International Journal of Business, Economics and Management Perspectives

Uluslararası İşletme, Ekonomi ve Yönetim Perspektifleri Dergisi

Volume/Cilt: 6, Issue/Sayı: 2, pp/ss. 414-439
E-ISSN: 2458-8997
URL: https://ijbemp.com
DOI: http://dx.doi.org/10.29228/ijbemp.66305
December / Aralık 2022

Article Type / Makale Türü
Araştırma Makalesi - Research Article

Application Date / Başvuru Tarihi
10.11.2022 / 11.10.2022

Admission Date / Yayına Kabul Tarihi
12.27.2022 / 27.12.2022

ABD-RUSYA İLE İLİŞKİLENDİRİLEN SİBER SALDIRILAR VE TÜRK KAMU YÖNETİMİNCE ALINMASI GEREKEN ÖNLEMLER*

CYBER ATTACKS RELATED TO US-RUSSIA AND MEASURES TO BE TAKEN BY THE TURKISH PUBLIC ADMINISTRATION

Ferit GÜVEN[1], Mehmet AKTEL[2]

ÖZ: Kamu yönetiminin karşılaştığı tehditlerden birisi de devlet destekli siber saldırılardır.Devlet destekli siber saldırılar; devletlerin bizzat desteklediği, yönettiği, bir başka gruba yaptırttığı ya da başka bir devletle işbirliği içinde gerçekleştirdiği, parasal, teknik ve yasal destek sağladığı, stratejik, siyasi, jeopolitik, ekonomik, askeri, istihbarat, endüstri, teknoloji konularındaki hedeflerine ulaşmak için başvurdukları saldırılardır. Siber uzayda, artık en tehlikeli ve zarar verici siber saldırı kaynağı devlet dışı aktörler değil, ulusal stratejilerine siber saldırı yeteneği ekleyen devletlerdir. Bu çalışmada Amerika ve Rusya'nın yaptığı ya da yaptırtığı siber saldırı örneklerinin bir kısmı incelenerek, Türk kamu yönetim sisteminin devlet destekli siber saldırılara karşı ne gibi önlemler alması gerektiği üzerinde durulmaktadır. Önerilen önlemler, devlet destekli siber saldırılara karşı Türkiye'nin yeni bir model oluşturmasına katkı sağlamayı amaçlamaktadır. Sonuç olarak Türk kamu yönetim sisteminin mevzuattan kurumsallaşmaya kadar siber saldırılara karşı yeterli bir donanıma sahip olmadığı görülmektedir. Bu yöndeki çalışmalar ivmelendirilmelidir.

Anahtar Kelimeler : Türk Kamu Yönetimi, Siber Saldırılar, ABD, Rusya.

ABSTRACT: One of the threats faced by the public administration is state-sponsored cyber attacks. State-sponsored cyber attacks; These are the attacks that the states personally support, manage, have another group do or carry out in cooperation with another state, provide financial, technical and legal support, and apply to achieve their goals in strategic, political, geopolitical, economic, military, intelligence, industry and technology. In cyberspace, the most dangerous and damaging source of cyberattacks is no longer non-state actors, but states that add cyberattack capability to their national strategies. In this study, some of the examples of cyber attacks that the USA and Russia have made or have made are examined, and it is emphasized what precautions the Turkish public administration system should take against state-sponsored cyber attacks. The proposed measures aim to contribute to Turkey's creation of a new model against state-sponsored cyber attacks. As a result, it is seen that the Turkish public administration system does not have sufficient equipment against cyber attacks, from legislation to institutionalization. Work in this direction should be accelerated.

Keywords: ***Turkish Public Administration, Cyber Attacks, USA, Russia.***

* Bu çalışma, Süleyman Demirel Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, doktora programında Prof. Dr. Mehmet Aktel danışmanlığında yürütülen ve Ferit Güven tarafından yazılan "Siber Saldırılar ve Türk Kamu Yönetiminin Çözümleri" isimli tezden türetilmiştir.

1. Dr., Bağımsız Araştırmacı, feritguven@hotmail.com, https://orcid.org/0000-0003-2401-7897
2. Prof. Dr., Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, mehmetaktel@sdu.edu.tr, https://orcid.org/0000-0001-6417-8498

EXTENDED SUMMARY

Research Problem

The research problem of the study titled "Cyber Attacks Associated with the USA-Russia and the Precautions to be Taken by the Turkish Public Administration" is aimed at investigating whether the Turkish Public Administration System is prepared for state-sponsored cyber attacks.

Research Questions

The main question of the study focuses on the Turkish Public Administration System (state), creating a structure that includes sufficient precautions against state-sponsored cyber attacks.

Literature Review

In the study, cyber attacks associated with the USA and Russia are examined through domestic and mainly foreign literature. The analysis is based on the content analysis of theoretical sources. The literature review was made through books, articles and internet resources. In the study, cyber attack evaluations about both countries are included. The cyber attack measures that the Turkish Public Administration System should take and a new administrative restructuring recommendation based on this constitute the main axis of the study.

Methodology

This article is based on the analysis of these documents, especially by scanning foreign sources. The information collected for the study was examined in the context of the Turkish administrative system, and suggestions were made for a new security structure.

Results and Conclusions

When we look at the findings of this study, it is seen that states have very important roles in providing cyber security. It is emphasized in the study that states should produce solutions in the form of protection, detection and response against cyber attacks. In addition, it has been determined that states should create cyber security strategies, appropriate institutional structures, legal regulations and budgets for the fight..

1. GİRİŞ

Siber uzayın karanlık tarafında kamu yönetiminin karşılaştığı tehditlerden birisi de devletler ile ilişkilendirilen (devlet destekli) siber saldırılardır. Siber uzayı hackerlar, hacktivist gruplar, içeridekiler, terör örgütleri, organize suç örgütleri siber saldırılar ile tehdit etmektedir. Ancak sınırsız siber uzayda, en tehlikeli ve en çok zarar verici siber saldırı kaynağı devlet dışı aktörler değil, ulusal stratejilerine siber saldırı yeteneği ekleyen devletlerdir. Devletler, siber saldırılara karşı siber saldırganları suçlasa da en zararlı siber saldırgan ve en tehdit edici güç gene devlettir. Devletlerle ilişkilendirilen ya da devlet destekli siber saldırılar, kamu yönetiminin kontrolündeki kritik altyapılara karşı yapılabilecek en yıkıcı siber saldırılar olacaktır (Lewis, 2018: 2, 3, 7).

Devlet destekli siber saldırılar; devletlerin arkasında olduğu, bizzat desteklediği, yönettiği, bir başka gruba yaptırttığı, ya da başka bir devletle işbirliği içinde gerçekleştirdiği, mali, teknik ve yasal destek sağladığı, stratejik, siyasi, jeopolitik, ekonomik, askeri, istihbarat, endüstri, teknoloji konularındaki hedeflerine ulaşmak için başvurdukları siber saldırılardır. Devlet destekli/ilişkili siber saldırılar, dünya genelinde artan bir şekilde uygulanmakta olan, bir siber saldırı çeşidi olarak karşımıza çıkmaktadır (Rainie vd., 2019: 64).

Devletler için, siyasi ve ekonomik etki yaratmak, karşı devletin kendi istediği bir kararı almasını sağlamak ya da istediğini alamayınca cezalandırmak için füzeleri kullanmak yerine günümüzde siber saldırılar yapılmaktadır. Düşük yoğunluklu çatışmalarda, kısa süreli operasyonlarda, savaşta ya da askeri harekât öncesi savaş alanını şekillendirmek, karşı tarafı zayıflatmak ve elindeki siber altyapıya dayandırılmış sistemleri etkisiz hale getirmek için devletler siber saldırı seçeneğini uygulamaktadırlar. Devletler, bazen de başka bir devletin başına bela olan hacker veya hacker gruplarının siber saldırılarını ya da hacktivistlerin siber eylemlerini destekleyebilmektedirler.

Devletler, politik baskı, siyasi kararları manipüle etmek, antlaşma öncesi masada elini güçlendirmek, savaş öncesi harekât sahasını şekillendirmek, düşmanın kritik altyapılarını kullanılamaz hale getirmek, diğer ülkenin savaşma azim ve iradesini kırmak, ekonomik karmaşa ve kayıp yaşatıp kendine müzahir olmasını sağlamak, gücünü göstermek, gözdağı vermek, kendisi için asıl tehdit olan büyük güce kendi siber yeteneklerini uygulayabilme seviyesini göstermek için siber saldırılar yapmaktadırlar. Siber saldırılar devletler için aynı zamanda kara, deniz, hava taarruzlarına göre ya da nükleer saldırıya göre daha ucuzdur. Saldırı sonucu oluşan yıkım ya da can kaybı diğerlerine göre daha azdır. Savaş sonrası yeniden oluşturulabilme imkânı sağlar ve uluslararası toplumun daha az tepkisini çeker (Lewis, 2018: 18, 27).

Günümüzde devletler savaşlarda kullandıkları tonlarca bombaların yarattığı yıkıma benzer bir zararı artık bir tuşla yapabilecek siber saldırı yeteneğine kavuşmuşlardır. Devletler bir taraftan siber güvenlik ve siber savunma çalışmaları yaparken diğer taraftan da siber saldırı hazırlıkları yapmakta ve açıkça ilan etmeden direkt saldırmaktadırlar (Peters, 2018: 13-15). Bazıları çoktan siber yeteneklerini

sahada sergilemeye ve bir güç unsuru olarak kullanmaya başlamışlardır. Bu konuda öne çıkan ve siber uzayda saldırı bağlamında aktif ve etkin olan ülkeler ABD, Rusya, Çin, İran, İsrail, Suriye ve Kuzey Kore'dir (Coburn, 2019: 142-143). İkinci Dünya Savaşı'ndan sonra süper güçlerin oluşturduğu ittifaklar arasında geçmişte gerçekleşen soğuk savaş şimdilerde siber savaşlara dönüşmüştür.

Çalışmada ABD ve Rusya ile ilişkilendirilen siber saldırı örnekleri yerli ve ağırlıklı olarak yabancı literatür üzerinden, içerik analizi yöntemi ile incelenmektedir. Metnin geneline bakıldığında; Trans-Sibirya Boru Hattı Patlaması/Siber Saldırısı, I. Körfez Savaşı / Çöl Fırtınası Operasyonu, Kosova Savaşı / Müttefik Güç Harekâtı, Kalıcı Özgürlük Operasyonu ve Irak'ın Özgürlüğü Operasyonu, Birleşik Koruyucu Operasyonu, Stuxnet, Edward Snowden Sızıntısı ve PRISM Veri Toplama Programı, Çeçenistan'a Yönelik Siber Saldırılar, Estonya'ya Yönelik Siber Saldırılar, Litvanya'ya Yönelik Siber Saldırılar, Gürcistan'a Yönelik Siber Saldırılar ve Ukrayna'ya Yönelik Siber Saldırı örnekleri incelenmiştir. İnceleme sonrası elde edilen veriler ışığında Türk Kamu Yönetim sistemine siber saldırılara karşı önerilerde bulunulmuş ve bu öneriler doğrultusunda yeni bir yapılanma ihtiyacı olduğu ortaya konulmuştur.

