ACADEMIC REVIEW OF HUMANITIES AND SOCIAL SCIENCES
Volume: 3 Issue: 1 Year: 2020, pp. 36-58

ARHUSS
ISSN: 2636-7645

SİBER UZAY'DA ÜSTÜNLÜK MÜCADELESİ; AMERİKA BİRLEŞİK DEVLETLERİ VE RUSYA FEDERASYONU [1]

Osman GİRGİN [2]

Received Date (Başvuru Tarihi): 05/05/2020
Accepted Date (Kabul Tarihi): 10/05/2020
Published Date (Yayın Tarihi): 15/06/2020

ÖZ

Ağ teknolojileri temelli gelişmeler günümüzde hayatın her alanına nüfuz etmiştir. Bu nedenle söz konusu teknolojilerin ile ilgili olarak önemli riskler ve yeni nesil tehdit odakları oluşmaktadır. Siber uzay kaynaklı tehditler gün geçtikçe daha fazla bir şekilde günlük hayatın her alanına nüfuz etmektedir. Devletler siber uzaya ilişkin stratejilerini belirleme noktasındaki gayretleri de artmaktadır. Karmaşık ve sınırı belli olmayan siber uzayda devletlerin etkinliği, güç politikaları ve işlevselliği daha fazla tartışılmaktadır. Kara, deniz, hava ve uzaydan sonra literatürde insan eliyle oluşturulmuş olan beşinci boyut olarak adlandırılan siber uzayı anlamaya yönelik analizlere günümüzde ağırlık verilmektedir. Siber uzayın sınırları belli olmayan ve anonim yapısı nedeniyle oluşturduğu güvenlik riskleri ortadadır. Bu itibarla da siber uzay ile ilgili gelişmeleri sahip oldukları teknolojik altyapı ve ekonomik büyüklük kapsamında Amerika Birleşik Devletleri (ABD) ile Rusya Federasyonu (RF)'nun küresel ölçekte domine ettikleri ifade edilebilecektir. Bu kapsamda çalışmada ABD ve RF'nin siber uzay alanı ile ilgili takip ettikleri stratejileri öncelikle analiz edilecektir. Vaka çalışması yönetimi bağlamında yapılacak analiz ile ilgili ülkelerin siber uzaya yönelik tecrübe etmekte oldukları gelişmeler açık kaynakların taranması kapsamında irdelenecektir. Sonuç olarak ise çalışmada siber uzayı anlamaya yönelik kavramsal bir çerçevenin oluşturulmasına çalışılacaktır.

Anahtar Kelimeler

ABD
RF
Siber Uzay
Siber Güç
Siber Güvenlik

THE STRUGGLE FOR SUPERIORITY IN CYBER SPACE; UNITED STATES AND THE RUSSIAN FEDERATION

ABSTRACT

Network-based developments have penetrated all areas of life today. For this reason, significant risks and new generation threat occur related to these technologies. Threats coming from cyber space penetrate more and more everyday life. States are also increasing their efforts to determine their strategies for cyber space. In complex and unlimited cyberspace, the effectiveness, power policies and functionality of states are further discussed. Today, we focus on understanding the cyber space, which is called the fifth dimension created in the literature by human, after land, sea, air and space. The security risks posed by cyber space due to its uncertain and anonymous structure are evident. In this respect, it can be stated that the developments in cyber space are dominated by the United States (USA) and the Russian Federation (RF) on a global scale within the scope of their technological infrastructure and economic size. In this context, the strategies followed by the USA and RF regarding cyber space will be analyzed first. In the context of a case study, the developments experienced by the countries regarding cyber space will be examined within the scope of scanning open sources. As a result, the study will attempt to create a conceptual framework for understanding cyber space.

Keywords

The USA,
The RF,
Cyber Space,
Cyber Power,
Cyber Security

Citation: Girgin, O. (2020), Siber Uzay'da Üstünlük Mücadelesi; Amerika Birleşik Devletleri Ve Rusya Federasyonu, ARHUSS, 3(1): 36-58

[1] *Bu çalışma, İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Uluslararası İlişkiler programı için hazırlanan "21'inci Yüzyılın Yükselen Güç Unsuru Siber Güç Ve Türkiye" başlıklı yüksek lisans tezinden türetilmiştir.*

2 *İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü Yüksek Lisans Öğrencisi, girginosman@outlook.com.tr*

1.GİRİŞ

Dünya'nın tarımsal toplumdan, endüstriyel topluma geçişi uzun yıllar almış olsa dahi; bilgi toplumuna geçişi, teknolojinin gelişimi sonrası kısa sürede gerçekleşmiştir. Teknolojinin hızla gelişmesi sayesinde, kişilerin bir birileri ile olan etkileşimi bilgisayar ekranı karşısında mümkün hale gelmiştir. Kişi ve kurumların gizli bilgilerine ulaşabilir olmak, günümüz yaşamında daha kolaylaşmıştır.

Devletler ve bireyler bilgisayar, taşınabilir bilgisayar ya da telefonların saklama hafızalarında kişisel verilerini, gizlilik derecesinde olan bilgi ve belgelerini uzun süreli olarak muhafaza edebilmektedirler. tutabilmektedir. Bu itibarla da ağ teknolojileri ile bağlı olan tüm objelerin oluşturduğu sanal alanın güvenliği de büyük önem arz eder hale gelmiştir (Burke,2018:139). Bu durumda devletlerin de güvenlik anlayışlarını klasik yöntemlerin ötesinde yeni bakış açılarıyla ele almaları da gerekmektedir. Bu noktada tarihi süreçte bilginin önemli olduğunu anlayan ve bilen her uygarlık, bilgiyi korumak için, döneme göre güvenlik anlayışlarını değiştirerek geliştirdikleri de hatırlanmalıdır.

Bilgi, her dönem büyük önem arz etmiştir. Bilişimin gelişmesi ve bireylerin internet üzerinden verileri hızlıca kullanması sonucu siber uzayda toparlanan ve ağlar ile birbirine bağlantılı halde olan bilgi günümüzde daha da önemli hale gelmiştir.

Günümüzde milyonlarca insanın internet kullandığı tartışılmazdır. Günümüzde 4.445.045.224 kişi internet kullanmakta, yılda ise 207.304.987.224 kadar da mail alışverişi olmaktadır. Bütün sosyal medya kullanıcılarını, kilitlenmiş olan internet sayfalarının hesaplaması yapıldığında, oluşan veri milyarlarla ifade edilebilecek durumu gelmiştir. (Darıcılı,2018:311).

2. SİBER UZAYA İLİŞKİN KAVRAMSAL ÇERÇEVESİ

Siber uzay hakkında ortak bir tanım üzerinde görüş birliğine varmak oldukça zor görülmektedir. Genel bir yaklaşım ile bu kavramı, internet altyapıları kapsamında insan eliyle oluşturulmuş teknolojik bir alan ve insanların birbirleriyle hızlı bir şekilde teknolojik platformda iletişim halinde bulunmaları olarak yorumlamak mümkün olabilir. Bu teknolojik platform sayesinde bilginin akış hızı da değişmiştir. Günümüzde bilgi sadece depolanan bir veri olmaktan çıkıp, teknoloji ile uyumlanarak işlenen ve çok hızlı şekilde kullanıcısı tarafından dağıtılan etkin bir araca dönüşmüştür. (Darıcılı,2017:2). Bilginin

insanüstü bir hızla aktarılması siber uzayın sonsuzluğu kavramı ile birleştiğinde, siber güvenliğin farklı boyutları öne çıkmaktadır. Siber alanların sağladığı imkânlar ile askeri alanda yeni cepheler, yeni haber platformları, finansal ve ekonomik verilere farklı erişim kaynakları ya da yeni dünya düzeninde alışılmışın dışında yeni politik alanlar açabileceği ön görülmektedir.

William Gibson, 1984 yılında yayınladığı Neuromancer isimli kitabında siber uzay alanından bahsetmektedir. Gibson kitabında, genç bir hırsız olan Case isimli şahsın bir jak ile siber uzay içerisinde bulunan sisteme bağlandığını ve işverenler tarafından verilen önemli yazılımlar sayesinde büyük şirketlerin sistemlerine giriş yaptığını anlatmaktadır. (Gibson,2012:8). Diğer yandan 4 Ekim 1957 yılında Sovyetler Birliği'nin dünya yörüngesine ilk uyduyu yerleştirmesi, daha sonra da Sputnik 2'yi uzaya göndermesi ve buna karşı ABD'nin ARPA (Advanced Research Projects Agency) teknolojisini geliştirmesi sonrasında İnternet'in temelleri atılmıştır. ARPA, ABD'nin ticari ve askeri faaliyetleri için kullanılmış ve 1970'li yıllarda da hızlı iletişim ağının gerekliliği neticesinde ABD müttefikleri tarafından da istifade edilmeye başlanmıştır. FTP (File Transfer Protocol) teknolojisi ile dosyalar aktarılmaya başlanmış ve böylece ARPA sistemi ile bugün ki internetin nüvesi gelişmeye başlamıştır. (Bıçakçı,2013:4-7) Sistem bir süre kullanıldıktan sonra, 1980'li yıllarda ilk virüsle karşılamıştır. Durum mesajlarına gelen virüs sistem durdurmuş ve siber güvenlik konusunu gündeme gelmesine neden olmuştur.

