kuvvetlere karşı avantaj sağlamıştır.

Savaş henüz patlak vermeden önce şifreli mesajları okumak amacıyla İngiliz hükümeti tarafından Bletchley Park ismi verilen bir grup kurulmuştur. Bu gruba 1938 yılında Alan Turing de davet edilmiştir. Turing doktora öğrenimi sırasında gerçekleştirmiş olduğu çalışmalarla Bletchley Park'ta oldukça faydalı olmuştur. Turing ve arkadaşları Enigma'nın mesajlarını kısmen çözmüş olsalar da her gün yenilenen algoritmalardan dolayı şifre çözmeyi sürekli hale getirebilecek bir karşı makine yapmak için çalışmalarını sürdürmüşlerdir. Aynı dönemde Adolf Hitler'in generalleri ile iletişim kurması için geliştirilen Geheimschreiber isimli bir makinenin de varlığından söz edilmekteydi. Dolayısıyla hem Enigma hem de Geheimschreiber için ayrı ayrı çalışmalar yürütülüyordu. Alan Turing'in zekası ve önceki çalışmaları bu konuda oldukça fayda sağlamış ve günümüz bilgisayarlarının atası kabul edilebilecek Clossus isimli makine bu dönemde geliştirilmiştir. Clossus bir mesajdaki 25000 karakteri anlık olarak tarayıp anlamlı mesajları ayırt edebilen icat edildiği dönem için oldukça gelişmiş bir makine olarak öne çıkmaktaydı. Bu sebeple iki ayrı makine yapılmadan Clossus ile hem Enigma'nın hem de Geheimschreiber'ın gönderdiği mesajlar çözülebilmekteydi. Dönemin savaş uzmanları tarafından Turing'in oluşturmuş olduğu makinenin, savaşı 2 yıl daha erken bitirdiği ve milyonlarca hayatı kurtardığı ifade edilmektedir (Copeland, 2004, s. 232).

İnternetin gelişimine bakıldığında yine askeri kurumların bu teknolojiye öncülük ettiği görülebilir. 1969 yılında Amerika Savunma Bakanlığı'nın kurmuş olduğu "The Advanced Research Projects Agency Network" yani daha yaygın ismiyle "ARPANET" dünyanın ilk paket dağıtım ağı yani internet ağı olarak kabul edilir. Savunma Bakanlığı öncülüğünde;

Kaliforniya Üniversitesi Los Angeles Yerleşkesi, Kaliforniya Üniversitesi Santa Barbara Yerleşkesi, Utah Üniversitesi, Stanford Araştırma Enstitüsü arasında ilk bilgisayar bağlantısı oluşturuldu. Kurulan protokolde gönderilen ilk ileti ise "lo" idi. Aslında gönderilmek istenen "login" kelimesiydi ancak gönderilen ilk iki harften sonra sistemlerde meydana gelen sorunlardan ötürü diğer harfler saatler sonra gönderilebilmiştir. Sonrasında ise ağ bağlantıları genişletilmiş, ordu ardından üniversiteler ve diğer devlet kurumları, internet aracılığı ile bağlantı kurmaya başlamıştır (Lukasik, 2011, s. 12).

Bunun yanında siber bir ordu fikri de zaman zaman ortaya atılmıştır Genellikle bilim kurgu filmlerinin konusu olmakla beraber yakın zamanda bunun artık gerçekleşebileceği görülmüş ve siber ordu çalışmaları hız kazanmıştır. Bunun öncülerinden biri de Amerika Birleşik Devletleri olarak karşımıza çıkmaktadır.

a) Amerika Birleşik Devletleri

Amerika Birleşik Devletleri, ordusu bünyesinde siber saldırılarına ilk olarak resmi bir yapılanmaya girmeden çok önce başlamıştır. Bunun ilk örneği ise 1. Körfez Savaşı sırasında yaşanmıştır. ABD bünyesinde faaliyet gösteren siber birimler Irak ordusunun kara, deniz ve hava kuvvetleri arasındaki koordinasyonu keserek savaş esnasında önemli bir üstünlük elde etmişlerdir. Ayrıca kriptolu telsiz frekanslarına sızarak frekansları karıştırmış ve Irak ordusunu yanlış noktalara yönlendirmişlerdir.

2. Körfez Savaşı esnasında da ABD mevcut siber gücünü ölçme imkanı bulmuştur. Bu defa yalnızca telsizlere değil Irak ordusunun diğer tüm haberleşme birimlerine sızma faaliyetleri gerçekleştirilmiş ve propaganda faaliyetleri bu yolla gerçekleştirilmiştir. Ele geçirilen haberleşme araçları ile görevli subayları psikolojik olarak etkileyecek ve ABD ordusuna teslim olmasını sağlayacak nitelikte mesajlar paylaşılmıştır (DARICILI, 2017, s. 341).