2. ABD İLE İLİŞKİLENDİRİLEN SİBER SALDIRILAR

Siber uzayda hackerlar, hacktivistler, içeridekiler, organize suç örgütleri, teröristler gibi siber saldırı aktörleri arasında siber operasyonlara karar veren unsurlardan birisi de devletlerdir (Lemieux, 2019: 141-142). Devletler için siber saldırılar, en az güç kullanarak en fazla etki yaratmadaki en etkin güç kullanımıdır. Karşı tarafta hem siber altyapısına zarar verirken hem de fiziksel zararlara da neden olabilmektedir. Karşı devleti hem tehdit etmek hem de politik baskı yapmak bağlamında, bir taraftan da uluslararası oluşabilecek bir karar aşamasında diğer çekimser devletlere karşı da gözdağı vermek anlamında siber saldırıları en iyi kullanan ülkeler arasında ABD ve Rusya bulunmaktadır. ABD ve Rusya'nın dış politikada baskı aracı olarak kullandığı yeni aygıt, siber saldırı tekniklerini kullandıkları siber operasyonlardır (Roscini, 2014: 78-82).

Siber operasyonlar hem sahada hem de hedef devlette politik, ekonomik ve askeri etkiler yaratabilmektedir. Siber operasyonlar devletlerin elinin altında her an kullanabileceği bir uçak filosu, füze sistemi gibi vurucu bir güç olmuştur. ABD askeri siber operasyonlar konusunda uzun zamandır aktif bir konumda olup, Körfez, Kosova ve Libya Savaşları gibi birçok operasyonda siber saldırı unsurunu kullanmıştır. ABD aynı zamanda, istihbarat edinmek, veri toplamak, stratejik amaçlarını desteklemek ya da karşı devletin kritik altyapılarını ortadan kaldırmaya yönelik geçmişte siber operasyonlar gerçekleştirmiştir (Brown vd., 2016: 125-126, 132-133) .

2.1. Trans-Sibirya Boru Hattı Patlaması/Siber Saldırısı (1982)

Trans-Sibirya Boru Hattı patlaması, ABD Başkanı Ronald Reagan'ın 18 Temmuz 1982 tarihinde Sovyetler Birliği'nin petrol ve gaz üzerinden Avrupa'yı özellikle de Polonya'yı baskılamasını

engelleme ve Sovyetler Birliği'ne petrol ve gaz sektörü ile ilgili teknoloji transferini önlemeye yönelik açıklamalarda bulunduğu bir dönemde gerçekleşmiştir (Davis, 1990: 87).

Soğuk savaş döneminde ABD, Sovyetler Birliği'nin Urengoy bölgesindeki doğal gaz kaynaklarını altı ayrı doğal gaz boru hattı projesi ile Batı Avrupa'ya taşımasını ve bu sayede yüksek miktarda gelir elde edip ekonomik olarak ilerlemesini engellemeyi hedeflemiştir (Inboden, 2016: 169-170). Doğal gazın Avrupa'ya gelmesinin özellikle İngiltere ve Almanya tarafından politik ve ekonomik bir avantaj olarak görüldüğü bir süreçte, Moskova'nın Sibirya gazı ile Avrupa'yı politik baskı altına almasını engellemek amacıyla gerçekleştirilmiştir. Trans Sibirya Boru Hattı patlaması/siber saldırısı Soğuk Savaş'ta kritik altyapılara karşı yapılan ilk devlet destekli siber saldırıdır (Adams, 2015: 74).

2.2. I. Körfez Savaşı / Çöl Fırtınası Operasyonu - Irak (1991)

Irak'a karşı gerçekleştirilen Çöl Fırtınası Operasyonu, bilgi ve iletişim teknolojilerinin askeri maksatlı olarak geniş bir şekilde kullanıldığı bir savaş olmuştur (Bannelier-Christakis, 2015: 350). ABD ve 38 ülkeden oluşan Koalisyon Güçleri, I. Körfez Savaşı'nda Irak'a ait ağırlıklı Rusya ve Çin menşeli radar sistemlerine, hava savunma ve füze sistemlerine, iletişim ve kritik altyapılara yönelik siber saldırılar ile Irak Ordusu'nun komuta ve kontrol etkinliği ortadan kaldırılmış, Irak askerlerinin ve halkının savaşma iradesi kırılmıştır (Adams, 2015: 24-25).

Körfez Savaşı'nın Amerika lehine başarı ile sonuçlanmasında Irak'a ait radar, hava savunma ve füze sistemlerine karşı yürütülen siber saldırıların etkisi büyük olmuştur. ABD ordusu sahte veriler yükleyerek Irak hava savunma radar ve silah sistemlerini etkisiz hale getirmiştir (Vego, 2007: 51). National Security Agency (NSA) tarafından, Irak hava savunma sistemini kilitleyecek şekilde, kod adı "AF/91" ya da "April Fools 1991" olan bir virüs geliştirilmiştir. "AF/91" virüsü, Irak tarafından satın alınan, savaş öncesi Irak'a gönderilen ve Irak'taki hava savunma radar ve silah sistemlerinde de kullanıldığı tespit edilen yazıcılara yüklenerek sistemlerde bir arka kapı girişi oluşturulmuştur. Bu arka kapı sayesinde yazıcılar üzerinden savaş boyunca sahte veriler üretilerek hava savunma sistemi etkisiz hale getirilmiştir (Futter, 2018: 76).

Körfez Savaşı'nda devletlerarası bir kriz çözülemeyip, savaş ortamına taşınmıştır. Körfez Savaşı'nda Koalisyon Güçleri'nce dönemin en gelişmiş bilgi ve iletişim teknolojileri en üst seviyede, saha operasyonlarına katkı sağlayacak şekilde kullanılmıştır. Irak'ın elindeki en etkili savunma gücü olan füze, radar ve hava savunma silah sistemleri siber saldırılar ile kullanılamaz hale gelmiş, etkinliklerini kaybetmişlerdir. Körfez Savaşı, siber saldırıların savaş ortamını öncesinde nasıl şekillendirebileceğini, savaş başladıktan sonra da karşı tarafın etkinliğini ve savaşma kabiliyetini nasıl ortadan kaldırabileceğini gösteren ve devamının geleceğini de dünyaya duyuran ilk örneklerden birisi olarak tarihe geçmiştir.

2.3. Kosova Savaşı / Müttefik Güç Harekâtı – Kosova (1999)

NATO'nun Kosova'daki sivillere uygulanan baskı ve katliamlara son verilmesi amacıyla eski Yugoslavya'daki bazı hedeflere yönelik 24 Mart 1999 tarihinde başlattığı Müttefik Güç Harekatı'nda (Bhatia, 2003: 184) tıpkı 1995 yılındaki Bosna Savaşı'nda kullanıldığı gibi siber saldırılar gerçekleştirilmiştir. ABD, Yugoslavya hava savunma sistemlerini siber saldırılar ile karıştırmış ve etkisiz hale getirmiştir. ABD, Sırp hava savunma sistemlerine de karıştırıcı ve yanıltan mesajlar göndermiştir (Dinniss, 2012: 285).

Kosova Savaşı siber uzaydaki ilk savaş mücadelesidir. Denning'in tabiri ile "internetteki ilk savaş" tır. ABD hava kuvvetleri Sırbistan hava savunma sistemlerine birçok siber saldırı gerçekleştirmişlerdir. İletişim kesintilerinden, medya üzerinden propaganda faaliyetlerine kadar siber uzayın tüm nevileri, o günün teknolojisi ile kullanılmıştır (Cavelty, 2008: 73-78).

2.4. Kalıcı Özgürlük Operasyonu - Afganistan (2001) ve Irak'ın Özgürlüğü Operasyonu - Irak (2003)

ABD, hem 2001 yılında başlayan Afganistan Kalıcı Özgürlük Operasyonu hem de 2003 yılında başlayan Irak'ın Özgürlüğü Operasyonu harekâtlarında, siber kapasitesini göstermekte ve etkili bir şekilde kullanmaktadır (Roscini, 2014: 189). ABD, özellikle terör örgütlerinin içine sızan, komuta ve iletişim sistemlerini takip eden, istihbarat toplayan ve kendi askeri birliklerinin sahadaki etkinliğini artıran tüm siber operasyonlarını kamuoyuna duyurmadan devam ettirmektedir (Jun vd., 2015: 21-22).

Sadece silahların kullanıldığı bir savaş alanı değil aynı zamanda siber savaşın da gerçekleştiği Irak'ta Amerikan Ordusu'na ait Network Special Forces birimi Irak'taki internet ve bilgisayar sistemlerine savaş boyunca 2.000'den fazla bilgisayar virüsü göndermiştir (Xiang vd., 2019: 697-699). ABD ayrıca bu harekât sahalarında hem görsel hem de sosyal medya üzerinden siber saldırı maksatlı propaganda, kırma gibi unsurları da uygulamaya devam etmiştir (Roscini, 2017: 109).

2.5. Birleşik Koruyucu Operasyonu - Libya (2011)

Libya'daki kriz 15 Şubat 2011 tarihinde Bingazi'deki Sokak protestoları ile başlamış ve takip eden günlerde Libya'nın geneline yayılmıştır. Gelişen olaylar ve diplomatik süreç içerisinde BM Güvenlik Konseyi, 17 Mart 2011 tarihinde 1973 sayılı karar ile Libya'yı uçuşa yasak bölge ilan etmiştir. NATO, 31 Mart 2011 tarihinde koalisyon güçlerinin komutasını devralmıştır. Bu tarihten sonra harekât Birleşik Koruyucu Harekâtı (Operation Unified Protector - OUP) diye adlandırılmıştır. Operasyonlar sonucunda kriz başladıktan yaklaşık 9 ay sonra, 20 Ekim 2011 tarihinde Kaddafi ve oğlu Sirte'de ele geçirilmiş ve öldürülmüşlerdir. Kaddafi'nin öldürülmesinden sonra 31 Ekim 2011 tarihinde NATO tarafından yapılan açıklama ile OUP sonlandırılmıştır (Great Britain: Parliament: House of Commons: Defence Committee, 2012: 13-15).

Libya harekât sahasında, OUP kapsamında gerçekleştirilen siber saldırılar; "war promoter" diye adlandırılarak "savaşı organize eden unsur" olarak tanımlanmıştır. Operasyon başlamadan önce, göstericiler iletişim ortamı olarak interneti ve sosyal medyayı kullanarak "demokrasi için savaşalım" çağrısı yapmışlardır. Sosyal medya ile Kaddafi'nin insan hakları ihlallerine yönelik uygulamalarına tüm dünyanın dikkatini çekmeyi başarmışlardır. Kaddafi karşıtları ve anti-hükümet güçleri bir araya gelmiş, Twitter ve Facebook üzerinden organize olarak anti-hükümet yanlısı faaliyetlere başlamıştır. Ülkede çatışmalar başladıktan sonra Libya devleti interneti kapatmış, Anti-hükümet güçleri Rafaff'a ait hücresel kablosuz networkü gasp etmişler, sistemdeki telefon numaralarını elde etmişler ve "free Libya – özgür Libya" adıyla yeni bir iletişim sistemi kurmuşlardır. Bunlara ilave olarak, Kaddafi karşıtları-Anti-hükümet güçleri ve koalisyon güçleri EC-130, RC-135, EA-18G ve EP3 gibi birçok siber silah ve donanım ile Libya devletine ait Tripoli hükümeti sistemlerine kablosuz network üzerinden izinsiz giriş operasyonları gerçekleştirmişlerdir. Bu siber saldırılar sonucunda devlet kurumları, askeri birliklere ait bilgi sistemleri ve radarlar ele geçirilmiş ve elektronik olarak karıştırılmıştır. Özellikle Kaddafi'ye direkt bağlı 32. ve 9. özel tugayların bilgi ve iletişim sistemlerine sızılmış, alıcı antenlere sürekli veri serileri gönderilerek önemli istihbarat bilgileri çalınmış ve sistem yöneticisi yetkisi ile tüm networkün kontrolü ele geçirilmiştir (Xiang, 2019: 699).