Siber uzay günümüzde yaşamımızın her alanına girmiştir. Öte yandan dinamik yapılarının çözülmesi ve bu alanda ki en önemli konu olan güvenlik zaaflarının azaltılması için siber gücün hangi statüde değerlendirileceği noktasında çeşitli fikirler ortaya atılmakta ve yoğun tartışmalar süregelmektedir. Uluslararası ilişkiler teorilerinin argümanlarıyla siber güç kavramının değerlendirilmesi oldukça karışık ve karmaşık bir hal almaktadır. Joseph Nye, insan yaşamına yoğun olarak giren siber alan ile güç dengelerinin çok yönlü bir değişim yaşayacağından bahsetmektedir. Siber gücün hem sert, hem de yumuşak güç olarak tarif edilebileceği değerlendirilmektedir. Enformasyon açısından diğerlerini etkilememesi durumunda yumuşak güç kavramı, başkalarına zarar verdiğinde ise sert güç olarak değerlendirebileceğimizi belirtmiştir. Sert güç kavramına örnek olarak Stuxnet saldırılarını göstermektedir (Güner,2014).

Ayrıca Nye, içinde bulunduğumuz yüzyıl ile geçmiş yüz yılların karşılaştırmasının dahi yapılamayacağını belirterek, teknolojik iletişim çağında, akan bilginin fazlalığı

sebebiyle, bilgilerin odak noktasının iyi tespit edilemeyeceğini, protokollerin çizgisine uyulmayan iletişim stratejilerinin bir işe yaramayacağını ve işlevsiz hale geleceğini belirtmektedir. Nye ayrıca, yumuşak güç ve akıllı güç elemanlarını doğru ve etkin kullanarak, gelişen teknoloji ile karşılıklı ağların oluştuğunu ve ağ kurmanın çok önemli bir seçenek haline geldiğini söylem olarak savunurken, siber alan kullanımının doğru güç unsurları ile kullanılmasına vurgu yapmaktadır (Nye,2003:153-167). Tüm toplumların siber alanlar aracılığıyla birbirine bağlı bir hayat yaşamaya başladığı bir dönemde, sınırlar ve mesafeler tehdit unsuru olmaktan çıkabilmektedir.

Ralph Langer, Stuxnet virüsünün yazılımını kırarak ün kazanmış bir isimdir. Langer, siber alan ve siber gücü tanımlamaktadır. Anılan siber alanı; "*insanlar tarafından meydana getirilmiş, akıllı elektrik şebekelerinin oluşturulması*" şeklinde tanımlamıştır. "*Bir aktörün, bireyin ya da toplumun yaşayacağı muhtemel bir çatışma sırasında, yaptırım uygulanması için oluşturulan dijital organizasyonu*" şeklindeki yaklaşımıyla da siber güç kavramını tarif etmiştir (Langer,2016). Daniel T.Khuel'in siber uzay ve siber güç alanlarında problemleri tanımlamak adına, siber uzayın insanoğlu tarafından üretilmiş olmasına rağmen, diğer dört doğal alandan (hava, deniz, toprak, uzay) farksız olduğunu, bu alanlara girmek ve kontrol altında tutmak için insan eliyle üretilmiş teknolojik imkanlara ihtiyaç duyulduğunu belirtmektedir. (Khuel,2009:28-29).Khuel ile benzer fikirleri olan John B. Sheldon'da siber alan ile siber gücün birbirinden ayırt edilmesi gerektiğini belirterek, siber alanı şu şekilde tanımlamaktadır; "*siber teknoloji işlemlerinin gerçekleştiği ve toplumu değiştiren matbaa, telgraf, radyo, televizyon ve telefondan sonra en büyük bilgi iletme ve alma alanıdır*". Siber gücü ise "*bu alanlarda, teknoloji ile gerçekleşmesi olası operasyonların, stratejik etki ve kontrolü*" olarak belirtmektedir. Sheldon siber alanlar içerisinde gerçekleşecek olan operasyonlarla, düşmanın tüm dijital bağlantılarının kesilebileceğini ve bir savaşta en önemli unsurlardan biri olan istihbarat birimlerinin kontrolünün karşı tarafın eline geçirilebileceğini savunarak, esasında savaşın doğasının yeni oluşumlarla dahi değişmediğini belirtmektedir. Sheldon ayrıca sert güç ya da yumuşak güç unsurlarının kara, deniz, hava, uzay gibi alanlarda tek başlarına kullanılmasının yetersiz olacağını belirterek, daha ekonomik olabilecek stratejik bir güç unsuru olarak siber gücü ulusal strateji planlamasında uygulamaya geçilmesi gerektiğini ifade etmiştir (Sheldon,2012:207-211).

Steven Bucci, siber alanlardan gelebilecek olan tehditlerin etki alanını basit ev kullanıcısı bireylere kadar indirgenebileceğini savunmaktadır. Siber tehdit unsurunun bireylerden, eğitilmiş ve konusunda uzman devletin kritik birimlerinde görevlilerine kadar uzanabileceğini, her tip kullanıcının kişisel bilgilerinin ve ulusal veri tabanlarında bulunan bilgilerin ele geçirilmesine uzanacak geniş bir siber saldırı alanının olabileceğini, en büyük tehdit aktörlerinin ise gelişmiş devletler olabileceğini belirtmiştir. Zira büyük ve gelişmiş devletlerin sahip olduğu yetenekli insan gücünün, ekonomik gücünün ve endüstriyel anlamda donanımlı olmalarının altını çizerek, gelişmiş devletlerinin siber alanda oluşturabilecekleri tehditlere vurgu yapmaktadır. Anılan ayrıca, siber saldırının belirli bir süre için ya da kalıcı olacak şekilde kontrollü yapılabileceğini ve bu saldırılar sırasında zorlayıcı güç şeklini alabileceğini, hedef aldığı kitlenin milliyetçi duygu ve hassasiyetlerini manipüle ederek, olayların yönünün kendi lehinde hızlandırabileceğini ifade etmiştir (Bucci,2012:57). Söz konusu ifadelerden anlaşılacağı üzere; Bucci siber gücü tam anlamıyla "*güç unsuru*" olarak tanımlamamıştır. Aksine adı geçen siber gücü; "*yumuşak güç, hem de sert güç çerçevesinde değişken unsurlar*" olarak kavramsallaştırmaktadır.

Bunlarla birlikte, yaşadığımız dönem terörist unsurları yok eden askeri güçler, bilgi aktarımlarını ise bir ağ aracılığıyla yapmaktadırlar. Ayrıca diplomaside siber gücün adımları atılmakta, büyük sermayeleri yönetenler dijitalleşme alt yapısını oluşturulmakta, dünya ve ülkeler üzerinde etkili güçler olan medya grupları siber ağlar ile anlık olarak bilgi yayılmaktadır. Facebook, Instagram, Twitter, Pinterest gibi geniş sosyal medya alanları sayesinde milyonlarca kişi aynı anda etkileşim kurarak büyük, küresel ve sınırsız bir bağ oluşturabilmektedir (Slaughter,2009:88-94). Gelişen internet teknolojisi ile kullanıcıdan kullanıcıya ve kullanıcılara bağlanabilen çok sayıda birey hızlı iletişim olanağından yararlanabilmektedir.