Amerika Birleşik Devletleri, özellikle 11 Eylül 2001'de yaşamış olduğu saldırılar sebebiyle bir histeriye kapılmış ve devletin ve de özellikle güvenlik birimlerinin etkinliğini oldukça etkin bir seviyeye çıkarmıştır. Başta fiziki silah envanterini genişletmekle başlayıp askeri müdahalelerle devam eden bu süreç, ordunun da yapılanmasını beraberinde getirmiştir. Bu bağlamda,öncelikle mevcut Uzay Komutanlığı bir dönüşüm geçirmiş ve uzayda etkinlik sağlama amacı yanında bir de siber güvenlikle ilgili görevler edinmiştir. Ancak 2008 yılına gelindiğinde ABD bunun yeterli olmayacağına kanaat getirmiş ve bir siber komutanlık kurulmasına yönelik çalışmalara başlamıştır ve 23 Haziran 2009 tarihine gelindiğinde United States Cyber Command (USCYBERCOM) resmi adıyla, Amerika Birleşik Devletleri Siber Komutanlığı'nı kurmuştur. Birleşik Devletler Siber Komutanlığı'nın görevleri ise şu şekilde belirlenmiştir:

- Savunma Bakanlığı'na bağlı bilişim ve bilgi ağlarını korumak ve bu noktada gerekli operasyonları gerçekleştirmek.

- Verilecek görevler doğrultusunda mevcut tüm sahalarda geniş ölçekli askeri siber operasyonlar düzenlemek.
- ABD'nin ve müttefik devletlerin internetteki dolaşım özgürlüğünü sağlarken düşman devletlerin faaliyetlerini baskılamak ve kısıtlamak amacıyla etkinliklerde bulunmak, planlar yapmak, koordinasyon faaliyetleri gerçekleştirmek ve bütünlük sağlamak olarak belirlenmiştir.
- Askeri ve sivil diğer otoriteler ile bilgi paylaşımında bulunmak, gerçekleşen ya da gerçekleştirilmesi planlanan operasyonlara dair bilgilendirmede bulunmak.
- Diğer ordu birimleri ile koordinasyon içerisinde hareket etmek.

11 Ekim 2012 tarihine New York'ta gerçekleşen bir konferansta ABD Savunma Bakanı Leon Panetta gelecek yıllarda ABD'nin siber bir Pearl Harbor tehlikesiyle karşı karşıya olduğunu ve bir takım düşman odaklarının ABD'nin kritik altyapısını siber yolla vurmak istediğini belirtmiştir. Pek çok altyapı faaliyetinin bilişim sistemleri üzerinden yürüdüğünü belirtmiş ve olası bir siber saldırı sonucunda elektrik, su gibi ve hatta ulaşım faaliyetlerinin kontrolü gibi bir takım durumların ciddi tehlikeye girebileceğini belirtmiştir. Tüm bu risklerden ötürü olası siber saldırılara karşı siber güvenliğin önemini vurgulayan Panetta siber ordunun bu tehlikelerin ortaya çıkması halinde anında karşılık vermesinin önemine dikkat çekmiştir (Yayla, 2013, s. 186-187).

ABD Siber Komutanlığı Ordu Siber Komutanlığı, Filo Siber Komutanlığı, Sahil Güvenlik Siber Komutanlığı ve Hava Kuvvetleri Siber Komutanlığı 4 alt birimden oluşmaktadır. 2013'te USCYBERCOM'da görev yapan asker sayısı 5000 olarak açıklanmıştır. Ancak bunun sonraki senelerde 21 bine çıkarılacağı iddia edilmektedir. Siber ordu ilk büyük muharip savaşını 29 Nisan 2016 tarihinde Irak Şam İslam Devleti (IŞİD) isimli örgüte karşı gerçekleştirmiştir. Özellikle internet alanında oldukça etkin olan IŞİD bu tarihten sonra bu alanda da bir savaş içerisine girmiştir. Birleşik Devletler Siber Komutanlığı'na bağlı birimler IŞİD'in faaliyet gösterdiği internet alanlarını izlemeye almış, internet üzerinden gerçekleşen para akışlarını kesintiye uğratmış ve propaganda yapmasını engellemeye yönelik girişimlerde bulunmuş ve oldukça önemli başarılar elde etmiştir (DARICILI, 2017, s. 341-342).

Geniş ölçekli siber savaş son zamanlarda ise ABD ve İran arasında yaşanmaktadır. 2015 yılına doğru başta İran olmak üzere pek çok ülkedeki devlet kurumlarına ait bilişim sistemleri Stuxnet ismi verilen bir virüsten etkilenmiştir. Windows işletim sistemleri üzerinden yayılan virüs kısa zamanda onlarca ülkede bilişim sistemlerine kritik ölçülerde zararlar vermiştir. Özellikle nükleer enerji sektöründe kullanılan sistemleri hedef alan virüs, reaktörlerdeki olağandışı durumların görülmesini engelleyerek nükleer felaketlere davetiye çıkarmıştır. Eski bir NSA (United States National Security Agency) çalışanı olan Edward Snowden, Stuxnet'in ABD ve İsrail ortaklığı sonucu ortaya çıkan bir virüs olduğunu ve tamamen İran'ın nükleer faaliyetlerin sekteye uğratmaya yönelik ola-

rak geliştirildiğini söylemiştir. Nitekim virüsün zararlarına bakıldığında en çok etkilenen ülkenin %58,85 ile İran olduğu görülmektedir. İran milyonlarca dolar zarar etmiştir. Ayrıcı nükleer santrallerindeki santrifüjleme makineleri olağanüstü hızlarda dönerek parçalanmıştır (Yazıcı, 2015). Bu yaşanan gelişmeleri siber savaşların ilk önemli adımları olarak görmek mümkündür.