ABD ve NATO'nun Kaddafi'ye karşı Libya'da başlattığı hava harekâtında, tıpkı 2003 yılında Irak'ta olduğu gibi (Lowenthal, 2017: 482) savaş boyunca Kosova ve Irak'taki benzerlikle Libya'nın tüm hava savunma sistemi siber saldırılar ile çökertilmiştir (Roscini, 2014: 234). Bu operasyon bir öncekilerle beraber değerlendirildiğinde gelinen noktada siber saldırıların stratejik bir silah olarak tanımlanmasını ve artan bir yoğunlukla da kullanılmaya devam edileceğini gösteren bir adım olarak görülebilir. Libya Savaşı, sokak protestolarının içeriğinin sorgulanması ya da sokak protestolarının başka devletlerce manipüle edilip siber katkı sağlanarak hükümet karşıtlarına destek verilmesi ve kullanılması açısından da kamu yönetimince dikkat edilmesi gereken bir operasyon olmuştur.

2.6. Stuxnet (2010)

Stuxnet, siber savaş döneminin, önceden belirlenen endüstriyel bir kritik altyapıya ve kesin bir hedefe yönelik gerçekleştirilen, kinetik bir silah kullanılmadan gerçek dünyada zarar veren en ünlü devlet destekli siber saldırı örneğidir (Mazanec, 2015: 20-21). Stuxnet, İran'ın Natanz bölgesindeki, çevresi 2.5 metre duvarla çevrili, yerin 8 metre altındaki nükleer silah yapımında kullanılan yıllık 500 kg'lık zenginleştirilmiş uranyum üretebilecek bir uranyum zenginleştirme nükleer tesisine sızmıştır (Shindler, 2014: 21). Stuxnet, 6.550 adet nükleer başlığa sahip Amerika'nın İran'ın nükleer programını durdurma hedefini gerçekleştiremese de uzun yıllar ertelediği, tarihin ilk siber füzesidir (Emery, 2012: 31-32). Stuxnet virüs programı Amerika'nın Olimpiyat Oyunları (Olympic Games) Operasyonu kod adı altında, İsrail ve Amerikalı istihbarat birimlerince geliştirilmiştir (Sanger, 2018: 7-8).

İlk kez bir Belarus bilgisayar güvenlik şirketi tarafından tespit edilen Stuxnet, Temmuz 2010 tarihinde dünya genelinde bir yıl içerisinde 100.000 bilgisayara, İran dışında 40.000 ayrı yerdeki bilgisayarlara bulaşmıştır. Saldırı, uzmanlara göre İran'ın nükleer programını en az 6-18 ay engellemiştir (Mazanec ve Thayer, 2015: 20-21). Kasım 2009 tarihinde, 8.700 civarında santrifüje sahip olduğu tahmin edilen (Zetter, 2014: 1) İran'ın nükleer programını kesin olarak durduramamakla beraber oldukça engellemiş ve yavaşlatmış olan Stuxnet (Lowenthal, 2017: 382), endüstriyel sistemler haricinde dünya çapında 10 milyon sivil makineyi de etkilemiştir (Rowe, 2017: 34). Stuxnet, füzelerin ateşlenmeyeceği, geleceğin savaşlarının bir odadaki masa üzerinden gerçekleşeceğinin öncüsüdür. Stuxnet ve benzeri virüsler devletler ve kamu yönetimi kurumları için gelecekte karşılaşmakta en çok korkulan virüslerin öncüsüdür.

2.7. Edward Snowden Sızıntısı ve PRISM Veri Toplama Programı (2013)

Edward Joseph Snowden, ABD hükümetine ait 1.7 milyon adet çok gizli belgeleri Hawaii'deki NSA merkezinden dışarı çıkarmıştır (Overbeck vd., 2016: 59-61). Snowden, sızdırdığı belgeleri ve bilgileri önceden gizli bir şekilde indirmiş (Gelles, 2016: 70), bir Universal Serial Bus (Evrensel Seri Veri Yolu – USB)'ye yüklemiş (Touhill ve Touhill, 2014: 175) ve USB belleği hep oynadığı 'Rubik-Küp'ün içerisine saklayarak NSA merkezinden dışarı çıkarmıştır (Holmes, 2017: 99).

Snowden'ın sızdırdığı belgeler 6 Haziran 2013 tarihinde the Guardian ve The Washington Post gazetelerinde yayınlanmış ve NSA'in PRISM adı verilen veri toplama programı ile dünya çapında gerçek zamanlı veri topladığı açığa çıkmıştır. Snowden'ın sızdırdığı belgelere göre NSA, sadece Şubat 2013 tarihinde küresel düzeyde 3 milyar farklı iletişim verisini toplamıştır. NSA, PRISM programı ile Google, Yahoo, Microsoft, Facebook, Youtube, Skype, AOL, Apple ve Paltalk gibi iletişim şirketlerine ait sitelerden, sosyal medya platformlarından ve her türlü iletişim cihazlarından veri toplamıştır. PRISM, sadece Big-Data denilen büyük veriyi değil, canlı görüşmeleri, dosya transferlerini, fotoğraf, video, geçmiş arama kayıtları, e-mail hesapları, sosyal medya hesapları ve detaylarına direkt erişim, dinleme, izleme ve kayıt altına alabilme imkânı sağlamıştır. NSA, telefon ve bilgisayar networklerindeki sınırsız seviyedeki bilgiyi toplamış ve takip etmiştir (Higgins, 2017: 46-47).

PRISM, NSA ajanlarına internet servis sağlayıcıları ve sosyal medya sitelerindeki istedikleri her türlü veriye direkt aracısız erişimlerini sağlayan bir programdır (Stacy, 2015: 190). Snowden belgelerine göre; PRISM, NSA tarafından 2007 yılından beri kullanılmaktadır (Hatashe, 2014: 8). Snowden belgelerine göre; NSA tarafından Amerika'da yapılan her telefon görüşmesinin sistematik olarak kayda alındığı (Cole, 2015: 129) milyarlarca e-mail, telefon mesajı, konuşma ve SMS'lerin her gün kaydedildiği açığa çıkmıştır. Ayrıca belgelere göre; Almanya Başbakanı Angela Merkel ve Brezilya Devlet Başkanı Dilma Rousseff'in telefonları dâhil birçok ülkede her ay yaklaşık 120 milyar telefon konuşmasının da kayda alındığı ortaya çıkmıştır.

NSA çok gizli bir program olan PRISM sayesinde hiçbir mahkeme kararı olmadan kişilerin her türlü e-posta, video, fotoğraf, saklı veriler, ses kayıtları, dosya transferleri, video konferans, yüklemeler, sitelere giriş bilgilerinin kayıtları ve sosyal medya detaylarına iletişim ve sosyal medya şirketleri ile işbirliği içerisinde bilgi alabilmiştir (Lee, 2015: 162).

ABD'nin siber saldırıları, politik, ekonomik, askeri baskı ve eylem unsuru olarak bir stratejik güce dönüştürdüğü gerçeği de bu veri sızıntısı ile gün ışığına çıkmıştır. Snowden veri sızıntısı ve PRISM, diğer devletler için siber tehdit değerlendirmesi ve siber güvenlik farkındalığı kapsamında algıyı değiştiren bir saldırıdır. ABD suçüstü bir şekilde yakalandığı bu siber saldırıyı yaparken, aynı zamanda kendisine tarihinin en büyük veri sızıntısı skandallarından birini yaşatacak şekilde, içerideki biri tarafından siber saldırıya uğramıştır.

3. ABD'NİN SİBER SALDIRI KAPASİTESİNİN DEĞERLENDİRİLMESİ

Devletler ellerindeki siber güç kapasitelerini duyurmak ve göstermek isterler. Devletler ve devlet destekli/ilişkili siber saldırılar, bir başka ülkeyi felce uğratacak, halkın o ülkedeki kamu kurumlarına ve yöneticilerine yönelik güvenini sarsacak siber saldırganlar ve tehditler arasına girmişlerdir. Siber saldırı gerçekleştiğinde, saldırının nereden geldiği ilk aşamada belirlenemediğinden, devletler karşılık vermede karmaşa yaşamaktadırlar. Bu da saldırıyı gerçekleştiren devlete, diğer manevraları için avantajlar kazandırmaktadır. Diğer silahlara göre siber silahlar geliştirmenin ucuzluğu ve kolaylığı, devletlerin bu güce sahip olmasını ve kullanmasını cazip kılmaktadır (Sanger, 2018: 31-32, viii, ix, xii).

ABD, gerçekleştirdiği siber saldırı ve operasyonlarla etkili bir siber güce sahip olduğunu ve istediğinde de bu gücünü en etkili bir şekilde kullanabileceğini tüm dünyaya duyurmuştur. ABD, son 40 yıl içerisindeki tüm okyanus ötesi askeri operasyonlarında siber kapasitesini hem saldırı hem de istihbarat kapsamında etkin bir şekilde kullanabildiğini, Türkiye'nin de politik ve askeri olarak müzahir olduğu tüm coğrafyalarda göstermiştir.

ABD, siber uzayı yaratan sibernetik bilimsel düşünce yaklaşımının geliştirildiği, internetin yaratıldığı, internetin fiziki altyapısı olan, fiber optik kabloların döşenmesini sağlayan en etkin devlettir. ABD, siber uzaya yönelik bilimin ve teknolojinin en çok üretildiği ülkedir. ABD, 1982 yılındaki Trans Sibirya saldırısı ile de ilk devlet destekli siber saldırı gerçekleştiren ülkedir. ABD, elindeki yazılım, donanım, nitelikli siber uzmanlar ve hacker ordusu ile dünyadaki en tehlikeli siber güçlerden birisidir. Gerçekleştirdiği virüs saldırılarından, veri sızıntısı saldırılarına kadar bir başka devletin kritik altyapılarına siber saldırı düzenleyebilen ABD, siber güç kapasitesini yeri ve zamanı geldiğinde kullanabilecek bir yeteneğe sahiptir. ABD siber gücünü, geçmişte gerçekleştirdiği siber saldırıların etkisi sayesinde, diğer devletlere karşı diplomaside kullandığı bir tehdit ve baskı aracına

dönüştürmüştür. ABD siber güç kapasitesini ve siber silahlarını, diplomasiyi baştan başlatmak, bir ülkeyi diplomasi masasına yeniden oturtmak ve kendi çıkarları doğrultusunda hareket etmesinden başka bir şansının olmadığını hatırlatmak için kullanmaktadır (Sanger, 2018: 17-18).

Türkiye, hem NATO üyesi olarak, hem de stratejik bir ortak olarak ABD ile uzun yıllardır siyasi, askeri ve ekonomik ilişkiler içerisindedir. Türkiye, aynı zamanda ABD çıkarları ile zaman zaman çatıştığı bir coğrafyada bulunmaktadır. Bu kapsamda Akdeniz, Ege, Suriye, Irak, Kıbrıs gibi harekât sahalarında ve terörizmle mücadele operasyonlarında ABD politikaları ile bazı anlaşmazlıklar yaşayan Türkiye, hem bir siber güç ortağı hem de bir siber tehdit olarak ABD'nin siber saldırı gücünü çok iyi analiz etmelidir. Ayrıca Türk kamu idaresi kendi siber güvenliğini kurgularken ve bu gücün siber güvenlik ürünlerini kullanırken ABD'nin siber güç etki ve tehdit kapasitesini dikkate almalıdır.