Tablo 1: Anlık Olarak İnternet Kullanıcıları (Erişim Tarihi: 27.10.2019)

Anlık olarak İnternet Kullanıcıları	*4,375,683, 375 ...*
Bugüne Kadar Açılan Web Sitesi	*1,724,197,975*
Bugün Gönderilen E-Posta	*248,873,292,621*
Bugün Google İle Yapılan Arama	*6,566,640,527*
Bugün Yayınlanan Tweetter	*731,863,260*

Bugün Youtube İçeriğinde İzlenen Video	*6,825,576,840*
Bugün İnstagram Yüklenen Fotoğraf Sayısı	*79,872,000*
Bugün Satılan Bilgisayar Sayısı	*677,467*
Bugün Satılan Akıllı Telefon Sayısı	*4,127,986*
Bugün Oluşan İnternet Trafiği	*6,832,743,426 GB*
Bugün İnternet İçin Kullanılan Elektrik	*3,923,676 Mega Wat*

Kaynak: https://www.internetlivestats.com/

Yukarıda ki tabloda gösterilen verilere bakıldığında; bu kadar anlık ve hızlı kullanımı olan siber alanın kendisinin bir yansıması olduğu açıkça görülebilmektedir. Yukarıda birçok araştırmacının tanımlamaları çerçevesinde siber uzay ve ya siber güç kavramı ile ilgili genel bir tanımlama yapılmasının oldukça zor olduğu anlaşılmaktadır. Bunun nedeni, bizce bu kavramların akademik sistemde arıtılmış olması ile ilgilidir. Siber uzay veya siber güç kavramının analitik bulanıklık içerisinde olduğu ve teorik kapsamda henüz yetersiz analiz düzeyinde kaldığı ileri sürülebilir.

3. SİBER UZAY'DA ÜSTÜNLÜK MÜCADELESİ OLUŞTURMAK

Siber uzayın devletlerin ulusal güvenlik alanlarını ne kadar zarara uğratabileceği tahmin edilememektedir. Bu nedenle, siber uzayın devlet güvenliği üzerinde yarattığı riskleri önceden tanımlamak mümkün olmayabilir. Bugüne kadar tespit edilebilen bazı saldırıların yıllık olarak devletlere bir trilyon dolardan fazla zarar vermiş olabileceği tahmin edilmektedir (Kane,2010:5). Teknolojinin hızını dahi takip edemediğimiz günümüzde, teknolojinin internet ile entegre olmasıyla çok dinamik bir yapı ortaya çıkarmaktadır. Bu dinamik yapının öğelerine baktığımızda karmaşık ve çok boyutlu bir içeriğe sahip olduğunu görebilmekteyiz. Bireylerden, uluslararası şirketlere, devletlere kadar uzanan birçok unsur bu yapıya dâhildir. Tüm bu karmaşık yapının içerisinde ağların güvenliğini sağlamak için devletlerin üst düzey güvenlik politikalarını, dijital dünya ve siber uzay alanlarına taşımaları gerekmektedir. Zira siber dünyada oluşabilecek zararlar hakkında birçok senaryo mevcuttur. Geçmiş yıllarda Yahoo gibi bazı internet sitelerinin hacklenmesi kötü bir senaryo olarak belirtilirken, bugün geldiğimiz noktada kötü senaryolar çok daha kapsamlı ve tehlikeli hale gelmiştir. Örneğin kötü niyetli şahısların, kurumların ya da devletlerin hedef aldıkları bir ülkeyi, internete bağlı olarak çalışan,

elektrik santralleri üzerinden gerçekleştirecekleri saldırı ile elektriksiz bırakabilmesi akla gelen kötü senaryolarda sadece bir tanesidir (Schmidt,2010:4). Benzeri Türkiye'de de görülmüştür. Batman Ilısu Barajı'ndan alacağını tahsil edemeyen Alman şirketi, santralde ki bilgisayarları şifreleyerek, tüm sistemi kilitleyebilmiştir (Milliyet Gazatesi,2003).Bu olayın sonucunda, Batman Ilısu Barajı'ndan elektriği sağlanan bölgelere uzun süre elektrik verilememiştir. Bu örnekten anlaşılacağı üzere sadece devletlerin değil, şirketlerin ve bireylerin bile siber araçları kullanarak ne derece güçlü olabilecekleri ve yol açabilecekleri tehdidi göstermesi açısından önemlidir (Canberk ve Sağıroğlu,2006:161).

Devletler için, siber uzayda sürekli ve güncel olan çalışmalar dengeleri sağlamak adına önemlidir. Yukarıda bahsedildiği gibi siber uzay ve siber güvenlik kavramları için genel bir tanım halen yapılamamaktadır. Siber saldırıların failinin meçhul olması sebebiyle, uluslararası hukuk çerçevesinde değerlendirilmesi mümkün olmamaktadır. Siber saldırıların kaynağının devletler mi ya da bireyler mi olduğunun tespitinin mümkün olmaması bu değerlendirmenin yapılamamasının temel nedenlerinden biridir (Gürkaynak ve İren,2011:265). Bunun yanı sıra devletler, siber güvenliklerini sağlamak amacıyla kendi milli yazılımlarını yapmaya, yazılımların içerik bilgilerini oluşturmaya ve yerli şifre sistemlerini üretmeye de gayret etmektedirler.

4. SİBER UZAY'DA AMERİKA BİRLEŞİK DEVLETLERİ

Soğuk Savaş'ın iki büyük aktöründen biri olan ve dünya üzerinde süper güç olarak tanımlanan ABD, kamu ve özel sektörde bilişim sistemlerini temellendirmek üzere bazı üniversiteleri seçerek çeşitli AR-GE enstitüler oluşturmaktadır. ABD, oluşturduğu bu mekanizma ile seçilen üniversitelerin her birini teknolojileri geliştirecek üstler olarak görmektedir (Atay ve Hancıoğlu,2019:522-525). ABD 20. Yy. başından itibaren teknolojik gelişmeler ile birlikte siber uzayda güçlü bir aktör olma yolunda hızlı bir ivme kazanmıştır (Darıcılı,2017:63).

İnternet, 1990'lı yıllardan önce sadece askeri platformda kullanılırken, 1990'lar sonrası sivilleşmeye başlamıştır. İnternet'in sivilleşmesiyle beraber; bu dönemde siber güvenlik stratejilerinde yeni düzenlemeler yapılmıştır. Www (Word Wide Web) sistemi ile bilgisayarların siber ağlara bağlantısı kolaylaşmış ve web partallarına daha hızlı erişim sağlanmıştır (Bıçakçı,2013:40). İnternet'in bireylerin kullanımına kadar indiği bu dönemlerde bireyin ve toplumun siber güvenliğinin sağlanması daha çok önem arz

etmiştir. Sanal sosyal ağların, birbirine bu derece hızlı bağlanabiliyor olmasıyla, küreselleşme kavramı giderek daha da artmaktadır.

Küreselleşmeyi oluşturan ana kavram olan siber uzay sistemini yönetmek ve domine etmek isteyen ABD, bu yönde teknoloji temellerini atmaya başlamıştır. 11 Eylül 2001 sonrası, ABD için güvenlik anlamında her şeyin değiştiği tarih olarak belirtilmektedir. Bu tarih sonrasında tehditlerin yeri, zamanı ve kaynağını önceden kestirmek oldukça zor hale gelmiştir. Siber tehditlerin riskleri de aynen bu şekilde tanımlanmaktadır. Siber tehdit unsurunun ne zaman, nereden ve kim tarafından geleceği tahmin edilememektedir. Bu sebeple; 21. yy.'ın güvenlik anlayışı, teknoloji ve internetin hızla gelişmesi nedeniyle küreselleşme eğilimleri çerçevesinde şekillenmektedir. ABD'nin siber güvenlik alanında ki çalışmaları, operasyonel birimler oluşturarak muhtemel tehditlere karşı proaktif tedbirler almak temelinde şekillenmektedir. (Yılmaz,2012).

4.1. Amerika Birleşik Devletleri'nin Siber Uzay'da Güvenlik Çalışmaları

Siber uzay, somut bir kavram olmadığı için bu alanda somut güvenlik tedbirleri de alınamamaktadır. Karmaşık bir yapısı olan siber uzay, sürekli olarak yeni tehditleri üretmeye devam edecektir. ABD'nin siber uzayda güvenlik olarak tanımladığı kavram şu hedefler dahilinde açıklanabilir; Hasım devletlerden gelebilecek saldırılara karşı koyabilme, istihbarat oluşturma ya da karşı istihbarat sağlamayı amaçlayan sistemler kurarak, güvenlik sağlama.

ABD'nin çok sayıda kişi tarafından kullanılan Google, Microsoft, Youtube, Facebook gibi siteler üzerinden, e-mail adreslerini takip ettiği ve sohbet alanlarını gizlice izlediği bilinmektedir (Karagül ve Özkan,2015). ABD'nin siber uzayda amaçladığı politikalar aşağıda ki gibi özetlenebilir (www.whitehouse.gov, 2020);

Politika: Yenilikçi iletişim ve ekonomik rahatlık üzerine kurulmuş, güvenlikli, gizlilik ilkelerine saygılı, gelecek nesillere kültürel mirasları aktararak, kişi ve kurumları güvenilir internet kullanımına teşvik etme. Ayrıca, en önemli konulardan biri olan siber güvenliğin devamlılığı sağlanma, güvenlik konusunda uzman kişiler yetiştirme, güvenliği en üst seviyeye taşıma.