20 Haziran 2019 tarihinde Amerika'ya ait bir casus insansız hava aracı İran tarafından düşürülmüştür. Söz konusu dönem için mevcut olan en yüksek teknolojiye sahip izleme ekipmanlarına sahip hava aracının değeri 120 milyon dolar olarak belirtilmiştir. 2016 yılında ABD'ye ait RQ-170 model insansız hava aracı yine İran tarafından düşürülmüş ve İran siber ordusu tarafından aracın kriptografisi çözülmüş ve aynı özelliklerde araçlar İran tarafından üretilmeye başlanmıştır. Silah olmayan orijinal modeline silah aparatları da ekleyerek mevcut RQ-170'i daha da geliştirilmiştir (Aksan, 2019). 20 Haziran 2019 tarihinde düşürülen hava aracının da benzer bir durumla karşı karşıya kalmasını istemeyen ABD bu noktada İran ile bir siber savaşa başlamıştır. ABD'nin siber savaş tehdidinin akabinde ilk saldırılar ise İran'dan gelmiştir. Amerikan hükümeti ve birtakım Amerikan şirketleri hedef alınmıştır. Amerika Birleşik Devletleri siber ordusu ise İran'ın petrol tankerlerini hedef almasına yönelik geliştirdiği sistemlere zarar vermiştir. İran kendi kurmuş olduğu takip sistemleri ile körfezde gerçekleşen petrol nakliyesini takip edebiliyordu ve bu doğrultuda bir takım casus programlar geliştirmişti. Amerika Birleşik Devletleri bu programları hedef almış ve ilgili veri tabanını silmiştir (Sözen, 2019).

Birleşik Devletler Siber Ordusu genellikle Ulusal Güvenlik Ajansı ile beraber hareket etmektedir. Ulusal Güvenlik Ajansı'nın başkanı ise aynı zamanda siber ordunun da komutanıdır.

b) Rusya Federasyonu

Rusya'nın Amerika'da olduğu gibi resmi bir siber ordu yapılanması mevcut değildir. Rusya ordusu hava, kara, deniz, uzay ve stratejik füze kuvvetleri olmak üzere 5 kuvvet komutanlığından oluşmaktadır. Resmi bir komutanlık kurulmamış olmasına rağmen Rusya'nın da siber alandaki devlet ölçekli faaliyetleri oldukça eskiye götürülebilir. 1980'lerde SSCB ordusunda görev yapan Mareşal Nikolai tarafından "Askeri Meselelerde Devrim" ismi verilen bir program başlatılmış ve ordu faaliyetleri ilk kez sanal alana da taşınmıştır. Oluşturulan bu programda ordunun otomasyona geçmesi, orduda bilişim eğitimlerinin sağlanması, bilgisayar envanterin çıkarılması gibi bir takım durumların gerçekleşmesi söz konusu olsa da ilerideki gelişmeler açısından öncü bir nitelik taşımıştır. Rusya siber ordu konusunda atılımı ise 1. Körfez Savaşı sonrası gerçekleştirmek istemiştir. Savaş esnasında Amerika'nın kullandığı siber faaliyetlerin etkisine şahitlik eden ve durumu yakinen izleyen Sovyetler Birliği, siber ordu konusunda adım atmak istemiştir ancak iç siyasi çalkantılar ve ardından gelen dağılma dönemi ile psikolojik, sosyolojik ve ekonomik anlamda çöküntüye uğrayan Rusya'nın yeniden toparlanması

oldukça uzun sürmüştür. Ancak 2000'lere gelindiğinde yeniden bu tartışmalar gündeme alınabilmiştir (Darıcılı & Özdal, 2017, s. 124).

09.09.2000 tarihinde Rusya Enformasyon Güvenliği Doktrini yayınlanmıştır. Doktrinde bilgi güvenliği, amaçlar, sanal gelecek gibi pek çok konu ele alınmıştır. Rusya Enformasyon Güvenliği Doktrini Rusya'nın siber güç olma yolundaki ilk belgesi olarak kabul edilmektedir.