4. RUSYA FEDERASYONU İLE İLİŞKİLENDİRİLEN SİBER SALDIRILAR

Rusya da tıpkı ABD gibi siber saldırı kapasitesini stratejik ve askeri çıkarları doğrultusunda kullanabilecek seviyeye çıkarmıştır. Rusya, Çeçenistan, Kırgızistan, Estonya, Litvanya, Gürcistan ve Ukrayna gibi ülkelerdeki Rusya karşıtı politikalara yönelik siber saldırılarda bulunmuştur. Siber saldırılar, Rusya'nın dış politikasının ve askeri operasyonlarının bir parçası olmuştur.

Büyük güçler için stratejik hedeflere ulaşmalarında en az risk içeren siber saldırı kullanımı, Rusya'nın da uyguladığı bir taktik olmuştur. Rusya, siber operasyonlar ile yeni modern askeri teknolojileri birleştirerek daha az maliyetli ve sonuç alabilen büyük güçlerden birisi olmuştur (Lewis, 2017: 64-65). Siber saldırılar, Rusya'nın Ukrayna ve Kırım krizinde de görüleceği gibi hibrit savaş konseptinin tamamlayıcı bir parçası olmuştur (Hopia, 2015: 34-35).

Rus hibrit savaş konsepti, siber saldırı teknikleri ve en az seviyede askeri birlikleri, sahadaki müzahir grupları, devlet dışı aktörleri ve sivil halkı da kullanarak özel operasyonlarla stratejik hedeflere ulaşılması olarak belirlenmiştir. En az kayıp ve maliyet hedeflendiğinden, krizi gerektiğinde yaratmak ve devam ettirmekte hibrit savaşın gereklerinden biri olabilmektedir (Medvedev, 2015: 19).

Rusya, siber saldırı yetenekleri ile artırdığı gücünü, eskiden yönetimindeki şimdilerde ise etki sahasındaki Çeçenistan, Kırgızistan, Estonya, Gürcistan, Tataristan ve Ukrayna'ya yönelik siber saldırılarla denemiş ve stratejik kazanımlar elde etmiştir. Rusya bu ülkeleri kendi siber kapasitesini diğer siber güçlere göstermek ve kanıtlamak için birer oyun sahası gibi kullanmıştır. Elde ettiği politik ve stratejik kazanımlar ile de siber saldırı yeteneğinin kendisine neler kazandırabileceğini görmüştür.

4.1. Çeçenistan'a Yönelik Siber Saldırılar (1997-2001)

Rusya ile Çeçenistan arasındaki ikinci savaş dönemi olan 1997-2001 yılları arasında Rus Ordusu yeniden Çeçenistan'a yönelik işgal girişiminde bulunmuştur. Kriz süresince Rus ve Çeçenler birbirlerine karşı siber saldırılarda bulunmuşlardır. Siber saldırılar ilk başlarda siber uzayda karşılıklı propaganda

savaşı şeklinde gerçekleşmiş, sonrasında ise Rusya'nın Çeçen web sitelerini kapatmasına kadar gitmiştir (McNabb, 2016: 109).

Sahada silahlı bir savaş sürerken, göreceli olarak hafif dereceli siber saldırılarla Çeçenler, hem içerde hem de dış dünyaya Çeçenistan krizine yönelik genel algıyı şekillendirmeye ve bu algının kontrolünü sağlamaya yönelik propaganda yapmışlardır. Bununla birlikte Rus gizli servisi Federal Security Service (FSB) hackerları ise Çeçen hackerları değişik taktiklerle saf dışı bırakmış ve birçok stratejik Çeçen web sitesini çökertmiştir (Rhodes, 2011: 33).

4.2. Estonya'ya Yönelik Siber Saldırılar (2007)

Rusya'dan ilk bağımsızlığını 1918 yılında kazanan Estonya, 1945 yılında yeniden Sovyetler Birliği'ne katılmıştır. 1991 yılında ise yeniden Rusya'dan ayrılarak bağımsızlığını kazanmıştır (Vesilind, 2008: 15, 78, 172). Estonya'ya yönelik 2007 yılında gerçekleştirilen siber saldırılar, bir ülkenin tamamının hedef alındığı ilk devlet destekli siber saldırılardır. Estonya devletinin tüm kamu kurumları, parlamentosu, bakanlıkları, kritik altyapıları, endüstri merkezleri ile eğitim, sağlık, bankacılık gibi tüm sistemlerine yönelik siber saldırılar gerçekleştirilmiştir.

Estonya Siber Acil Müdahale Ekibi 'ne göre, ilk saldırı dalgasında devletin tüm sistemleri saniyede 4 milyon veri paketi şeklinde 24 saat bombardımana uğramıştır. Saldırı ile sistemlere normal zamana göre 1.000 kat daha hızlı bir veri akışı olmuştur. İkinci dalgada, bir günde 55 ayrı farklı BotNet saldırısı ile Estonya'ya saldırılmıştır. Estonya'daki internet sunucularına bir günde her biri en az 10 saat süren saniyede 95 megabits veri yükü ile 10 büyük saldırı gerçekleştirilmiştir. Saldırılarda üçüncü dalga ise 18 Mayıs 2007 tarihinde başlamıştır. Dünya genelindeki bir milyon zombi (köle) bilgisayarlarla koordineli bir şekilde Estonya web siteleri çökertilmiş ve kapatılmıştır. Ülkenin en büyük bankası olan Hansabank kapanmıştır. Saldırılarda Peru, Vietnam, Amerika, Brezilya ve Kanada'dan köle bilgisayarlar kullanılmıştır. Estonya Dışişleri Bakanı saldırıyı "AB saldırı altında ve Rusya Estonya'ya saldırıyor" diye duyurmuştur. Estonya'da devlet durmuş, ülkede benzin istasyonları, marketler bile çalışmamıştır. Bankacılık sektörü bir günde bir milyon dolar kaybetmiştir. Devlet küresel dünyadan destek ve yardım talep etmiştir. Her şeyden öte Rusya, bu siber saldırılar ile Estonya halkına, "acaba devamında bir Rus işgali olur mu" korkusu ve paniği yaşatmıştır (Russell, 2014: 75-82). Halkın devlete olan güveni sarsılmış, aynı zamanda maddi kayıp ve can güvenliğine yönelik endişesi de artmıştır.

Rusya'nın Estonya siber saldırısı tam 3 hafta sürmüştür. Hackerlar tarafından 75 ayrı ülkede, bir milyon bilgisayarla yaratılan BotNet ağı üzerinden koordineli bir şekilde Estonya siber ağlarına saldırılmıştır. Rusya, Estonya'daki tüm ana sistem bilgisayarlarını çökertmiştir. Estonya devlet başkanlığı, parlamentosu, devlet bakanlıkları, politik partiler, Estonya'nın 6 büyük basın yayın kuruluşundan üçü, 2 büyük banka ve birçok iletişim şirketi hedef alınmıştır. DDoS saldırılarla internet trafiği akımı oluşturulmuş ve çok geniş bir coğrafyada internete bağlı web siteleri, bilgisayar ve iletişim

ağları kapatılmıştır. Siber saldırı sonrasında ise tahmin edildiği gibi Rusya saldırıyı inkâr etmiştir (Rhodes, 2011: 33, 35).

Estonya siber saldırısı değerlendirildiğinde; bir ülkenin tüm kamu yönetimi hizmetlerini internet üzerinden gerçekleştirmesi ancak bu hizmetlerin siber güvenliğinin yeterli seviyede alınmaması açısından bir zafiyet yaratmış ve saldırı sonrasında devlet çökmüştür. Rusya siber saldırı ile bir devleti dizlerinin üzerine çökertebildiğini ve bunu bir tek mermi atmadan, bir tek füze ateşlemeden, bir tek uçak bile uçurmadan gerçekleştirebildiğini tüm dünyaya göstermiştir.

Estonya saldırısı ile Rusya'nın, Türkiye'nin de içerisinde bulunduğu yakın coğrafyasında etkin ve aktif bir siber güç olduğu ve tehdit haline dönüştüğü görülmüştür. Siber saldırıların, Rusya'nın diplomatik krizlerde kullanabileceği en etkin gelişen ve geliştirmeye devam ettiği silahlarından biri olduğu ve siber saldırıları başka devletleri etkileme, ikna ve cezalandırma aracı olarak da kullanabileceği görülmüştür. Rusya'nın Estonya siber saldırısı, Türkiye gibi devletlerin siber güvenlik stratejileri ve politikaları, siber güvenlik kapsamındaki uluslararası işbirliği, e-devlet uygulamaları ve kritik altyapı kurgulamalarında kendilerini çok sorgulayacakları ve dersler çıkarmaları gereken bir siber saldırı olmuştur.

4.3. Litvanya'ya Yönelik Siber Saldırılar (Haziran 2008)

Litvanya, 2004 yılında NATO ve AB üyesi olmuştur. Litvanya'nın nüfusunun %6'sı Rus kökenlidir. Rusya karşıtı politikalar yürüten Litvanya'ya Haziran 2008 tarihinde, üç gün boyunca süren Rusya destekli siber saldırılarda IP aldatması ile 300'den fazla Litvanya resmi web siteleri kırılarak, sayfalarına Rus Bayrağı yerleştirilmiş ve sitelerde anti-Litvanya şarkıları çalınmıştır (McNabb, 2016: 111).

Sonraki zamanlarda da Rusya, siber saldırılarla Litvanya'nın enerji ve elektrik altyapısını hedef almış ancak Litvanya'nın elektrik sistemi dağıtım ve kontrolü internete bağlı olmadığı için zarar verememiştir (Butrimas, 2016: 94). NATO'nun 2013 yılı içerisinde Litvanya'da gerçekleştirdiği "Steadfast Jazz" tatbikatı aşamasında da ülke siber saldırıya uğramıştır. Litvanya'da Nisan 2016 tarihinde düzenlenen Rusya'nın Kırım'ı ilhakı ve işgaline yönelik uluslararası toplantılarda, Kırım Tatarları Dünya Kongresi ve Kırım İşgalinde Yaşanan İnsan Hakları İhlalleri Kongre'lerinde de Litvanya Parlamentosu siber saldırılara uğramıştır (Brişingaite vd., 2017: 73).

4.4. Gürcistan'a Yönelik Siber Saldırılar (Ağustos 2008)

Rusya tarafından başlatılan askeri harekâttan önce siber saldırılardaki ilk dalgada, önce Gürcistan Devlet Başkanı'nın web sitesindeki resmi, Adolf Hitler'in resmi ile yer değiştirilmiştir. Tüm internet trafiğinin içerideki ve dış dünya ile bağlantısı engellenmiştir. E-mail alma ve gönderme sistemi kullanılamamış, ülke dış basın yayın ve haber kaynaklarından yoksun bırakılmıştır. Bankacılık, kredi

kartı sistemleri ve mobil iletişim aksatılmış ve felce uğratılmıştır. Rusya, saldırıların sorumluluğunu almamış, hacktivist gruplara topu atmıştır (Caldwell vd., 2016: 153).