Bozulma ve Koruma: ABD'nin teknolojik alt yapısını bozma girişimlerini tespit etme. Amerikan halkına karşı oluşabilecek siber tehditleri analiz ederek, gerekli karşı tedbirleri alma.

Uluslararası İş Birliği: Konu kapsamında diğer devletler ile sürekli koordine sağlama. Küreselleşen internet kullanımı ile birlikte siber uzay politikalarını uygulayabilme ve devamlılığı tesis etme. Devletin yetkili birimleri, özel şirketlerin yönetim kurulu başkanları ile gerekli fikir alışverişi sağlanma. Siber güvenlik alanlarında, iş birlik için katılım stratejileri düzenleme.

ABD' nin Uzun Süreçte Siber Uzayda İşgücü Sağlaması: Siber güvenlik çalışmalarında yer alabilecek profesyonel kadrolar oluşturmak için, ilkokul çağından, yükseköğrenim müfredatlarına kadar dersleri organize etme. Bu sayede yetenekli ve zeki öğrencilerin geleceğin ABD'sine ait siber güvenlik politikalarında, özel eğitim programlarına dahil olması sağlama. Devletin güvenlik ve terörle mücadele birimleri ile özel sektör iş birliği yaparak, siber güvenlik iş gücünü arttırmak adına devlete raporlar sunma. ABD tüm politikalarını her zaman geleceğe yönelik ve uzun vadeli hazırlama. Siber güvenlik alanında, rekabet politikalarını geliştirmek için diğer devletlerin işgücü durumunu sürekli kontrol etme, bu konuyla ilgili de uzun vadeli politikalar düzenleme.

4.2. Amerika Birleşik Devletleri Kaynaklı Olduğu İleri Sürülen Ve Amerika Birleşik Devletleri'ni Hedef Alan Siber Saldırılar

Teknolojinin hızlanmasıyla birlikte, siber uzayda yaşanan gelişmeler devletler, devlet dışı aktörler ve kişiler tarafından yapılabilecek siber tehditleri daha sık gündeme getirmektedir. Kuşkusuz ki bu gelişmeler, ABD'nin gündemine yeni gelmemiştir. Uzun yıllar içerisinde bu alan için hazırlanılmış ve çalışmalar yapılmıştır. Siber uzay kavramının tanımlamasında genel bir ifade kullanılamadığı gibi, siber saldırıların tanımlaması da halen yapılamamaktadır. Genel olarak siber saldırı şu iki şekilde gerçekleşmektedir. Bilgisayara uzaktan yerleştirilen bir virüs odağının, tüm bellekte ki verileri silmesi birinci yöntem olarak kabul edilmektedir. İkincisi ise nispeten daha az zararlı olabilecek şekilde, bilgisayara yerleşen virüsün sistemi, ağları kullanılamaz ya da güvensiz hale getirmesini amaçlayan yöntemlerdir (Lin,2010:63).

Siber saldırıların yapılma amacı genelde belirsizlik taşımaktadır. Kişisel ya da kurumsal bilgileri ele geçirerek istihbarat oluşturma, bir nedene bağlı olmayan apolitik saldırı veya bilgisayarların ve internete bağlantısı olan teknolojik eşyaların kontrol

etmek, yönetmek gibi motivasyonlar ile oluşabilmektedir. Yöntemleri ve yapılış biçimleri açısından siber tehditler çok çeşitlilik göstermektedir. Oluşabilecek bir siber saldırıda da devletlerin alacağı önlemler karmaşık bir yapı taşımaktadır. Aşağıda bugüne kadar ABD'ye karşı yapılmış ya da ABD tarafından gerçekleştiği iddia edilen bazı siber saldırlar incelenmektedir.

Haınan Adası Olayı: İlk siber savaş olarak anılan "World Wide Web War 1" saldırısıdır. Çinli bir grup tarafından ABD' ye karşı yapılmış ilk siber saldırıdır. 1 Nisan 2001 yılında ABD EP-3E uçağı ile Çin Shenjang J-8 uçağının çarpışması bu siber saldırıya neden olmuştur. Siber saldırı sonrası Beyaz Saray'ın resmi web sitesi saatlerce kapalı kalmış, Adalet Bakanlığı'nın resmi web sitesi de tamamen kilitlenmiştir. ABD' ye ait pek çok internet sitesinde, Çin bayrağı dalgalandırılmış ve Çin marşları çalınmıştır (Smith,2012).

Titan Rain Saldırısı: Titan yağmuru olarak adlandırılan siber saldırıdır. Saldırının Çin tarafından yapıldığı ileri sürülmektedir. ABD'nin askeri üslerine, savunma hatlarına ve havacılık şirketlerine karşı yapıldığı bilinmektedir. Devlet adına büyük önem arz eden, gizlilik derecesi yüksek bilgilere erişildiği tahmin edilmektedir. Titan Rain, ABD 'ya karşı yapılan en yoğun saldırı olarak bilinmektedir (Kabay,2005).

Körfez Savaşı: ABD' nin Irak'a karşı iki farklı zamanda başlatmış olduğu savaşlardır. Birincisi 1993 yılında, akıllı silahlar ve ileri bilgisayar teknolojisinin kullanıldığı saldırılarından oluşmaktadır (Clarke ve Knake,2011:32). 2003 yılında ki ikinci saldırıda ise ABD Irak'ı işgal edeceğini saldırı öncesi e-posta ile Iraklı komutanlara bildirmiş, savaşmadan teslim olma çağrısı göndermiştir. Birçok Iraklı askerin de bu çağrıya olumlu yanıt verdiği ileri sürülmektedir (Çiftçi,2017:183). Körfez Savaşları, televizyon ve internet üzerinden canlı olarak takip edilebildiği için, adeta bir iletişim savaşı olarak tanımlanmaktadır (Bıçakçı,2012).

ABD Askeri Bilgisayarına Saldırı: Mc Kinnon adlı hacker, ABD askeri sistemlerine karşı saldırı yaptığı iddiası ile tutuklanmıştır. McKinnon, 1990 yıllarında bir grupla birlikte siber saldırılar ile ilgili çalışmalar yapmış ve ABD'nin uzaylılar ile ilgili bazı bilgileri dünya kamuoyundan sakladığını düşünerek, on iki yıl sürecek bir saldırı planlamıştır. 2001-2002 yıllarında, bu saldırının ortaya çıkmasıyla, ABD yaklaşık 800.000 dolar değerinde zarara uğramıştır (BBC News,2012).

ABD İnsansız Hava Araçlarına Saldırı: Özellikle Afganistan ve diğer savaş alanlarında kullanılan İHA'larda, pilotların bilgisayarlarında virüs izlerine rastlanmıştır. ABD Hava Kuvvetleri Komutanlığı tarafından rapor edilen bu virüslerin ne amaçla hazırlandığı bilinmemektedir. Bu virüs için 'keylogger' tanımlaması yapılmaktadır. Bilgisayarların tüm tuş hareketlerini kaydettiği bilinen virüsün, ABD Hava Kuvvetleri'nde ne kadar yayıldığı ve hangi güçler tarafından, ne amaçla yapıldığı halen bilinmemektedir (Shactman,2011).

ABD İstihbarat Servislerinin Saldırıları: Siber uzaydan gelebilecek tehditler çok çeşitli olabilmektedir. Ülkeler, kontrol bakımından kilit noktasında bulunan önemli mekanizmaları yönetemeyebilir, devletlerin ulusal güvenliğine ait veriler çalınabilir. Risk ve verilebilecek zararın büyüklüğü ise; saldırıyı yapan unsurların ya da kişilerin bilgi, deneyim, donanım durumlarıyla paraleldir. Bu sebeple devletler tarafından, başka devletlere yapılan siber saldırı faaliyetlerinin, nasıl yapıldığına dair net bir çıkarım yapmak mümkün değildir. Zira 2011 yılında, ABD 'nin istihbarat birimleri Kuzey Kore, Çin, İran ve RF'yi hedef alan başta olmak üzere bilinen 231 adet siber saldırı gerçekleştirmiştir (Gelleman ve Nakashima,2001).

ABD Başkanlık Seçimlerinde Siber Saldırı: ABD'nin ulusal başkanlık seçimlerinde, ilk kez Rusya' nın siber bir müdahalede bulunduğu dile getirilmektedir (Embel,2016). Seçim döneminde, Trump'ın rakibi olan Hillary Clinton'ın bu siber saldırılarla ilgili bilgilere ulaşarak kamuoyuna açıkladığı bilinmektedir. O dönemde, görevde olan ABD başkanı Obama ise RF Devlet Başkanı Putin'i ABD seçimlerden uzak durması için uyarmaktadır. Aynı zamanda hükümet tarafından ilgili Amerikan istihbarat birimlerine gerekli talimatları verilmiş ve araştırılması istenmiştir. ABD' de yaşayan 35 Rus İstihbarat Görevlisi konu ile ilgili oldukları gerekçesiyle sınır dışı edilmişlerdir. ABD sınırları içinde faaliyet gösteren Rus teknoloji firmalarına yaptırım uygulanması da bu saldırılar ile bağlantılı olarak gündeme gelmiştir (The New York Times,2016).