12 Mayıs 2009 tarihinde "2020'ye Doğru Ulusal Güvenlik Strateji Belgesi" ilan edilmiştir. Bu belge Rus istihbaratına bir rehber görevi görmek ve ulusal güvenlikteki gerekli rolleri ortaya koyması açısından önemlidir. Belgede, gelişen teknolojinin aynı zamanda pek çok riski de beraberinde getirdiğine değinilmiştir.

2011'de ise "Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler" isimli bir belge yayımlanmıştır. Rus Siber Savaş Doktrini olarak da belirtilen bu belgede siber savaşın mantığına vurgu yapılmıştır. Buna göre ulusal bilgi sistemlerine zarar veren, hükümeti ve toplumu bu yolla etkilemeye çalışan, Rus kültürünü, sosyolojisini ve ekonomisini yok etmeye çalışanlara karşı gerçekleştirilecek enformatik faaliyetler siber savaşın mantığını oluşturmaktadır (Darıcılı & Özdal, 2017, s. 125).

Rusya'da resmi bir siber komutanlık olmamasına karşın ordunun ve istihbarat servisinin bünyesinde siber yapılanmalar mevcuttur. Siber savunma; Federalnaya Slujba Bezopasnosti (Rusya Federal Güvenlik Servisi/FSB), SluzhbaVneshney Razvedki (Rusya İstihbarat Servisi/SVR) ve Glavnoye Razvedyvatel'noye Upravleniye'nin (Rusya Askeri İstihbarat Kurumu/GRU) müşterek faaliyetleri ile yürütülmektedir.

FSB (Rusya Federal Güvenlik Servisi) devlet güvenliğine yönelik faaliyetlere karşı istihbarat toplamakla görevlidir. KGB'nin devamı niteliğinde olan kurum özellikle ayrılıkçı grupların durumlarını kontrol altında tutmaya çalışmaktadır. Fakat bunun yanında FSB'nin siber güvenlik ile ilgili rolü de bulunmaktadır. Bu bağlamda, Rusya vatandaşı veya yabancı kişilerin telekomünikasyon bilgilerini kontrol etmek görevlerinden bir tanesidir. FSB'nin Rusya içi siber etkinliğinin fazla olduğu bilinmektedir.

SVR (Rusya İstihbarat Servisi) ise ülke dışındaki istihbarat faaliyetlerinden sorumlu olan kurumdur. Genellikle GRU ile birlikte istihbarat toplamakta olan SVR başta SSCB'den ayrılan ülkeler olmak üzere, Suriye, Küba, Vietnam gibi pek çok ülkede espiyonaj faaliyeti göstermektedir. Rus menşeili bir takım yazılımlar ve uygulamalar vasıtasıyla uluslararası casusluk faaliyetlerinde bulunduğu iddia edilmektedir.

GRU (Rusya Askeri İstihbarat Kurumu) ise genellikle diğer istihbarat örgütleri arasındaki dengeyi sağlamakla görevlidir.

2014 yılında Sergei Shoigu Rus ordusunun siber savunmasını şu sözlerle aktarmıştır: "Rus ordusu siber tehditler karşısında giderek bağımsız bir yapılanmaya kavuşmak-

tadır. Hükümet olarak bu amaçla 500 milyon dolar bütçe ayırdık. Faaliyetler hem yurt içi hem de yurtdışında sürecektir. Bunun için insan kaynağı envanterini genişletip yazılım uzmanları ve yabancı dil bilen personel istihdam edeceğiz" demiştir (Darıcılı & Özdal, 2017, s. 131).

Sonraki yıllarda ise yazılım alanında uzmanlaşan üniversite öğrencilerinin orduya katılmasına yönelik girişimlerde bulunulmuştur. Alanında uzman bilgisayar mühendislerine, programcılara, web tasarımcılarına, orduya katılmak için gereken bir takım kriterlerden muaf olacak şekilde, orduya katılmaları için teklifler götürülmüştür (Saygun, 2017).

Son yıllarda ise Rus devlet kurumlarına ait internet siteleri ise oldukça fazla siber saldırıya maruz kalmıştır. Saldırılar genellikle Amerika ve Avrupa ölçekli olmuştur. Rusya Federal Eğitim ve Bilim Denetim Servisi'nin resmi sitesi Haziran 2019'da saldırıya uğramış ve bir süre lise öğrencilerinin katılmış olduğu sınavlara erişim sağlanamamıştır (Sputnik News, 2019). Saldırı daha büyük sonuçlar yaratmadan atlatılsa da Rusya'da bu konuda ciddi çalışmalar yapılması gerektiği konusunu bir kez daha gündeme getirmiştir.