Siber saldırının stratejik kullanımına uygun olarak, ülkenin çoğunluğunun içerisi ve dışarıyla olan iletişimi kesilmiştir (Mowbray, 2014: 278). Siber saldırılar ile Gürcistan devletinin kamu hizmetlerinde internet üzerinden sağladığı kontrol Rusya'nın eline geçmiştir. Siber saldırılarla iletişim, finans ve kamu kurumlarına ait 54 web sitesi tamamen kapatılmış ve çökertilmiştir.

Gürcistan bankaları savaş boyunca hizmet verememiştir. Siber saldırılar sonucunda bankalarda oluşan zarar sadece işlem yapılamaması değil, bankaların verileri ve siber altyapısı yok edilmiştir. Rus hackerlar, yarattıkları BotNet ile Gürcistan bankaları gibi davranıp yabancı bankalarla bağlantıya geçmişler, yabancı bankalar dalgalı siber trafikten dolayı bağlantıyı Gürcistan kaynaklı bir siber saldırı zannetmişlerdir. Dolayısıyla yabancı bankalar zarar görmeyelim diye Gürcistan bankaları ile bağlantıyı kesmişlerdir (Rhodes, 2011: 35, 36).

Rusya'nın Gürcistan'a yönelik siber saldırıları askeri harekâtın başlama tarihi olan 08.08.2008 tarihinden çok önce 19 Temmuz'u 20 Temmuz'a bağlayan gece başlamıştır. Rus askeri birlikleri ülkeye girmeden önce Gürcistan'ın siber altyapısı ve internet bağlantılı tüm kamu sistemleri çökertilmiş ve dış dünya ile bağlantıları kesilmiştir. Rusya Gürcistan Savaşı, devletlerarasındaki bir cephe savaşında siber saldırıların ilk kez kullanılması açısından tarihteki yerini almıştır (Mazanec ve Thayer, 2015: 20).

Gürcistan saldırısı, klasik savaş öncesi kullanılan ilk siber saldırı olarak tarihe geçmiştir. Savaş kazanmak isteyen devletlerin siber yeteneklerini ön hatlara sürmesinin savaşı kazanmadaki önemini göstermiştir. Devletlerin askeri yeteneklerini siber saldırı kapasiteleri ile birleştirmesi ve muharebe sahasında uygulaması gerekliliği ortaya çıkmıştır. Ayrıca geleceğin savaşlarının komutasında siber operasyonların da diğer muharebe unsurları ile beraber planlanması ve koordine edilmesinin harekâtın başarısına yüksek derecede olumlu etki edeceği görülmüştür. (Rios, 2009: 153-154).

4.5. Ukrayna'ya Yönelik Siber Saldırılar (2014-2016)

Ukrayna'da kriz Kasım 2013 tarihinde başlamıştır. Rusya yanlısı Ukrayna Devlet Başkanı Viktor Yanukovich'in AB ile ticaret anlaşmasını geri çevirmesi ve Rusya ile 15 milyar dolarlık kredi anlaşması yapması üzerine, halkın %87'sinin ülkenin ekonomik durumundan, %79'unun da hükümet politikalarından memnun olmadığı bir kriz ortamında protestolar başlamıştır (Reisinger, 2014: 1-12; Dyczok, 2015: 91).

Protestocular kendilerini "Euromaidan" diye adlandırmışlardır. Sosyal medya üzerinden organize olan ve toplanan protestocular (Simons, 2016: 288), yine sosyal medya üzerinden uluslararası toplumun dikkatini çekmişler, dış ülkelerdeki politikacılarla ve uluslararası basınla bilgi paylaşmışlardır (Krasynska, 2015: 177-179). Sosyal medya üzerinden #Euromaidan ve #DigitalMaidan gibi twitter hesapları ve facebook hesapları ile sayıları 300 binleri bulan protestocuları meydana toplamışlardır.

Protestocular, sosyal medyada 9 ayrı dilde yayın yaparak seslerini dünyaya duyurmuşlardır (Ronzhyn, 2014: 242-244).

Rusya bu krizi beklediğini gösterircesine, Ukrayna sınırına askeri birliklerini yığmış, Kırım içlerine de özel kuvvetlerini sızdırmıştır. 26 Şubat'ta Rusya, 150 bin asker ile dört gün süreli kara, hava ve deniz kuvvetlerinin katılımı ile Ukrayna sınırında ve Kırım açıklarında savaş gemileri ile tatbikat başlatmıştır. 27 Şubat'ta Ukrayna özel polis gücü tarafından ağır silahlarla ve zırhlı ekiplerce, Kırım ve Ukrayna arasındaki kilit noktalar Rusya lehine ele geçirilmiştir. Aynı tarihlerde üzerinde işaretleri olmayan maskeli üniformalı silahlı ekipler (Bunların sayıları önce 2.000 sonrasında 6.000 olduğu ifade edilen Rus Özel Kuvvetleri Spetsnaz Taburları olduğu anlaşılmıştır), Kırım'ın başkenti Simferopol (Akmescit)'deki parlamento binası ve başkanlık konseyi binasını ele geçirmişler ve Ukrayna Bayrağını indirip Rus Bayrağını çekmişlerdir. Sergey Aksyonov'u da Kırım başbakanı olarak atamışlardır. Rusya Parlamentosu'nun da onaylaması ile Rus askeri birlikleri Kırım'a hareket etmişlerdir. 28 Şubat'ta da Belbek hava üssüne Rus savaş helikopterleri ve uçakları inmiştir. Rusya böylece Nisan 2014 tarihine kadar 40.000 kişilik askeri birliklerini Ukrayna içine ve sınırına konuşlandırmıştır (Kofman, 2017: 1-3, 7-10).

Rusya, Ukrayna'daki Turuncu Devrim esnasında da özellikle seçimlerde veri sızıntısı gerçekleştirmiş ve seçim sonuçlarını etkilemeye çalışmıştır (Koval, 2019: 83). Snake, 2008 yılındaki Rusların Agent.btz kötücül yazılımının ilk versiyonlarından birisidir. Snake, Ukrayna'ya ilk saldırısını 2010 yılında gerçekleştirdikten sonra, 2011 yılında 3 kez, 2012 yılında 6 kez, 2013 yılında 8 kez, 2014 yılında ise tam 14 kez Ukrayna sistemlerine siber casusluk maksadıyla saldırmıştır (Daly, 2019: 73-76). Protestocuların meydanı terk etmeme kararı almalarından sonra 2 Aralık 2013 tarihinden itibaren başlayan siber saldırılarda ayrıca MiniDuke, NetTraveler ve RedOctober gibi kötücül yazılımlar Ukrayna sistemlerine enjekte edilmiştir. Ayrıca Ukrayna içinde yaşayan Rusya yanlısı içeridekiler 'den de siber saldırılar gerçekleştirilmiştir (Valeriano, vd, 2018: 137).

Saldırıdan çıkarılan dersler kapsamında Rusya, Ukrayna üzerinde, sistematik bir strateji izleyerek uzun zamana yaydığı bir siber saldırı gerginliği ve gerilimi yaratmış, Ukrayna kamu yönetimi ve toplumu üzerinde bir siber saldırı baskısı ve stresi oluşturmuştur. Bu baskı, halkı bıkma noktasına getirmiş ve kamu hizmetlerinin güvenliği konusunda devlete olan güven olumsuz yönde etkilenmiştir. Rusya bir devletin içine yıllar öncesinden yerleştirdiği kötücül yazılımlarla casusluk yaparak, karşı devletteki istediği bilgileri sistematik bir şekilde ele geçirmiştir.

5. RUSYA DEVLETİ İLE İLİŞKİLİ SİBER SALDIRILARIN DEĞERLENDİRİLMESİ

Rusya, eskiden sözünden çıkmayan ancak 1990'lardan sonra "rengârenk devrimlerle" elin altından kaybolan çevre ülkelerine karşı siyasi baskı, politik etki ya da ceza maksadıyla siber saldırılar

düzenlemiştir. Rusya, özellikle Estonya, Gürcistan ve Ukrayna'ya yönelik siber saldırıları ile bir bakıma kendisinden kopan, Batı ile bütünleşen, NATO'ya ve AB'ye üye olan, stratejik konumlarını ve ittifak seçimlerini değiştiren bu ülkeleri cezalandırmıştır. Rusya, bu saldırılar ile siber kapasitesini sahada denemiş, siber saldırıları askeri harekâtlarda kullanarak savaşın kazanılmasına katkı sağlayan siber yeteneklerini etkin kullanabildiğini tüm dünyaya göstermiştir (Daly, 2019: 71-73)

Rusya, Soğuk Savaş sonrasında Estonya ve Gürcistan krizleri ile siber uzayda da savaş kapasitesini sergileyerek artık yeniden ABD ile karşı karşıya gelebileceğini göstermek istemiştir (Trenin, 2010: 195). Rusya önümüzdeki dönemde de stratejik hedeflerine uygun olarak dış politika ve propaganda aracı olarak, aynı zamanda da askeri harekâtlarında savaş kazandıran bir unsur olarak siber saldırıları kullanmaya devam edecektir (Rugge, 2018: 16).

Rusya siber saldırı kapasitesini artırırken kendisine yönelik bir siber saldırıya karşı da hazırlık yapmaktadır. İnternetin fiziki altyapısı olan fiber optik deniz altı kablolarında bir kopma olması, bu hatlardan üzerinden veya wi-fi sistemler üzerinden küresel seviyede bir siber saldırı olması durumunda yaşanabilecek internet kesintisine karşı kendi ulusal internet sistemini kurmuş ve 23 Aralık 2019 tarihinde ülke çapında küresel interneti kesip, Russian Network (RuNet)'i devreye almıştır (Wakefield, 2019).

Rusya Devleti, RuNet ile internetin kesintiye uğratıldığında kritik altyapıların zarar görmesini engellemek veya güçlü siber saldırılarla karşılaşıldığında hazırlıklı olmak ve ülkeyi korumak istese de bir taraftan da internet üzerinden Amerikan kültürünün ve Batı ideolojisinin kendi halkına erişmesinin de önüne geçmek istemektedir (Nikkarila ve Ristolainen, 2017: 28-29).

Rus siber saldırı kapasitesi Türkiye için önemlidir. Rusya destekli bu siber saldırılar, siyasi, ekonomik krizler ve terörizmle kavrulan bir coğrafyada, Türkiye'nin de içinde bulunduğu bir bölgede gerçekleşmiştir. Bu bağlamda; Rus siber kapasitesi Türk kamu yönetimince çok iyi irdelenmeli ve Rusya'nın kurguladığı politikalarda siber saldırıları oyun değiştirici bir güç olarak kullanabileceği unutulmamalıdır.

6. DEVLET DESTEKLİ SİBER SALDIRILARA KARŞI TÜRK KAMU YÖNETİMİNCE ALINMASI GEREKEN ÖNLEMLER

Kamu yönetiminin bürokratik organizasyon süreci ve altyapısı siber uzayın sunduğu hizmetlerle değişim ve dönüşüm içerisine girmiştir. Siber uzayın militarize edilmesinin artık bir risk olmaktan öte zaten bir gerçek olduğu ve birçok devletin siber savunma gücü adı altında teknolojiler, doktrinler ve stratejiler geliştirdiği, hatta siber operasyonlar düzenlediği bir dünyada, devletler hem hedef hem de şüpheli bir hale gelmiştir (Roscini, 2014: 280). Siber saldırıların trafikten bankacılığa, barajlardan eğitime, kişilerden kamu yönetimine kadar her seviyede o kadar çok etki alanı var ki, siber uzayda gerçekleşen bir saldırı gerçek fiziki uzayı etkileyebilecek konumdadır. Bu durum devletleri siber uzayla

ilişkili tehditlere karşı güvenlik önlemlerine ve siber saldırılara karşı çözüm üretmeye itmektedir (Loukas, 2015: 3-4).