5. SİBER UZAY'DA RUSYA FEDERASYONU

Sovyetler Birliği, Soğuk Savaş'ın en önemli unsurlarından bir diğeridir. Birliğin dağılma sonrası RF, Sovyetler Birliği'nin bıraktığı boşluğu adeta doldurmuştur. 1991 yılında Gorbaçov'un istifa etmesinden sonra, Yeltsin dönemine giren Sovyet Sosyalist Cumhuriyetler Birliği (SSCB), tarihte ki varlığını adeta yeniden tamamlayarak milletlerarası platformda yeni bir dönemin başlanmasına vesile olmuştur. Oluşan yeni

dönemde RF tarafından izlenen politikalar ile dünya farklı bir yapılanmaya doğru evrilmiştir Armaoğlu,2014:846). Gorbaçov'dan sonra tüm sistemi değişen RF'nin 1990-2000 arası politik atılımlarını görmek pek mümkün olmamıştır. RF, büyük ve güçlü devlet olma yolunda ki stratejik politikalarını 2000'lerden sonra uygulamaya başlamıştır (Sönmezoğlu ve Bayır,2014:473).

RF, eskiden SSCB'ye bağlı olan, şu anda bağımsızlığını kazanmış, yeni devletleri politik ve ekonomik çıkarları doğrultusunda kullanmaktadır. Dolayısıyla siber güvenlik alanında da aynı stratejiyi kullanacağı düşünülebilecektir. Zira çevresinde bulunan Estonya ve Gürcistan gibi ülkelere siber saldırılar yaparak bu ülkeleri baskı altına almaya gayret gösterdiği de ileri sürülebilir (Keleştemur,2015:187). Putin döneminden sonra milli yatırım politikasını hayata geçiren RF'nin, siber güvenlik alanında da milli yazılımlar ürettiği ve virüsler geliştirdiği bilinmektedir. Ayrıca, RF'nin bazı yasa dışı gruplara da bu konuda destek verdiği de ileri sürülmektedir. Bu konuyla ilgili olarak ise şu olayı örnek verebiliriz; 27 Nisan 2007' de Estonya' ya yapılan DDoS saldırıları sonrası yapılan tetkikler sonrasında gözlemcilerin yaptığı tespitlerle, bu bilgisayar korsanlarının Rus Devleti'nin bilgisi dahilinde saldırılar yaptığı ısrarla iddia edilmiştir (Wedermye,2012).

5.1. Rusya Federasyonu'nun Siber Uzay Kapsamındaki Güvenlik Stratejileri

RF, 10 Ocak 2000 yılında ulusal güvenlik meseleleri kapsamında bir dış politika belgesi yayınlamıştır. Bu belgede siber güvenlik kavramından da bahsedilmektedir. Yayınlanan belge özetle şu başlıkları içermektedir(https://www.mid.ru, 2000);

- RF, iç ve dış güvenlik politikalarında bireyi, toplumu ve devleti güvence altına almaktadır.
- 1990 sonrası oluşturulan ulusal politikalarda, yeni bir dönemin başladığı ve karşılıklı bağımlılık politikaları içerisinde bulunacağının altı çizilmektedir. Bağımlılık politikasında siyasi, ekonomik, teknolojik ve çevresel faktörlerin önemli rol oynadığı belirtilmektedir.
- Siber güvenlik konusundan ise bilgi güvenliği olarak bahsedilmektedir. Modern teknolojik gelişmelere önem vererek, devlete ait bilgilere izinsiz bir şekilde erişilmesi koruma altına alınmaktadır.
- Siber uzayda ulusal güvenliğin tehdidi sürekli artmaktadır. Küresel güç olan diğer ülkeler Rusya'yı, siber uzay alanından uzaklaştırabilecek, muhtemel düşmanlar üzerinde egemenlik kurabilecek teknolojik cihazlar üretmektedirler. Siber savaşın

dünya genelinde büyük bir tehlike olduğunun algılanması ve tanımının netleştirilmesi gerekmektedir.

- RF, Dünya'da ki teknolojik süreçleri takip etmek için, bütçe kaynakları oluşturmaya ağırlık vermektedir. Bilim eğitimini destekleyerek, milli teknolojik altyapısına, hızlı ve ulusal uygulamalar hazırlamaktadır.
- RF, siber güvenliğini sağlamak için önceliklerin üçe ayırmaktadır. Bunlardan birincisi; sanal bilginin kullanıldığı yerlerde, vatandaşların anayasal hak ve özgürlüklerini korumaktır. İkincisi; RF'nin dünya ile eşzamanlı uyumu sağlanırken, ulusal data altyapısını daha iyi hale getirerek koruma altına almaktır. Üçüncüsü ise siber alanda ki rekabet ile mücadele etmektir.

RF, bulunduğumuz çağda ulusal güvenliğini oluşturmak ve olası tehditlere yerinde müdahale edebilmek için kaynakların akılcı kullanımına öncelik vermektedir. Siber uzay, RF için adeta, yeni bir savaş platformudur (Cirlig,2014). RF'nin siyasal stratejisinde, tüm savaş platformları, mutlaka en üst seviyede hazırlanır. Bu kapsamda RF, ülke menfaatlerini kollamak için, siber uzayda savaşmaktan çekinmemektedir (Darıcılı,2017:122). Bu açıdan bakıldığında, RF'nin oluşturacağı stratejilerde, askeri silahlar ile siber silahları birlikte kullanacağı anlaşılmaktadır.

9 Eylül 2000 tarihinde RF yeni bir doktrin yayınlanmıştır (www.mid.ru, 2000). Bu doktrine göre; bilgi, bilginin altyapısı ve vatandaşların kendi arasında ki dijital iletişimde akışı sağlayan sistemlerin, belli bir düzende olması gerekmektedir. Milli güvenliğin sağlanması, kişisel güvenliğin sağlanması ve toplum güvenliği, teknolojinin hızlı gelişimlerini takip etmekten geçmektedir. Devletin iç ve dış politikaları oluşturulurken, bilgi güvenliği alanlarında stratejik ve güncel görevler oluşturulmaktadır.

RF'nin 2000 yılında yayınladığı doktrin, daha sonra geliştirilerek yeniden düzenlenmiş ve 2016 yılında yeni bir doktrin olarak yayımlanmıştır (www.mid.ru, 2000). Bu doktrine göre; devletlerarası iyi ilişkiler sağlamak için, istikrarlı, çatışmasız ve eşit stratejik ortaklıklar oluşturulmalıdır. Eşit bir şekilde istikrar sağlamak ve stratejik ortaklık oluşturmak için beş itici güçten bahsedilmektedir:

- Bilgi güvenliğini sağlamak, ulusal menfaatlerde devamlılık tesis etmek ve bağımsız bir politika oluşturabilmek adına RF'nin egemenliğini korumak,

- Uluslararası hukuka aykırı oluşumlar, siyasi suç unsurları ya da terör unsurlarına destek için, yasadışı olarak bilgi teknolojilerini kullananlara karşı uluslararası bir siber güvenlik platformunun oluşturulmasında görev almak ,
- Siber uzayın kendine özel yapısını dikkate alarak, ülkeler arasında doğabilecek husumetler ve savaşlar için hem önleme, hem de çözmeyi amaçlayan uluslararası mekanizmaları oluşturmak,
- Siber uzay alanlarında, ilgili uluslararası kuruluşlar ve devletler ile eşitlik ilkesini koruyarak işbirliği yapmak,
- Siber uzay ve güvenlik alanlarında milli oluşumlar sağlamak

5.2.Rusya Federasyonu'nun Siber Uzay'a Yönelik Spesifik Politikaları

RF, toprak bütünlüğünü, halkının güvenliğini, ulusal anlamda kritik altyapılarının kontrolünü sağlamak için ulusal teknolojinin kullanılmasını benimsemektedir. İnternet yolu ile içeriden dışarıya, bilgi sızdırılmasını kanunlar doğrultusunda düzenlemektedir. Böylece meydana gelebilecek siber tehditlere karşı, devletin kontrolü sağlanmaktadır. RF'nin çıkarları kapsamında, siber uzayı en üst düzeyde domine eden devletlerden biri olduğu bilinmektedir (Darıcılı,2017:138).