Tüm bu tehditler neticesinde oldukça radikal bir adım atan Rusya bir süredir gerçekleştirmeyi planladığı internet uygulamasını 24 Aralık'ta düzenlemiş ve bu tarihte tüm dünya ile olan internet bağlantısını kesmiştir. Kimi kaynaklar bunun bir siber saldırı tatbikatı olduğunu belirtirken Rusya ise ülkenin ulusal internet altyapısının küresel DNS'ye bağlı kalmadan çalışıp çalışmayacağına yönelik bir deneme yapıldığını ve sonucun olumlu olduğunu belirtmiştir. Buna göre olası bir siber saldırı altında Rusya istediği anda uluslararası internet ağından ayrılabilecek (Baki, 2019). Hem Rus devlet kurumuna ait internet siteleri hem de Rusya ölçekli firmalara ait internet sitelerini kapsayacak şekilde kurulan bu intranet ağı olası siber saldırılardan ülkenin en az zararı görmesini sağlayacak.

c) İran

Ortadoğu coğrafyasına bakıldığı zaman etrafında en fazla düşman unsuru bulunduran ülkelerden birisi İran'dır. Bu durum GSYH ile karşılaştırıldığında İran'ın savunma harcamalarının daima yüksek bir harcama kalemi oluşturmasına yol açmaktadır. İran, bir caydırıcılık unsuru olarak da elinde daima nükleer gücü bulundurmaktadır; ancak İran'ın varlığı ve savunma harcamaları da diğer ülkeler açısından bir tehdit unsuru olarak kabul edilmektedir. Bundan ötürü İran İslam Devrimi'nden beri süregelen adı konulmamış bir savaş hali yaşanmaktadır. Bu kimi zaman İran-Irak Savaşı gibi sıcak çatışma halinde yaşansa da çoğu zaman ambargolar veya bir takım engellemelerle devam etmektedir.

İran'ın yeni savaş düzeninin sanal dünyaya da taşındığını idrak etmesi 2010'ların başlarında olmuştur. İran'daki, başta nükleer tesislerdeki bilgisayarlar olmak üzere, pek çok bilgisayarda Flame ismi verilen bir virüs keşfedilmiştir. O zamana değin geliştirilen virüsler genellikle bilgisayar sistemlerini çökertmek için kullanılırken bu virüs bilgisayar ara birimlerini çalıştırabilecek bir takım özelliklere sahiptir. Öyle ki bilgisayarda

mevcut mikrofon özelliklerini açarak virüsün etkileşim halinde olduğu programcıya ses kayıtları başta olmak üzere tüm bilgisayar verilerini gönderebilmekteydi. İran Petrol Bakanlığı virüsten kimin sorumlu olduğunu bilmediklerini ifade etse de İsrail Başbakan Yardımcısı Moşe Yalon'un İran'ın nükleer çalışmalarını bertaraf etmek için siber saldırıların olabileceğini söylemesi olayın failinin kim/kimler olduğunu özetler nitelikte olmuştur (Köylü, 2012).

İran siber dünyada da etkinliği artırmak istemiş ve ilk büyük saldırısını Ağustos 2012 tarihinde gerçekleştirmiştir. Suudi Arabistan'a ait petrol şirketi Saudi Aramco'yu hedef alan siber saldırılar başlatılmıştır. Saldırılar sonucunda kuruma ait bilgisayarların yarısı (30 bin adet bilgisayar) devre dışı bırakılmış ve bilgisayarlardaki mevcut veriler silinmiştir. Ancak verilerin kopyalanıp kopyalanmadığı bilgisine ulaşılamamıştır. Hemen ardından Katar'ın doğalgaz şirketi Ragas da bu virüsün hedefi olmuştur. Aramco kadar ciddi etkileri olmamakla birlikte Ragas da bu virüsten büyük oranda zarar görmüştür. İran resmi bir açıklama yapmamış olsa da virüsün içeriği ve saldırı zamanlaması İran'ı işaret etmektedir. Virüsün kodlarında İran'ın kutsal değerlerine ait ifadeler geçmekte olup saldırının Kadir gecesi düzenlenmesi ve aynı zamanda saldırıyı gerçekleştiren grubun kendilerine "Hz. Ali'nin Kılıcı" ismini takmış olması gibi pek çok unsur şüpheleri doğrudan İran'a yöneltmektedir. Virüsün bulaştığı bilgisayarlarda ise yanmış bir Amerikan bayrağı resmi bulunmakta idi (Çelik, 2014).

Bu olaydan 4 yıl sonra Aralık 2016 tarihinde yine aynı firmalar bu virüsün saldırısına uğramış ancak verilen zararla ilgili bir açıklama yapılmamıştır. Bu defa bilgisayarlara ise boğularak hayatını kaybeden 4 yaşındaki Suriyeli mülteci Aylan Kurdi'nin fotoğrafı konulmuştur (Çelik, 2016).