İnternet, ülkeler arasındaki sınırları önemsizleştiren, etkisizleştiren bir konuma gelmiştir. Ulus devletler, uluslararası ortamda siber saldırı karmaşasının içerisindedir. Bu karmaşada kamunun siber güvenliği, devletin kendisi tarafından sağlanmalıdır (Sienkiewicz, 2017: 7-8, 20). Üretilen her yeni ürün ile internete daha da fazla bağımlı hale gelen uluslararası toplum ile birlikte siber kaynakları, politikaları ve işlemsel süreçleri genişleyen devletler, bu sistemlerini savunmak durumundadırlar (Arashi, 2017: 1-24).

Kamu yönetimi siber saldırılara karşı politikalar, uygulamalar, yönetmelikler, usuller, düzenlemeler, yasalar ve kurallar ortaya koyarak, siber saldırılara karşı mücadelede üzerine düşeni yapmalıdır (Solomon, 2014: 4). Siber saldırılara karşı uluslararası işbirliğinin yanında devletin yapması gereken üç temel prensip ise koruma, tespit ve tepkidir. Siber saldırılardan toplumu ve devleti korumak, siber saldırı kaynaklarını, siber tehditleri ve devlete ait sistemlerdeki zayıflıkları/açıklıkları tespit etmek, son olarak da zayıflıklara/açıklıklara ve siber saldırılara uygun çözümlerle tepki vermek devletin en temel görevleri arasındadır.

Kamu yönetimince siber güvenliğe yönelik yapılması gerekenler; öncelikle ulusal siber güvenlik stratejisi belirlenmeli, bu stratejiye uygun kurum kuruluşlar oluşturulmalı, yasal düzenlemeler ve bütçe belirlenmeli, özel ve sivil otoritelerle işbirliği sağlanmalı, siber güvenliği oluşturacak ve yönetecek nitelikli insan yetiştirilmeli, kamuoyunda farkındalık eğitimi ile teknolojik araştırma ve geliştirme faaliyetleri süreklilik arz edecek şekilde yapılmalıdır (Theohary ve Rollins, 2009: 6).

Devletler, kritik altyapılara yönelik siber riskleri belirlemeli, kritik altyapıların siber güvenliğine yönelik bir siber savunma yapısı kurmalıdır. Kritik altyapıların siber kontrol altyapısı yedekli olmalı ve kritik altyapıların siber altyapıdan bağımsız fiziksel işletim altyapısı da olmalıdır (Andress ve Winterfeld, 2014: 36-37, 74). Kamu yönetimi kritik altyapıların bir parçası olan kendi kişisel ve kurumsal sistem ve bilgisayarlarını kullanan personelini de siber saldırılara karşı eğitmelidir (Amoroso, 2013: 56-57).

Kamu yönetimi, "sokaktaki adama" hackerler ve siber saldırılar konusunda farkındalık kazandırmalıdır (Lehtinen ve Russell, 2006: 3). Devlet, siber güvenliğe yönelik temel anlamda yasal ve kurumsal altyapıyı kurgulamalı, ulusal seviyede kurumsal risk analizi yapmalı, kurumlar arası iletişimde güvenli bir fiziksel siber altyapı tesis etmeli, tüm sistemlerin işletim güvenliği, fiziksel koruması, erişim güvenliği ve devamlılığı olmalı, kamu personelinin siber güvenlik farkındalığı olmalıdır. Bunun yanında siber saldırılara ve tehditlere yönelik araştırma geliştirme, saldırıyı fark etme, tespit, saldırıya cevap ve oluşan zararı belirleme, onarma, yenileme ve iyileştirme konuları kapsamında kararlar almalı, parasal kaynak aktarmalı ve kurumsal yapılar oluşturmalıdır (Johnson, 2015: 62-63).

BM tarafından 2011'den itibaren gündeme alınan ve 27 Haziran 2016 tarihinde BM İnsan Hakları Komisyonu Raporu ile açıklandığı şekilde internet erişimi, temel insan hakları kapsamına alınmıştır (Report of the Human Rights Council, 2017: 34). Devletler, internet üzerinde en yetkili ve etkili role sahip bir pozisyondadır. Devletler bireye, topluma temel bir hak olarak sunduğu internet hizmetinin altyapısını ucuz, sağlam, etkili, kesintisiz ve güvenli erişimi sağlayacak bir konuma getirmelidir (Shackelford, 2014: 46, 56). Kamu yönetimi olarak bireysel siber güvenliği de kapsayacak şekilde eğitimsel, yasal, yönetim ve teknik olarak bir siber güvenlik yaklaşımı ve siber fiziki yapı kurulmalıdır. Kamu idaresi ülkede fiziksel siber altyapıyı kurmak için güvenli bir fiber optik kablo sistemi oluşturmalıdır (Ghernaouti-Helie, 2013: 18).

Kamu yönetimine bağlı siber güvenlik ile ilgili birimler, sistemi çok iyi bilmeli, siber saldırganlar sistem hakkında hiç bir şey bilmemeli, sisteme sızmamalı, sistem dışarıdan yetkisiz erişime kapalı olmalı, sistemin zayıflıkları olmamalı, her an kontrol edilmelidir. Açıklıklar ve zayıflıklar anında giderilmeli, sistemin zarar görme ihtimali sıfır olmalı, siber güvenlik birimleri sisteme sızmayı anında tespit etmeli ve cevap verip sistemi yeniden işletmeye almalıdır (Boyer ve McQueen, 2008: 248).

İnsan kaynakları yönetimi ve kamu yöneticileri açısından özellikle stratejik seviyedeki pozisyonlarda siber güvenlik eğitimi ve farkındalığı yüksek personel görevlendirilmelidir (Trim ve Lee, 2014: 221). İçerideki tehdidi de göz önünde bulundurarak kritik altyapılardaki siber riskleri azaltmak için ön araştırmadan geçmiş güvenli personel alınmalı, bu tür personeli eğitmek için de özel sektörle işbirliği ve bilgi alış verişi sağlanmalıdır. Kamu yönetiminin yetkili unsurları, üniversiteler ve endüstri şirketleri ile kamu personeline yönelik siber güvenlik eğitimi geliştirmelidir (Amoroso, 2013: 30-31). Diğer ülkelere yönelik gerçekleştirilen siber saldırılar araştırılmalı, alınan dersler ve ödevler çıkarılmalıdır. Bu saldırılardan elde edilen bilgiler, tecrübeler ve en iyi siber güvenlik uygulamaları ülkeye kazandırılmalıdır (Westby, 2004: 103).

Ancak en gelişmiş aygıtlar da kullanılsa, en üst seviye algoritmalarda kurgulansa, kamu yönetiminde ve toplumda siber saldırılara karşı yüzde yüz bir güvenlik zinciri oluşturulamayacağı, yapılan çalışmaların sürdürülebilir bir garantisinin de olamayacağı bilinmektedir (Mehan, 2008: 49). Bununla beraber tam olarak siber güvenliğin gerçekleşmesi imkânsız da olsa devletlerin yerine getirmesi gereken temel hususlar gerçekleştirilmelidir. Teknolojik gelişmelerinin yasal düzenlemelerden daha hızlı ilerlediği ve gerçekleştiği bir çağda, yönetimler teknolojik hıza ayak uydurmaya ve yasal düzenlemeleri hızlı bir şekilde gerçekleştirmeye çalışmalıdır (Marzilli, 2005: 10, 15).

Devletler, siber saldırılara karşı uluslararası antlaşmalardan, kamusal uygulamalardan, suça yönelik yasalardan, hukukun genel kaidelerinden ve prensiplerinden, yargı kararlarından faydalanarak, kamunun tamamını siber saldırılara karşı koruma anlayışı ile hareket ederek, siber saldırıları önlemek için çözümler üretmelidir. Devletler siber güvenliğe katkı sağlayacak gerekli bilimsel, teknolojik ve

kurumsal tedbirleri, siber saldırıların gelişen doğasına uygun olarak almaya devam etmelidir. En önemlisi, siber güvenliğin etkin unsuru olan nitelikli insan kaynağını yetiştirmelidir (Carr, 2011: 61-67).

Kamu yönetimi, sistem siber saldırıya uğrasa da en kısa sürede kamu hizmetlerinin devamlılığını sağlayacak şekilde yedek sistemleri devreye almalı, kamu hizmeti durdurulmamalıdır. Kamu hizmetleri siber sistemler ortadan kalkması durumuna göre de işletilmeye hazır olmalıdır. Devlet, siber saldırılara karşı uluslararası antlaşmalardan, kamusal uygulamalardan, suça yönelik yasalardan, hukukun genel kaidelerinden ve prensiplerinden, yargı kararlarından faydalanarak kamunun tamamını siber saldırılara karşı koruma anlayışı ile hareket ederek siber saldırıları önlemek için çözümler üretmelidir.

Türk kamu yönetimi uluslararası standartlarda geçerliliği olan bir siber güvenlik stratejisi ve uygulama politikası ile bakanlık seviyesinde bir sorumlu bir kurum koordinasyonunda ve ulusal siber güvenliğin sağlanmasına yönelik teknik eksikleri tespit edecek, altyapı çalışmalarını gerçekleştirecek, siber uzaya ait bilimin ve teknolojinin üretilmesine yönelik yatırımları gerçekleştirecek, yasal düzenlemeleri oluşturacak, uygulamalarını yapacak, takip edecek, denetleyecek, ülke çapında gayretleri birleştirecek, tek elden tüm kurumlar ve özel sektör ile işbirliğini organize edecek, uygun bütçeyi planlayacak, bilgi, tecrübe ve yetenekleri bir araya getirecek etkinlik seviyesi yüksek üst bir kamu kurumu oluşturulmalıdır.

Bu kamu kurumu, gelecekte internet teknolojisi ve siber uzaydaki gelişmelerle birlikte, akıllı şehirler, yapay zekâ, nesnelerin interneti ve her şeyin interneti uygulamaları ve ürünlerinin daha çok hayatımıza girmesi ile birlikte bunlara uygun olarak Türkiye'deki siber uzayı düzenleyecek ve işletecektir. Bu birim, ülkeyi siber saldırılardan koruyacak ve siber güvenlikten sorumlu olacak bir Siber (Uzay) Bakanlığı veya Siber Güvenlik Bakanlığı şeklinde kurgulanmalı ve altyapısı şimdiden düzenlenmelidir.

Kamu yönetimi kendisinin de içinde olduğu enerji, ulaşım, iletişim, sağlık, tarım, eğitim, güvenlik, ekonomi gibi kritik altyapıların siber güvenliğinden sorumludur. Türk kamu yönetiminde tüm kritik altyapılardaki siber altyapıyı kapsayan bir ulusal siber güvenlik anlayışı belirlenmeli ve siber güvenliğin sadece veri ve erişim güvenliği olmadığı kamu yöneticileri ve personelince anlaşılmalıdır.