2000'li yıllardan itibaren, etkin ve dominant uluslararası politika izleyen RF'nin, siber uzay alanlarında ki politikalarının başarılı olabilmesi için, savunma önlemlerinin sert ve dominant biçimde yürütmesi gerektiğini bilmektedir. RF'nin siber güvenlik politikalarını içeren bazı belgelerin ana başlıkları ise aşağıda belirtilmektedir;

- RF silahlı kuvvetlerinin, teknolojik altyapısını ve siber sistemlerini geliştirmek,
- Siber güvenlilikten sorumlu olan güçleri korumak ve askeri, siyasi alanlardan gelebilecek her türlü savaşa hazırlıklı olmak,
- Bağımsız Devletler Topluluğu (BDT) ve Şangay İşbirliği Örgütü (ŞİÖ) öncelikli olacak şekilde, Birleşmiş Milletler (BM) sözleşmesinin kanuni hükümlerine ve uluslararası hukuka uyarak, siber güvenliği güçlendirmek ve uluslararası düzeyde diğer unsurlarla beraber çalışabilmek,
- BM bünyesinde, uluslararası siber güvenlik anlaşmalarını sağlamak için çaba harcamak ve genel kabul görmüş normları, uluslararası hukukun ilkelerini, siber alana genişletecek anlaşmalar sağlamak,
- Siber alanda meydana gelebilecek çatışmaların erken tespitini sağlamak ve suç ortağı olanlara erken müdahale edebilmek,

- Çatışmanın nedenlerini belirleyerek, acil zamanlarda çatışmayı önlemek için bu sebepler üzerinde kontrol sağlamak,
- Olası bir çatışma sebebiyle doğabilecek mali problemlere karşı önlem almak,
- Birbiriyle çatışan taraflar arasında barışı sağlamak ve çatışmayı önleyebilmek,
- Herhangi bir çatışma olması halinde, kamuoyuna tarafsız bir şekilde açıklama yapmak,
- Kamuoyunun uygun yönlendirilmesini sağlamak ve saldırının diğer alanlara yayılmasını önlemek

RF'nin siber güvenlik stratejilerini askeri sistem üzerinden oluşturacağı, yukarıda ki ana başlıklarda görülebilmektedir. Öte yandan RF Genel Kurmay Başkanı General Valery Gerasimov 2013 yılında yayınladığı makalesi kapsamındaki tartışmalar ise bizce RF'nin siber güvenlik stratejisinin irdelenmesi amacı kapsamında önemlidir.

Gerasimov bu makalede teknoloji çağında ki savaşların nasıl olacağı, askerin bu yeni sisteme ne şekilde hazırlanacağı ve silahlanmanın nasıl olacağını tartışılmaktadır. Bu soruların genel olarak cevabı ise günümüzde savaşların seyrinin değiştiği, yapay zeka kullanılan modern silah ve ekipmanların ve Ar-Ge çalışmalarının büyük önem kazandığı, robot teknolojisinin savaşlarda aktif olarak rol alacağı belirtilmektedir (Gerasimov,2013).

Siber güvenliğe büyük önem veren RF, 29 Kasım 2013 tarihinde de yeni bir siber güvenlik stratejisi belgesi daha yayınlamıştır(www.council.gov.ru,2013). Genel olarak RF'nin bu belgede gündeme getirilen siber güvenlik yaklaşımları ise şöyledir;

- *Siber güvenlik stratejisinin geliştirilmesinin önemi*: İnternet ve siber uzayın bileşenleri, RF'nin ekonomik gelişiminde önemli bir etken oluşturmaktadır. Bu nedenle bilgi teknolojilerinin verimli kullanılabilmesi için, ulusal sektör geliştirilmelidir. Siber uzay, sınırsız alanı, yapısı ve teknolojiye bağlı olması sebebiyle, vatandaşlar için yeni fırsatlar doğururken siber saldırılar gibi tehditleri de bünyesinde oluşturmaktadır.
- *Bilgi güvenliğin yapısında siber güvenliğin yeri*: Siber uzay sonsuz ve sınırsız bilgi alanı olarak düşünülmektedir. Bu sebeple bilginin üretilmesi, başka bir forma dönüştürülmesi, platformlar yoluyla iletilmesi, kullanımı, depolanması ile ilgili faaliyet alanlarında, hem bireylere hem de devlete karşı meydana gelebilecek siber saldırılara karşı tüm bileşenlerin korunmasına büyük önem verilmektedir. RF

tanımlamalarında 'siber güvenlik' ve 'bilgi güvenliği' aynı kavram olarak gösterilmektedir.

- *Siber güvenliğin mevzuattaki yeri*: Siber güvenlik stratejileri, ülkede uygulanan genel yönetmeliklerle uyumludur. Başlıca önemli konuları güvenliğin sağlanabilmesi için var olan hukuksal boşlukları ortadan kaldırmak, sivil toplum kuruluşlarını, özel şirketleri ve diğer devletleri, siber güvenlik sürecine dâhil edebilmek, siber güvenlik mekanizmalarını geliştirerek, tüm bileşenlerin çalışmalarını sistematik ve fonksiyonel hale getirmek, tehditleri bertaraf edebilmek için gerekli tedbirleri üretmektir.
- *Siber güvenlik stratejisinin temel ilkeleri*: Bireyin, toplumun, özel şirketlerin anayasal hak ve özgürlüklerini güvence altına almak, devletlerin temel fonksiyonlarını, ileri düzey askeri altyapılarını ve sitemlerini korumak, toplumların, kamu çalışanlarının dijital okuryazarlık seviyesini yükselterek, teknoloji alanlarda bilinçlendirmek, siber uzaydan gelebilecek her türlü tehdide karşı risk analiz parametrelerini oluşturmak ve sürekli gelişen, değişen tehditlere karşı koyabilmek için, gerekli olan araçların yazılım ve donanımlarının güncellemesini sağlamaktır.
- *Siber güvenlik stratejisinin öncelikleri*: Tehdit ve saldırılara karşı milli koruma sisteminin geliştirilmesi ve teşvik edilmesi, ulusal bilgileri içeren platformların, güvenlik unsurlarının sürekli olarak yenilenmesi ve güncellenmesi, ülke halkının teknolojik kültür seviyesinin yükseltilmesi, global siber güvenlik seviyesini geliştirmek içi, diğer devletler ile anlaşmaların yapılması ve işbirliğin arttırılmasıdır.

5.3. Rusya Federasyonu Kaynaklı Olduğu İleri Sürülen Ve Rusya Federasyonu'nu Hedef Alan Siber Saldırılar

Siber uzayda meydana gelen tehditlere karşı, ülkeler şeffaflık ilkesini ön planda tutmalı ve buna göre davranmalıdırlar. Ancak devletler gücü elinde bulundurmak ve karşılarında ki devletleri domine edebilmek adına, siber uzayı askeri ve savaşmaya hazır bir platform haline dönüştürmektedirler. Siber uzay, bireylerden devlete, toplumlardan devlet dışı aktörlere kadar çok büyük bir alanı kapsamaktadır. Bu sebeple siber uzayı askeri bir savaş yapısına indirgemek çok yanlış olacaktır. Teknoloji ve enformasyonun

hızla yayıldığı şu zamanlarda, siber tehditlere karşı korunabilmenin çok zor olacağı da bilinmektedir.

RF, hem kendi verilerini koruyabilmek, hem de diğer ülkeler üzerinde egemenlik sağlayabilmek için siber uzay çalışmalarına öncelik vermektedir. RF'nin siber saldırgan grupları ve suç örgütleri ile bağlantılı saldırılar gerçekleştirdiği tahmin edilmektedir (www.siberbulten.com,2015). RF'ye yönelik olarak düzenlenen ve RF'nin gerçekleştirdiği iddia edilen bazı siber saldırılar aşağıda incelenmektedir;

Estonya Saldırısı: Estonya, interneti en fazla kullanan ülkelerden biri olduğu için e-stonya olarak anılmaktadır. Estonya yönetimine karşı, 2007 yılında bir siber saldırı yapılmıştır. Bu saldırının kimler tarafından yapıldığı halen bilinemezken, Estonya yönetimi saldırıdan RF'yi sorumlu tutmaktadır. Özellikle devlet kurumları ve özel şirketlerin web sitelerine düzenlenen bu kapsamında, Estonya NATO'dan sorumluların bulunabilmesi adına yardım talep etmiştir (BBC,2007).