İran'da çok güçlü bir siber saldırı ekibinin olduğu bilinmekle beraber İran'da da Rusya'da olduğu gibi ordu içerisinde resmi bir yapılanma mevcut değildir. İran resmi makamlarınca bu konu ile ilgili bir açıklama yapılmazken son yıllarda İranlı hacker sayısındaki artış dikkat çekmiştir. APT33 isimli bir hacker grubunun İran'ın resmi siber ordusu olduğu iddia edilmektedir; ancak İran tarafından henüz resmi bir açıklama yapılmamıştır. Genellikle havacılık ve enerji sektöründe faaliyet gösteren Suudi ve Amerikan kuruluşlarını hedef alan APT33 grubunun son olarak, Amerikalı mail servisi Microsoft Outlook'u saldırı düzenlendiği bilinmektedir. Amerika Birleşik Devletleri Siber Komutanlığı ise güvenlik açıklamaları konusunda endişelerini aktarmış ve güvenlik açıklarından yararlanarak sızmaların genellikle İran destekli APT33 tarafından gerçekleştirildiğini belirtmiştir (Yinanç, 2019).

d) Türkiye

Türkiye'de de uzun zamandır siber alana yönelik çalışmalar hız kazanmış ve bir siber komutanlık kurulmasına yönelik çalışmalar yapılmıştır. Ancak henüz kara, deniz ve hava kuvvetlerine bir kuvvet komutanlığı olarak siber komutanlık eklenmemiştir. 2012 yılında TSK Siber Savunma Merkezi Başkanlığı kurulmuştur. Bu kurum 2013 ta-

rihinde "TSK Siber Savunma Komutanlığı"na dönüştürülmüştür. Ancak Siber Savunma Komutanlığı'nın amacı Türk Silahlı Kuvvetleri'nin ve Genelkurmay Başkanlığı'nın internet sitelerini korumak ve olası saldırıları engellemek olarak tanımlanmıştır. Yani bir sanal muharebeden ziyade savunma işlevi ile donatılmıştır. TSK yetkilileri nükleer saldırı tehditlerinden sonra siber saldırıların dünyadaki en büyük ikinci tehdit unsuru haline geldiğini belirtmiş ve NATO ile müşterek halde siber savunmanın gerçekleştirildiğini belirtmiştir (Uslu, 2016). Ardından Cumhurbaşkanlığı Savunma Sanayi Başkanlığı bünyesinde Siber Savunma Merkezi Projesi için çalışmalara başlanmış ve 2018'in ilk yarısında ordunun gerekli siber donanıma sahip olması için gereken faaliyetlerin gerçekleştirilmesi planlanmıştır (T.C. Savunma Sanayii Başkanlığı , 2016). Ancak istenen başarı sağlanamamıştır.

Türkiye'de henüz silahlı kuvvetlere bağlı bir siber bir kuvvet komutanlığı bulunmamakla birlikte bir siber ordu kurulması için bakanlıklarda da çalışmalar gerçekleştirilmiştir. 2013 yılında başta Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na bağlı olarak kurulan, ardından Bilgi Teknolojileri ve İletişim Kurumu bünyesinde devam eden Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. Kurum, siber saldırılarının tespit ve bertaraf edilmesinde kamu ve özel kişiler arası koordinasyonun sağlanmasında görev yapmaktadır. Ayrıca 2017 yılında yaptığı bir konuşmada Ulaştırma, Denizcilik ve Haberleşme Bakanı Ahmet Arslan tarafından Türkiye'nin çeşitli devlet kurumlarında 13 bin beyaz şapkalı hackerın görev yaptığı ifade edilmiştir (Babacan, 2017). Bununla beraber 2013 yılında Emniyet Genel Müdürlüğü bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı kurulmuştur. Bu birimin öncelikli amacı internette ve internet vasıtasıyla gerçekleşen suçlarla mücadele olarak tanımlanmıştır. Siber ordu niteliği taşımasa da siber suçlara karşı caydırıcılık sağlaması açısından faydalı bir girişim olarak görülmektedir.

Türkiye'ye yönelik siber saldırılar genellikle bankacılık veya hizmet sektöründeki firmalara yönelik olmuştur. 28 Ekim 2019 tarihinde Garanti BBVA'ya yönelik bir takım siber saldırılar gerçekleşmiştir. Kurum yöneticileri müşterilerine ait bilgilerin çalınmadığını; yalnızca internet servislerinde bir takım yoğunlukların yaşandığını dile getirmişlerdir (Hürriyet, 2019).

26 Aralık 2019 tarihinde ise Kişisel Verileri Koruma Kurumu, Türkiye'nin en büyük e-alışveriş sitelerinden biri olan n11.com'dan üyesi olan 832 adet müşterinin e-posta adresinin çalındığını duyurmuştur. İnternet ortamında yapılan alışverişlerde kişilerden cep telefonu numaraları, ev adresleri, bazı özel bilgilerinin istendiği düşünüldüğünde oldukça büyük oranda bir veri sızıntısı riskinin olduğu öngörülmektedir (KVKK, 2019).

Tüm bu sebeplerle Türkiye'nin prorfesyonel anlamda bir siber komutanlığa sahip olması bir zorunluluk arz etmektedir. Özellikle son zamanlarda gerçekleştirilen saldırılarda nükleer santrallerin ve enerji santrallerinin başlıca hedefler olduğu görülmektedir. Türkiye nükleer enerji konusunda henüz yeterli bilgi birikimine sahip olmamakla birlikte hali hazırda Sinop ve Mersin'de iki adet nükleer santral yapım projesine sahiptir. Nükleer santrallerin Türkiye'ye için getirilerinin oldukça fazla olacağı düşünülmektedir.