Türkiye'deki kritik altyapıların fiziki güvenliğinin sağlanması ulusal siber güvenliği artıran bir unsur olduğu unutulmamalıdır. Türkiye'deki kritik altyapıların fiziksel siber altyapısı ve ağ sistemlerinin fiziksel saldırılara karşı da güvenliği sağlanmalıdır. Türkiye'deki kritik altyapılara yönelik siber risk analizi yapılıp tehditler belirlenmeli ve eksikler giderilmelidir. Siber tehdit analizi yapan resmi ve özel kuruluşlar kurulmalı, bu kuruluşların uluslararası düzeyde araştırma yapmaları ve çözümler üretmeleri için mali olarak teşvik edilmeleri gerekmektedir..

Kritik altyapılara yönelik siber saldırılarda çok önemli bir etken olan içerideki tehdit göz önüne alındığında ise bu kurumlara yönelik personel alımı ve insan kaynakları politikası çok iyi belirlenmelidir.

Türkiye'de kritik altyapılar gün geçtikçe siber altyapı üzerinden SCADA sistemleri ile yönetilmekte ve bu konuda yeni teknolojik projeler üretilmektedir. Ancak Türkiye'de bu çalışmada da belirtildiği gibi; enerji hatları, elektrik kesintileri, havaalanları, bankalar, üniversiteler, hastaneler, bakanlıklar gibi kritik altyapılara yönelik gerçekleştirilen geçmişteki siber saldırılarda bu sistemlerin siber güvenlik düzeyleri yetersiz kalmıştır. Kritik altyapıları işleten SCADA sistemlerindeki yabancı yazılım ve donanımdan oluşan cihazların siber güvenlik kontrolleri yapılmalı, bu konuda standartlar belirlenmeli ve bu teknolojinin yerli ve milli olması sağlanmalıdır.

Eğer siber uzayda var olmak istiyorsak, milli yazılım ve donanıma ihtiyacımız bulunmaktadır. Türkiye'de bireylerden kamu yönetimini oluşturan kurumlara kadar kullanılan siber güvenlik ürünlerinin %90-95'i yabancı firmaların ürünlerinden oluşmaktadır (Savunma Sanayi Dergilik, 2020). Dünyadaki yazılım sektörünün ve siber güvenlik ürünlerinin müşterisi olmaya devam etmemek için yerli ve milli siber güvenlik çözümleri ile milli yazılımlar geliştirilmelidir. Ayrıca siber uzay koşullarında hackerların, internetin bağışıklık sistemi olduklarını unutmadan kamu yararına çalışmaları sağlanmalıdır (Sanalp, 2016: 67) .

7. SONUÇ

Devletler ellerindeki siber güç kapasitelerini göstermek isterler. Devletler ve devlet destekli/ilişkili siber saldırılar, bir başka ülkeyi felce uğratacak, halkın o ülkedeki kamu kurumlarına ve yöneticilerine yönelik güvenini sarsacak siber saldırganlar ve tehditler arasına girmişlerdir. ABD, gerçekleştirdiği siber saldırı ve operasyonlarla etkili bir siber güce sahip olduğunu tüm askeri operasyonlarında siber kapasitesini hem saldırı hem de istihbarat kapsamında etkin bir şekilde kullanabildiğini, Türkiye'nin de politik ve askeri olarak etkili olduğu tüm coğrafyalarda göstermiştir.

ABD, elindeki yazılım, donanım, nitelikli siber uzmanlar ve hacker ordusu ile dünyadaki en tehlikeli siber güçlerden birisidir. Gerçekleştirdiği virüs saldırılarından, veri sızıntısı saldırılarına kadar bir başka devletin kritik altyapılarına siber saldırı düzenleyebilen ABD, siber güç kapasitesini yeri ve zamanı geldiğinde kullanabilecek bir yeteneğe sahiptir. ABD siber gücünü diğer devletlere karşı diplomatik tehdit ve baskı aracına dönüştürmüştür.

Türkiye, hem NATO üyesi olarak, hem de stratejik bir ortak olarak ABD ile uzun yıllardır siyasi, askeri ve ekonomik ilişkiler içerisindedir. Türkiye, aynı zamanda ABD çıkarları ile zaman zaman çatıştığı bir coğrafyada bulunmaktadır. Bu kapsamda Akdeniz, Ege, Suriye, Irak, Kıbrıs gibi harekât sahalarında ve terörizmle mücadele operasyonlarında ABD politikaları ile bazı anlaşmazlıklar yaşayan Türkiye, hem bir siber güç ortağı hem de bir siber tehdit olarak ABD'nin siber saldırı gücünü çok iyi

analiz etmelidir. Ayrıca Türk kamu idaresi kendi siber güvenliğini kurgularken ve bu gücün siber güvenlik ürünlerini kullanırken ABD'nin siber güç etki ve tehdit kapasitesini dikkate almalıdır.

Rusya bağlamında konuya yaklaşıldığında ise 1990'lardan sonra etki alanından çıkan çevre ülkelerine karşı siyasi baskı, politik etki ya da cezalandırma amacıyla siber saldırılar düzenlemiştir. Rusya, özellikle Estonya, Gürcistan ve Ukrayna'ya yönelik siber saldırıları ile bu ülkeleri cezalandırmıştır. Rusya, bu saldırılar ile siber kapasite ve yeteneğini sahada göstermiştir. Rusya, bu siber saldırılarla yeniden ABD ile karşı karşıya gelebileceğini göstermiştir. Rusya önümüzdeki dönemde de stratejik hedeflerine uygun olarak siber saldırıları kullanmaya devam edecektir. ABD ve Rus siber saldırı kapasitesi Türkiye için önemlidir. Bu ülkelerin siber saldırı kapasiteleri Türk kamu yönetimince çok iyi değerlendirilmeli ve gerekli önlemler alınmalıdır.

Siber kapasitesi yüksek olan bu devletler örnekleri çalışmada sunulduğu gibi diğer devletlerin verilerine erişmekte, verilerini değiştirmekte, siber casusluk yapmakta, kamu sistemlerini durdurabilmekte ve bozabilmektedir. Bu çeşit siber yöntemlerle istedikleri an kritik altyapıları işlemez hale getirebilecek siber saldırılar düzenleyebilmektedirler. Devletlerle ilişkili veya devlet destekli siber saldırılar ile kamu yönetiminin tüm unsurları, hizmetleri ve yöneticileri hedef alınabilmektedir. Bu tarz siber saldırılar yüzünden, siber uzaya taşınan kamu hizmetlerindeki aksamalar toplumun kamu yöneticilerine ve kurumlarına olan güveninin zedelenmesine, zaman, üretim ve mali kayıplara neden olabilmektedir. Türkiye, ABD, Rusya, İsrail, İran, Suriye, Kuzey Kore ve Çin gibi siber saldırıları stratejik, politik ve askeri taktik bir silah olarak kullanabilen ülkelerin mücadele coğrafyasında bulunmaktadır. Dolayısıyla bu ülkelerden gelebilecek bu çeşit siber saldırılara karşı yurt dışı firmalardan alınan ürünleri çok iyi testlerden geçirilmeli ve sık sık bu tarz gömülü siber saldırı programlarına karşı sistemler kontrol edilmelidir. Diğer devletlerin siber saldırı kapasiteleri ile tehdit dereceleri çok iyi takip edilmeli ve bu konuda uluslararası işbirliği devam ettirilmelidir.

Siber saldırılara karşı kamu yönetiminin kriz anlarında da farkındalığı yüksek olmalıdır. Ayrıca bu gibi krizler, küresel internetin fiziki altyapısında bir kopma olduğunda ya da ülkenin tamamını etkileyecek bir siber saldırı ile küresel internete erişilememesi durumuna göre Türkiye içinde, dışa kapalı bir ulusal internet ağı tesis edilmeli, sosyal medya, e-posta, web, arama motoru gibi uygulamalar geliştirilmeli ve e-devlet hizmetleri bu ağ üzerinden kurgulanmalıdır. Türkiye bu kendi iç ulusal interneti ile küresel internet ağı kesintiye uğradığında ya da tüm ülkeyi etkileyecek bir siber saldırı olduğunda bu ağı devreye alarak topluma sunduğu kamu hizmetlerini kesintisiz devam ettirebilmelidir.

Türkiye de herhangi bir siber saldırıda, kamu yönetiminin kurumsal işleyişini aksatmamak ve kritik altyapıların zarar görmeden çalışmasını sağlamak için ülke genelinde işleteceği ve istediğinde devreye alacağı kendi ulusal internet altyapısını kurmaya yönelik çalışmalarına hemen başlamalıdır. Bu ağ kurulduktan sonra mutlak suretle bu ağın işleyişi ve güvenliği test edilmelidir.

Siber güvenlik ulusal güvenliğin değişmez bir parçasıdır. Siber uzayın varoluşsal bir getirisi olan siber saldırılar, bir ülkede hem parasal kayıplara, hem kamu hizmetlerinin aksamasına, hem de devletin ulusal ve uluslararası düzeyde itibar kaybına neden olmaktadır. Kamu yönetimi idarecilerinin bu saldırıları engellemek ve siber güvenliğe yönelik çözümler üretmek kaçınılmaz bir sorumluluk haline gelmektedir.

8. KAYNAKÇA

Adams Jr, J. A. (2015). Cyber Blackout: When The Lights Go Out-Nation At Risk, Victoria Canada: Friesen Press.

Amoroso, E. G. (2013). Cyber Attacks: Protecting National İnfrastructure. USA: Elsevier Publishing.

Andress, J. ve Winterfeld, S. (2014). Cyber Warfare: Techniques, Tactics And Tools For Security Practitioners, USA: Elsevier Publishing.

Arashi, R. (2017). Defense Policy And The Internet Of Things: Disrupting Global Cyber Defenses. Deloitte.

Bannelier-Christakis, K. (2015). Is The Princible Of Distinction Stil Relevant İn Cyberwarfare?, (Eds.), Research Handbook On International Law And Cyberspace, İçinde (343-365). United Knigdom: Edward Elgar Publishing.

Belmas, G., Overbeck, W., Shepard, J. (2016). Major Principles Of Media Law, Boston Usa: Cengage Learning.

Bhatia, M. V. (2003). War And Intervention: Issues For Contemporary Peace Operations, USA: Kumarian Press.

Boyer, W. ve Mcqueen, M. (2008). Ideal Based Cybersecurity Technical Metrics For Control Systems (Ed.), Critical Information Infrastructures Security İçinde (246-260). Berlin, Germany: Springer Science & Business Media.

Brilingaite, A., Bukauskas, L., Kutka, E. (2017). Development Of An Educational Platform For Cyber Defence Trainig (Eds.), ECCWS 2017 16th European Conference On Cyber Warfare And Security İçinde (73-81). UK: Academic Conferences And Publishing Limited.

Brown, G. D., Walker. P., Bell A. W. (2016). Military Cyberspace Operations, (Eds.), U.S. Military Operations: Law, Policy, And Practice, İçinde (123-166). New York: Oxford University Press.

Butrimas, V. (2016). International Implications Of Securing Our SCADA/Control System, (Eds.), Handbook Of SCADA/Control Systems Security, İçinde (81-106). USA: CRC Press.

Caldwell, D., ve Williams Jr, R. E. (2016). Seeking Security In An Insecure World, Maryland: Rowman & Littlefield Publishers.

Carr, J. (2010). Inside Cyber Warfare: Mapping The Cyber Underworld. USA: O'Reilly Media Inc.

Cavelty, M. D. (2008). Cyber-Security And Threat Politics: Us Efforts To Secure The Information Age, New York: Routledge.