Gürcistan Saldırısı: Gürcistan'ının hedef alındığı saldırılar, yapılış biçimi ve hedef aldığı kurumlar olarak Estonya saldırılarına çok benzerlik göstermektedir. İlk hedef olarak finans kuruluşları, devlet kurumları ve medyanın kilitlenmesi amaçlanmıştır (Darıcılı,2017:211). Bu saldırıların da RF tarafından yapıldığı bilinmektedir. RF, stopgeorgia.ru adlı site aracılığıyla birçok Rus hackeri bu saldırılara davet etmiştir (Çiftçi,2017:186). Rus istihbarat birimleri tarafından, saldırının yapıldığına dair pek çok kanıt olmasına rağmen, RF saldırıyla bir ilgisi olmadığını savunmuştur.

Kırgızistan Saldırısı: 2009 yılında, ABD'nin Kırgızistan'a üs kurma planlarını hayata geçirmiştir. Bu sırada Kırgızistan'a büyük bir siber saldırı gerçekleştirilmiştir. Kırgızistan internet sitelerinin %80'i kullanım dışı kalmıştır(www.kotuamacliyazilim.com,2016). RF, ülkede Amerikan üslerinin yapılmasına şiddetle karşı çıkmaktadır. Gürcistan ve Estonya' ya yapılan saldırılar gibi bu saldırılar da, DDoS atakları şeklinde planlanmıştır (Darıcılı,2017:9).

Litvanya Saldırısı: Litvanya'nın yaygın olarak kullandığı internet sitelerine, RF'nin orak ve çekiç simgelerini yerleştirerek yaptığı ileri sürülen ataklardır. Estonya, Gürcistan ve Kırgızistan'da olduğu gibi DDoS sistemi ile saldırılar gerçekleştirilmiştir (Darıcılı,2017). Litvanya Cumhurbaşkanı Alexander Lukashenko, eski Sovyet yönetimi ile ilgili bir takım iddialar ortaya atmıştır. İnsanlık dışı uygulamaların varlığıyla ilgili yapılan

açıklamalar, bu siber saldırının sebebi olarak görülmektedir (McLaughlin ,2008).Tüm bu veriler ışığında, Litvanya' ya karşı yapılmış olan siber saldırının da RF tarafından yapıldığı ifade edilmektedir. Litvanya'nın Kırım Tatarları üzerine, mecliste yaptığı görüşmelerden sonra, 2016 yılında yine bir saldırı dalgası daha yaşanmıştır (Euronews,2016). RF'nin Kırım ile tarihsel bağı düşünüldüğünde, bu saldırının yine RF tarafından yapıldığı değerlendirilebilecektir.

Ukrayna Saldırısı: RF'nin Kırım'da bazı bölgeleri işgal etmesinden sonra, Ukrayna devlet adamlarının cep telefonlarına yönelik gerçekleştirilen siber saldırıdır (Polityuk ve Finkle,2014). 23 Aralık 2015 tarihinde, Ukrayna'da 225 bin vatandaşın elektriği kesilmiştir (Volz,2016). Siber saldırganlar tarafından bilgisayarlara gönderilen virüsler ile geniş çaplı elektrik kesintileri yapılabileceği ilk kez uzmanlarca kabul görmüştür. Ukrayna Cumhurbaşkanı Yardımcısı, kendisiyle yapılan bir röportajda, Ukrayna'nın siber güvenlik politikalarını geliştirmek için çok çalıştığını, çünkü devamlı olarak RF tarafından siber saldırılara maruz bırakıldığını, bugüne kadar gerçekleşen siber saldırıların %99' nun RF tarafından yapıldığını belirtmiştir (Timtchenko,2017).

RF'ye yapılan siber saldırılar incelendiğinde ise ABD dışında siber saldırı gerçekleştiren devlet, birey ya da terör grubu ile karşılaşılmadığı görülmektedir. RF'nin ise genellikle, Türkiye'de dahil olmak üzere, çevresinde bulunan ülkelere siber saldırılar gerçekleştirdiği düşünülmektedir (Demirtepe,2008:32). RF, devletlerarası platformlarda siber suç işleyen ve siber suçluları destekleyen bir devlet olarak görülmektedir (www.kaspersky.com.tr,2018). Devletlerin öncelikli amacı, devletin varlığını, bütünlüğünü ve ulusal çıkarlarını korumak için güçlü olmaktır. RF tarafından gerçekleştirilen siber saldırılar incelendiğinde, bölgesindeki devletlerin siyasi kararlarını, kendi lehine çevirebilmek ve onları domine edebilmek adına bu saldırıları gerçekleştirdiği düşünülmektedir.

SONUÇ

Gelişmiş ülkelerin sanal dünyadan muhtemel saldırıları minimize edilmiş zararla çıkmak amacıyla siber güvenlik strateji belgeleri hazırlamaktadırlar. Bu belgeler kapsamında ise gerekli idari yapılanma oluşturarak, teknik personel temin ve savunma sistemleri kurmanın yöntemleri belirlenmektedir. Zira günümüzde siber güvenlik ulusal güvenlik politikaların ayrılmaz bir parçası haline gelmiştir. Askeri doktrinlerde ise siber uzay artık gelecek yıllarda kullanılacak olan bir çatışma alanı olarak tanımlanmaktadır.

Uluslararası sistem tarafından hava, deniz, kara ve uzay alanları belirli uluslararası politikalar çerçevesinde koruma altına alınmıştır. Siber uzayın ise anonimliği, karmaşıklığı ve insan eliyle oluşturulması bu alanlardan farklılaşmasına neden olmaktadır.

ABD, internetin yaygınlaşması ve hayatın her alanına nüfuz etmesiyle uyumlu olarak, siber uzayı stratejik hedef olarak görmektedir. ABD, ekonomik büyüme, küresel rekabetçilik ve toplumunun refahı için temel hizmetlerde kullanılmaya başlanan internetin güvenliğini sağlamayı temel hedef olarak belirlemiştir. Ayrıca ABD, siber güvenliği sağlamak adına öncelikle teknoloji sektörüne, kritik altyapılarına, savunma ve finansal hizmet sektörlerine odaklanmıştır. Özel şirketler, akademisyenler ve sivil toplum kuruluşları ile birlikte işbirliği sağlamakla, halkın siber güvenlik farkındalık seviyesini yükseğe çekmeye çalışmaktadır. ABD'nin siber uzayı ve interneti domine eden temel aktör konumu noktasında şüphe bulunmamaktadır. Bu liderlik konumu kapsamında ABD siber güvenliğini temin amacıyla geniş bir bütçe ayırmakta ve kaçınılmaz olduğunu düşündüğü siber savaşlara odaklanarak milyonlarca siber uzman yetiştirmeye gayret göstermektedir.

RF ise temel olarak bilgi güvenliğine odaklanmaktadır. 2000'li yılların başında bilgi güvenliği üzerine doktrin oluşturmak üzere güçlü bir yapı tesis etmeye başlamıştır. RF'nin bu kapsamda özellikle devletin çıkarlarına öncelik verdiği görülmektedir. Siber uzayı savaş alanı olarak tanımlamaktadır. Dolayısıyla siber uzayda egemen güç olabilmek için saldırgan bir strateji izlemektedir. RF'nin bu stratejileri dahilinde siber suç örgütleri ile işbirliği içerisinde bulunduğuna dair iddialar bulunmaktadır. Söz konusu illegal saldırılar sonrası RF'nin siber alanda düşman sayısı çoğalırken, ABD gibi öncü rakiplerin gelişmesi ise daha da ivme kazanmıştır. RF'nin siber uzayda zorlayıcı bir diplomasi içerisinde bulunarak özellikle yakın bölgesinde bulunan devletlere çok sayıda siber saldırılar gerçekleştirdiği iddia edilmiştir. RF'nin küresel anlamda güce sahip olmak adına istihbarat toplama alanında siber imkânlarını geliştirdiği ileri sürülmektedir. RF'de ABD gibi siber güvenlik alanında uzman personel yetiştirmeye gayret etmektedir.

Siber güvenlik ve siber uzay alanına ilişkin gelişmelerin ABD ve RF'nin izleyeceği politikalar dahilinde gelecekte şekilleneceği değerlendirilmektedir. Gelişen teknoloji ve dijital açıdan giderek sosyalleşen toplum için İnternet artık çok daha önem arz etmektedir. Bu kapsamda sadece RF ve ABD değil, uluslararası sistemdeki birçok devletin

de siber saldırı ve savunma kapasitelerini geliştirme noktasında ciddi gayretler içerisinde olacağı kesindir.