Bundan ötürü olası saldırılar karşısında da Türkiye'nin kendisini korumak ve gerekli caydırıcılığı sağlamak adına ordu bünyesinde bir yapılanmaya gitmesi konusunda zorunluluk doğmaktadır. Sadece nükleer enerji değil günümüzde gelişen elektrikli otomobillerden yapay uydulara kadar pek çok sistem siber tehdit altındadır. Örneğin, Chris Roberts isimli bir siber güvenlik uzmanı NASA'nın internet sistemlerine girerek buradan Uluslararası Uzay İstasyonu'na giriş protokollerini elde edebilmiştir (Tolga Yanık, 2019). Türkiye'nin de son yıllarda Göktürk uyduları aracılığı ile bu alanda yatırım yaptığı düşünüldüğünde yine bir korunma ihtiyacı ortaya çıkmaktadır.

e) Sonuç

Hem ülkemizde hem de dünyada artık önü alınamaz bir şekilde teknolojiyle bütünleşme durumu yaşanmaktadır. Bunun yararları gündelik hayatın pek çok noktasında kendini göstermektedir. Örneğin, akıllı telefonlar ile binlerce kilometre mesafedeki insanlarla sesli ve görüntülü iletişim kurulabilmekte veya onlarca kitabın içerikleri küçük cihazlara yüklenerek her an ulaşılabilir olmaktadır. Teknolojinin faydaları oldukça uzun bir liste oluşturacaktır. Aynı şekilde teknolojinin zararları ve yarattığı riskler azımsanmayacak bir miktara ulaşmaktadır. Örneğin, 2019 yılında gerçekleştirilen bir araştırmada insanların %67'sinin online alışverişi tercih ettiği gözlenmiştir (Sakarya & Yardımcı, 2019). Böylesine büyük bir rakam dolandırıcılık ve hırsızlık yöntemlerinin de sanal ortamlara taşınmasına yol açmıştır. Bunun yanında sosyal medya kullanımı beraberinde insanların özel bilgilerinin istismarı gibi durumları da gündeme getirmiştir. Fakat yaratacağı büyük olumsuzluklar ve etki alanının genişliğinden ötürü devletler seviyesinde yaşanan siber güvenlik sorunları bireysel risklerden daha öncelikli olmaktadır. ABD tarafından İranlı General Kasım Süleymani'ye düzenlenen suikast sonrası dünya gündeminde ilk dillendirilen konu İran'ın siber bir saldırı hazırlığı yapıp yapmadığı olmuştur (Seldin, 2020). Bir savaş senaryosunda dahi ilk ortaya atılan durum fiziki saldırı değil sanal bir saldırı durumu olmuştur. Bu durum dahi gelecekte siber saldırıların ve siber savaşların rolüne dair bir ipucu niteliğindedir.

Sonuç olarak savaş paradigmasında geleneksel orduların halen en etkin güç olmasının yanında bu ordulara aynı zamanda siber orduların da eklenmesi bir zorunluluk haline gelmektedir. Devletlerin, kurumların ve kişilerin internet üzerinde de bir mevcudiyeti bulunmaktadır ve tıpkı fiziksel olarak bunların korunması gerektiği gibi sanal anlamda da korunması bir gereklilik arz etmektedir. Bu bakımdan özellikle ülkemiz bünyesinde geç kalınmadan gerekli donanım sağlanmalı ve etkin bir siber ordu kurulmasına yönelik çalışmalara başlanmalıdır. Ancak siber ordu kurmak tek başına yeterli bir girişim olmayacaktır. Teknoloji ve insan kaynağı bakımından sürekliliğin sağlanması, kullanılan teknolojinin millileştirilmesi, bu alanda faaliyet gösteren kamu kurumlarının ve özel sektör kuruluşlarının koordine edilmesi, yükseköğrenim seviyesinde AR-GE faaliyetlerinin teşvik edilmesi siber orduların kurulması ve güçlendirilmesi için stratejik öneme sahip adımlar olarak öne çıkmaktadır.

Etik Beyanı: Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu yazar beyan eder. Aksi bir durumun tespiti halinde Kamu Yönetimi ve Teknoloji Dergisinin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalış-manın yazarlarına aittir.

Yazar Katkıları: Meryem Orak çalışmanın tamamında tek başına katkı sunmuştur.

Çıkar Beyanı: Yazar ya da herhangi bir kurum/ kuruluş arasında çıkar çatışması yoktur.

Teşekkür: Yayın sürecinde katkısı olan hakemlere teşekkür ederim.

Ethics Statement: The author declares that the ethical rules are followed in all preparation processes of this study. In the event of a contrary situation, the Journal of Public Administration and Technology has no responsibility and all responsibility belongs to the author of the study.