Coburn, A., Leverett, E., Woo, G. (2019). Solving Cyber Risk: Protecting Your Company And Society, New Jersey: John Wiley & Sons.

Cole, D. (2014). What Should We Do About The Leakers? (Ed.), After Snowden: Privacy, Secrecy, And Security İn The Information Age, İçinde (121-140). New York: Macmillan.

Daly J. C. K. (2019). In Russia Cyberattacks Are Used To Punish Its Former Republics, (Ed.), Cyberterrorism And Ransomware Attacks, İçinde (71-76). New York: Greenhaven Publishing.

Davis, B. L. (1990). Qaddafi, Terrorism, And The Origins Of The U.S. Attack On Libya, New York: Praeger Publishers.

Dinniss, H. H. (2012). Cyber Warfare And The Laws Of War, New York: Cambridge University Press.

Dyczok, M. (2015). Mass Media Framing, Represenations And Impact On Public Opinion, (Eds.), Ukraine's Euromaidan: Analyses Of A Civil Revolution,İçinde (77-94). Stutgart Germany: İbidem Press.

Emery, J. (2012). Cyber Warfare: The Stuxnet Virus And Its Implications For Interstate Conflicts, (Ed.), On The Cyber, İçinde, USA: Lulu.

Futter, A. (2018). Hacking The Bomb: Cyber Threats And Nuclear Weapons, Washington, DC: Georgetown University Press.

Gelles, M. G. (2016). Insider Threat: Prevention, Detection, Mitigation, And Deterrence, Oxford: Butterworth-Heinemann.

Ghernaouti-Helie, S. (2013). Cyber Power: Crime, Conflict And Security In Cyberspace. Switzerland: Ecole Polytechnique Federale De Lausanne (EPFL) Press.

Hatashe (2014), Story Of PRISM And Others, USA: Lulu Press.

Higgins, M. (2017). Edward Snowden: Nsa Whistle-Blower, Minesota: ABDO Publishing.

Holmes, D. E. (2017). Big Data: A Very Short Introduction, New York: Oxford University Press.

Hopia, H. (2015). Dawn Of The Drones: Europe's Security Response To The Cyber Age, Brussels: Wilfried Martens Centre For European Studies.

House Of Commons Defence Committee. (2012). Operations In Libya: Ninth Report Of Session 2010-12, London: The Stationery Office.

Inboden, W. (2016). Grand Strategy And Petty Squabbles, (Eds.), The Power Of The Past: History And Statecraft, İçinde (151-180). Washington Dc: Brookings Institution Press.

Jun, J., Lafoy, S., Sohn, E. (2015). North Korea's Cyber Operations: Strategy And Responses, Washington: Rowman & Littlefield.

Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., Ve Oberholtzer, J. (2017). Lessons From Russia's Operations In Crimea And Eastern Ukraine, California: Rand Corporation.

Koval, N. (2019). In Ukraine A Revolution Coincided With Foreign Cyberattacks, (Ed.), Cyberterrorism And Ransomware Attacks, İçinde (83-88). New York: Greenhaven Publishing.

Krasynska, S. (2015). Digital Civil Society: Euromaidan, The Ukrainian Diaspora, And Social Media, (Eds.), Ukraine's Euromaidan: Analyses Of A Civil Revolution, İçinde (177-198). Stutgart Germany: İbidem Press.

Lee, N. (2015). Counterterrorism And Cybersecurity: Total Information Awareness, Switzerland: Springer International Publishing.

Lehtinen, R., Russell, D., Gangemi, G. T. (2006). Computer Security Basics, Usa: O'reilly Media, Inc.

Lemieux, F. (2019). Intelligence And State Surveillance In Modern Societies: An International Perspective, Bingley: Emerald Group Publishing.

Lewis, J. A. (2017). Cybersecurity: A U.S. Perspective, (Eds.), A Roadmap For U.S.-Russia Relations, İçinde (62-67). New York: Rowman & Littlefield.

Lewis, J. A. (2018). Rethinking Cybersecurity: Strategy, Mass Effect, And States, New York: Rowman & Littlefield.

Loukas, G. (2015). Cyber-Physical Attacks: A Growing Invisible Threat, Oxford: Butterworth-Heinemann.

Lowenthal, M. M. (2017). Intelligence: From Secrets To Policy, Usa: Cq Press.

Marzilli, A. (2005). Policing The İnternet. New York: Infobase Publishing.

Mazanec, B. M. (2015). The Evolution Of Cyber War: International Norms For Emerging-Technology Weapons, Nebraska: Potomac Books Of University Of Nebraska Press.

Mazanec, B. M. ve Thayer, B. (2015). Deterring Cyber Warfare: Bolstering Strategic Stability In Cyberspace, UK: Palgrave Macmillan.

Mcnabb, D. E. (2016). Vladimir Putin And Russia's Imperial Revival, New York: CRC Press.

Medvedev, S. A. (2015). Offense–Defense Theory Analysis Of Russian Cyber Capability, USA: The Naval Postgraduate School (NPS) Institutional Archive.

Mehan, J. E. (2008). Cyberwar, Cyberterror, Cybercrime. UK: IT Governance Publishing.

Mowbray, T. J. (2014). Cybersecurity: Managing Systems, Conducting Testing, And Investigating Intrusions, Indiana: John Wiley & Sons.

Nikkarila, J. P., ve Ristolainen M., (2017). Runet 2020: Deploying Traditional Elements Of Combat Power In Cyberspace?, (Eds.), Game Changer: Structural Transformation Of Cyberspace, İçinde (27-50). Tampere Finland: Finnish Defence Research Agency Publications.

Peters, J. (2018). Critical Perspectives On Cyberwarfare, New York: Enslow Publishing.

Rainie, L., Anderson, J., Connolly, J. (2019). State-Sponsored Cyberattacks Are Likely To Increase, (Ed.), Cyberterrorism And Ransomware Attacks, İçinde (64-70). New York: Greenhaven Publishing.

Reisinger, H., ve Golts, A. (2014). "Russia's Hybrid Warfare: Waging War Below The Radar Of Traditional Collective Defence", Research Paper, Research Division, Rome: NATO Defence College.

Rhodes, R. (2011). Cyber Meltdown: Bible Prophecy And The Imminent Threat Of Cyberterrorism, USA: Harvest House Publishers.

Rios, B. K. (2009). Sun Tzu Was A Hacker: An Examinaiton Of The Tactics And Operations From A Real World Cyber Attack (Eds.), The Virtual Battlefield: Perspectives On Cyber Warfare, İçinde (143-155). Amsterdam: IOS Press.

Ronzhyn, A. (2014). The Use Of Facebook And Twitter During The 2013-2014 Protests In Ukraine (Eds.), ECSM 2014 Proceedings Of The European Conference On Social Media, İçinde (442-449). UK Brighton: Academic Conferences Limited.

Roscini, M. (2014). Cyber Operations And The Use Of Force In International Law, United Kingdom: Oxford University Press.

Roscini, M. (2017). Military Objectives In Cyber Warfare, (Eds.), Ethics And Policies For Cyber Operations: A NATO Cooperative Cyber Defence Centre Of Excellence Initiaitive, İçinde (99-114). Switzerland: Springer International Publishing.

Rowe, N. C. (2017). Challenges Of Civilian Distinction In Cyberwarfare, (Eds.), Ethics And Policies For Cyber Operations: A NATO Cooperative Cyber Defence Centre Of Excellence Initiative, İçinde (33-48). Switzerland: Springer International Publishing.

Rugge, F. (2018). An 'Axis' Reloaded?, (Ed.), Confronting An 'Axis Of Cyber'?: China, Iran, North Korea, Russia In Cyberspace, İçinde (13-38). Milano: Ledizioni Ledi Publishing.

Russell, A. L. (2014). Cyber Blockades. Washington, DC: Georgetown University Press,

Sanalp, S. (2016). "Çeşitli Ülkelerde Usom Ve Some Yapılandırılması Ve Türkiye Modeli Önerisi". (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Bilgi Üniversitesi, İstanbul.

Sanger, D. E. (2018). The Perfect Weapon-War, Sabotage And Fear In The Cyber Age, New York: Broadway Books.

Savunma Sanayi Dergilik, "Siber Uzay, Milli Güvenlik Açısından Kritik Hale Geldi", 09.03.2020, https://www.savunmasanayiidergilik.com/tr/haberdergilik/siber-uzay-milli-guvenlik acisindan-kritik-hale-geldi, (26.05.2020).

Shackelford, S. J. (2014). Managing Cyber Attacks In International Law, Business, And Relations. New York: Cambridge University Press.

Shindler, C. (2014). Introductions: Israel And The World Powers, New York: IB Tauris Publishers.

Sienkiewicz, H. J. (2017). The Art Of Cyber Conflict, Indianapolis: Dog Ear Publishing.

Simons, G. (2016). Euromaidan And The Geopolitical Struggle For Inflence On Ukraine Via New Media, (Eds.), Eurasia 2.0: Russian Geopolitics In The Age Of New Media, İçinde (275-294). Maryland: Lexington Books.

Solomon, M. G. (2019). Security Strategies In Windows Platforms And Applications, USA: Jones & Bartlett Learning.

Stacy, I. (2015). Watching, Policing: Surveillance And Complicity, (Eds.), The Wire And America's Dark Corners: Critical Essays, İçinde (170-191). North Carolina: Mcfarland & Company, Inc., Publishers.

Theohary, C. A. ve Rollins, J. (2009). Cybersecurity: Current Legislation, Executive Branch Initiatives, And Options For Congress, Washıngton DC: Congressional Research Service.

Thomas A. Johnson, Critical Infrastructures, Key Assets: A Target-Rich Environment, (Ed.), Cybersecurity: Protecting Critical Infrastructures From Cyber Attack And Cyber Warfare, İçinde (33-66). USA: CRC Press.

Touhill, G. J. ve Touhill, C. J. (2014). Cybersecurity For Executives: A Practical Guide, New Jersey: John Wiley & Sons.

Trenin, D. (2010). Afterword, (Ed.), The Politics Of Security In Modern Russia, içinde (195-198). Farnham: Ashgate Publishing.

Trim, P. ve Lee, Y. (2014). Cyber Security Management: A Governance, Risk And Compliance Framework. USA: Gower Publishing Limited.

UN. (2017). "Report Of The Human Rights Council", Erişim adresi http://undocs.org/en/A/72/53, (26.09.2020).

Valeriano, B., Jensen, B., Maness, R. C. (2018). Cyber Strategy: The Evolving Character Of Power And Coercion, New York: Oxford University Press.

Vego, M. N. (2007). Joint Operational Warfare: Theory And Practice, USA: Government Printing Office.

Vesilind, P. (2008). The Singing Revolution, Tallinn Estonia: Varak Publishers Ltd.

Wakefield, J. (2020). "Russia 'Successfully Tests' Its Unplugged Internet", 24 December 2019, https://www.bbc.com/news/technology-50902496, (12.04.2020).

Westby, J. R. (2004). International Guide To Cyber Security, USA: American Bar Association.

Xiang, P., Tianye, X., Zhiting, X., Xuan, G. (2018). The Enlightment Of Nine Classical Cyber Warfare, (Eds.), Advances On Broad-Band Wireless Computing, Communication And Applications, İçinde (695-703). Switzerland: Springer International Publishing.

Zetter, K. (2014). Countdown To Zero Day: Stuxnet And The Launch Of The World's First Digital Weapon, New York: Crown Publishers.