KAYNAKÇA

Atay,Ö.ve Hancıoğlu,Y.(2019). İngiltere, Amerika Birleşik Devletleri ve Türkiye'nin Ulusal İnavosyon Sistemlerinin İncelenmesi: Türkiye İçin Öneriler, Ankara Üniversitesi SBF Dergisi, 74(2)

Armaoğlu, F. (2014). 20. Yüzyıl Siyasi Tarihi 1914-1995. İstanbul:Timaş Yayınevi

BBCTurkısh.(2007).Estonya'ya Siber Saldırı. http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml (Erişim tarihi:01.04.2020)

BBC News.(2012). Profile: Garry Mckinnon, https://www.bbc.com/news/uk-19946902 (Erişim tarihi:19.03.2020)

Bıçakçı,S.(2013).21. Yüzyılda Siber Güvenlik. İstanbul: Bilgi Üniversitesi Yayınları

Bıçakcı,S.(2012).Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu,Uluslararası İlişkiler Dergisi, 9 (34) s. 207

Burke , P.(2013).Bilginin Tarihi Nedir?(Çev.T.Sivrikaya).İstanbul:Islık Yayınları

Bucci,S.(2012). Joining Cybercrime and Cyberterrorism A Likely Scenario, Cyberspace and National Security Threats, Opportunities and Power İn a Virtual World, der.

Derek S. Reveron, Washington: Georgetown University Press

Canbek,G.ve Sağıroğlu,Ş.(2006).Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Koruma Yöntemleri. Ankara: Canbek Yayınevi

Cirlig, C.C.(2014).Cyber defence in the EU Preparing for cyber warfare?, European

Parliamentry Research Service.https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf.(Erişim tarihi:28.03.2020)

Clarke,R.A.ve Knake, R.K.(2011).Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit.(Çev.M. Erduran).İstanbul: İKÜ Yayınevi

Concept Of A Cyber Securıty Strategy Russıan Federatıon.(2013). http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (Erişim tarihi:29.03.2020)

Çiftçi,H.(2017). Her Yönüyle Siber Savaş, Ankara: Tübitak Popüler Bilim Kitapları

Darıcılı,A.B.(2017). Rusya Federasyon'un Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi, Bilig, S.83

Darıcılı,A.B.(2018). Askerleştirilen ve Silahlandırılan Siber Uzay . Ankara: Nobel Yayınları

Darıcılı,A.B.(2017).Siber Uzay ve Siber Güvenlik Nedir?, Bursa :Dora Basımevi

Demirtepe,T.M.(2008). Orta Asya ve Kafkasya'da Güç Politikası.Ankara: Usak Yayınları

Euronews. (2016). Litvanya Meclisi'nin İnternet Sitesine Siber Saldırı.https://tr.euronews.com/2016/04/11/litvanya-meclisi-nin-internet-sitesine-siber-saldiri. (Erişim tarihi :01.04.2020)

Embel, E.(2016).Kronik: ABD Başkanlık Seçimleri. Ankara Üniversitesi Siyasi Bilimler Dergisi, 4(71), s.1319

Gelleman,B. ve Nakashima,E.(2001).The Washington Post, "U.S. spy agencies mounted 231 offensive cyber-operations in 2001 documents Show. https://www.washingtonpost.com/world/national-security (Erişim tarihi :19.03.2020)

Gerasimov,V.(2013). The Value Of Scıence In Predıctıon. https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf (Erişim tarihi:29.03.2020)

Gibson,W.(2012). Neuromancer.(Çev. G. Gülbay).İstanbul: Altıkırkbeş Yayıncılık

Güner,R.(2014).Joseph Nye ile Siber Güvenlik, Siber Güç ve Siberuzayın Geleceği Üzerine mülakat,https://www.academia.edu/37696368/Joseph_Nye (Erişim tarihi : 26.10.2019)

Gürkaynak M. ve İren,A.A.(2011).Reel Dünyada Sanal Açmaz: SiberAlanda Uluslararası İlişkiler, Süleyman Demirel Üniversitesi İktisadi ve İdariBilimler Fakültesi Dergisi,16 ,265

İnternet Lives, https://www.internetlivestats.com/ (Erişim tarihi :27.10.2019)

Kabay,M.E.(2005).Indurtrial Espionage, Part 8: Chine and Titan Rain.https://www.networkworld.com/article/2315467/industrial-espionage--part-8--china-and-titan-rain.html (Erişim tarihi :18.03.2020)

Kane,R.K.(2010).Internet Governance in an Age of Cyber Insecurity, E-kitap: Council Special Report No. 56

Kaspersky Team.(2018). Birçok Yanlışı Toplayınca Bir Gerçek Elde Etmezsiniz.2 Nisan 2020 tarihinde https://www.kaspersky.com.tr/blog/frequently-alleged-nonsense/4703/ (Erişim tarihi :02.04.2020)

Khuel,D.(2009).From Cyberspace to Cyberpower: Defining the Problem,Washington: National Defense Universıty Press

Keleştemur, A.(2015). Siber İstihbarat. İstanbul:Level Kitap

Karagül,S.Özkan,M.F.(2015).Bilgi Teknolojileri ve Uluslararası İlişkilerde Fırsat-Tehdit Paradoksu, Bilgi Ekonomisi ve Yönetimi Dergisi, 10(1)

Langer,R.(2016). Cyber Power - An Emerging Factor in National and International Security.https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue- no-8/cyber-power-an-emerging-factor-in-national-and-international-security (Erişim tarihi :27.10.2019)

Lin,H.S.(2010). Offensive Cyber Operations and the Use of Force, Journal of National Security Law and Policy, 4(63)

McLaughlin, D.(2008).Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites.https://www.irishtimes.com/news/lithuania-accuses-russian-hackers-of-cyber-assault-after-collapse-of-over-300-websites-1.942155. (Erişim tarihi :01.04.2020)

Milliyet Gazetesi İnternet Sitesi.(2003). Batman Barajı Şifrelendi.https://www.milliyet.com.tr/ekonomi/batman-baraji-sifrelendi-517687 (Erişim tarihi :02.02.2020)

Nye,J.(2003).Amerikan Gücünün Paradoksu,.(Çev: G. Koca). İstanbul: Literatür Yayınları.

Polityuk,P.ve Finkle,J.(2014). Ukraine Says Communications Hit, Mps Phones Blocked.https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304 (Erişim tarihi :01.04.2020)

Schmidt,N.(2014). Introduction to Security Studies, Bratislava: Cenaa,

Shactman,N.(2011).Exclusive: Computer Virus Hits U.S. Drone Fleet. https://www.wired.com/2011/10/virus-hits-drone-fleet/ (Erişim tarihi :19.03.2020)

Sheldon,J.(2012).Toward a Theory Of Cyber Power Strategic Purpose İn Peace and War, Cyberspace and National Security Threats, Opportunities and Power İn a Virtual

world, der. Derek S. Reveron, Washington: Georgetown University Press, 201

Slaughter,A.M.(2009).America's Edge: Power in the Networked Century. Foreign Affairs Dergisi, (01/02), 88-94

Smith,C.S.(2012).The First World Hacker War, https://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html,adresinden (Erişim tarihi :18.03.2020)

Siber Bülten. (2015). Rusya Siber Alanda Neden Saldırıyor?.https://siberbulten.com/uluslararasi-iliskiler/rusya-siber-alanda-neden-saldiriyor/ (Erişim tarihi :1.4.2020)

Siber Savaşlar: 5. Boyutta Savaş.(2016).https://www.kotuamacliyazilim.com/siber-savaslar-5-boyutta-savas/ (Erişim tarihi :01.04.2020)

Sönmezoğlu,F.ve Bayır,Ö.E.(2014). Dış Politika Karşılaştırmalı Bir Bakış. İstanbul: Der Yayınları

The Ministry of Foreign Affairs of the Russian Federation, Natıonal Securıty Concept Of TheRussıanFederatıon.(2000).https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768,(Erişim tarihi :26.03.2020)

The White House Executıve Orders (2015)Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. https://www.whitehouse.gov/ (Erişim tarihi :18.03.2020)

The New York Times.(2016).The Russian Hacking in 200 Words. https://www.nytimes.com/interactive/2016/12/29/us/politics/russian-hack-in-200-words.html (Erişim tarihi:19.03.2020)

Timtchenko,İ.(2017). Shymkiv: Ukrainians Not Prepared for Cyber Attacks. Kyiv Post .https://www.kyivpost.com/business/shymkiv-ukrainians-not-prepared-cyber-attacks.html (Erişim tarihi :02.04.2020)

Volz,D.(2016). U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage. Reuters.https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K, (Erişim tarihi :02.04.2020)

Yılmaz, S.(2012).ABD İstihbaratında Yaşanan Değişimler, Turan Stratejik Araştırmalar Merkezi Dergisi, 4(13)

Wedermye,L.J.(2012). The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict,Mıchgıan State Unıversıty College Of Law. https://digitalcommons.law.msu.edu/king/241/.(Erişim tarihi :25.03.2020)