Author Contributions: Meryem Orak has contributed to all parts and stages of the study

Conflict of Interest: There is no conflict of interest among the author and/or any institution.

Acknowledgement: I would like to thank the referees who contributed to the publication process.

Kaynakça

Aksan, S. (2019, Haziran 20). *Yeni Şafak*. Aralık 31, 2019 tarihinde https://www.yenisafak.com/gundem/iranin-abd-ucagini-dusurmesi-nasil-sonuclar-doguracak-3495626 adresinden alındı

Babacan, N. (2017, Mayıs 17). *Hürriyet*. Ocak 17, 2020 tarihinde http://www.hurriyet.com.tr/gundem/13-bin-hackerla-siber-ordu-40461432 adresinden alındı

Baki, O. (2019, Aralık 23). *Webtekno*. Aralık 31, 2019 tarihinde https://www.webtekno.com/rusya-kuresel-internet-agiyla-baglantisini-kesti- h82374.html adresinden alındı

Copeland, B. J. (2004). *The Essential Turing.* New York: Oxford University Press.

Çelik, M. (2014, Ağustos 29). *Siber Bülten*. Aralık 31, 2019 tarihinde https://siberbulten.com/makale-analiz/turkiyenin-kacan-son-firsati-suudi- siber-komutanligi/ adresinden alındı

Çelik, M. (2016, Aralık 26). *Siber Bülten*. Aralık 31, 2019 tarihinde https://siberbulten.com/uluslararasi-iliskiler/shamoon-kabusu-4-yil-sonra- geri-dondu/ adresinden alındı

Darıcılı, A. B., & Özdal, B. (2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi. *Bilig*, 121-146.

DARICILI, D. A. (2017). *Amerika Birleşik Devletleri'nin Siber Kapasitesinde Rol Oynayan Kurumsal Yap Ilanmaların Analizi.* Bursa: Dora Basım Yayım Ltd. Şti.

Köylü, H. (2012, Mayıs 12). *Deutsche Welle* Türkçe. Aralık 31, 2019 tarihinde https://www.dw.com/tr/en-tehlikeli-vir%C3%BCs-flame/a-15988868 adresinden alındı

Lukasik, S. J. (2011). Why the Arpanet Was Built. *IEEE Computer Society*, 4-21.

Sakarya, G., & Yardımcı, N. (2019, Mart 29). *TRT Haber*. Ocak 16, 2020 tarihinde https://www.trthaber.com/haber/yasam/turkiye-alisverisi-internetten-mi- yoksa-magazadan-mi-yapiyor-410153.html adresinden alındı

Saygun, M. (2017, Ocak 17). *Cybermag*. Aralık 31, 2019 tarihinde https://www.cybermagonline.com/rus-siber-ordusu-suvarilerini-nasil- toplu-yor adresinden alındı

Seldin, J. (2020, Ocak 11). *Voice of America*. Ocak 16, 2020 tarihinde https://www.amerikaninsesi.com/a/iranin-siber-saldirilar%C4%B1na-karsi- abd-alarmda/5241558.html adresinden alındı

Sözen, M. (2019, Eylül 2). *Siber Bülten*. Aralık 31, 2019 tarihinde https://siberbulten.com/uluslararasi-iliskiler/abd-siber-saldiriyla-iranin-kritik- veri-tabanini-sildi/ adresinden alındı

Sputnik News. (2019, Haziran 2). Ocak 16, 2020 tarihinde https://tr.sputniknews.com/rusya/201906021039225374-rus-egitim-denetim- kurumuna-siber-saldiri/ adresinden alındı

T.C. Savunma Sanayii Başkanlığı. (2016, Temmuz 24). https://www.ssb.gov.tr/Website/contentlist.aspx?PageID=1083&LangID=1 adresinden alındı

Tolga Yanık, M. T. (2019, Nisan 27). *Anadolu Ajansı*. Ocak 31, 2020 tarihinde https://www.aa.com.tr/tr/bilim-teknoloji/canim-sikildi-nasayi- hackledim/1463872 adresinden alındı

Uslu,S. (2016, Haziran 4). *Anadolu Ajansı*. Ocak 17, 2020 tarihinde https://www.aa.com.tr/tr/turkiye/turk-ordusunun-yeni-kuvveti-siber- savunma/584061 adresinden alındı

Yayla, M. (2013). HUKUKİ BİR TERİM OLARAK "SİBER SAVAŞ". *TBB Dergisi*, 178-202.

Yazıcı, M. (2015, Mayıs 23). *TUIC Akademi*. Aralık 31, 2019 tarihinde http://www.tuicakademi.org/stuxnet-virusu-iran-a-nasil-etki-etti/ adresinden alındı

Yinanç, B. (2019, Temmuz 8). *Hürriyet*. Aralık 31, 2019 tarihinde http://www.hurriyet.com.tr/teknoloji/iranli-hacker-grubu-outlook-uzerinden-kurbanlarini-vuruyor-41267003 adresinden alındı