Ulisa: Uluslararası Çalışmalar Dergisi
Ulisa: Journal of International Studies
AUİLS | 2017 Özel Sayısı - AUİLS | 2017 Special Issue

# Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi

Dr. Ali Burak DARICILI*

## ÖZ

Amerika Birleşik Devletleri (ABD) ve Rusya Federasyonu (RF), günümüzde siber uzayı domine eden en önemli küresel siber güçlerdir. İki devletin siber güçlerinin sistematiğine ve planlamasına yönelik detayların temelleri ise Soğuk Savaş döneminde ABD ve Sovyet Sosyalist Cumhuriyetleri Birliği (SSCB) arasındaki askeri rekabetin ortaya çıkardığı teknolojik yeniliklere dayanmaktadır.

1990'lı yıllar ile birlikte ağ teknolojilerinin hızla gelişmesi, ayrıca internetin sivilleşerek ticarileşmesi ve yaygınlaşmasının bir sonucu olarak, ABD ulusal ve uluslararası düzeyde siber güvenlik stratejilerini hızla geliştirmeye başlamış ve günümüzdeki güçlü siber kapasitesine ulaşmıştır. 2000'li yıllar sonrasında attığı adımlar ile birlikte RF'de, espiyonaj, kontr/espiyonaj, dezenformasyon, elektronik savaş kabiliyetleri, psikolojik savaş ve propaganda, siber saldırı gibi kabiliyetleri de kapsayan etkili bir siber kapasiteye sahip olabilmiştir.

Öte yandan iki devlet arasındaki siber mücadele ise RF'nin, Demokrat Parti Ulusal Komitesi bünyesinde görev alan bazı siyasilerin ve danışmanların e-postalarını siber saldırı yöntemleri ile temin ettiği ve bu e-postalardan bazılarını kamuoyuna sızdırdığı, böylelikle de aktif bir şekilde ABD seçim sürecini kendi ulusal çıkarları doğrultusunda diğer başkan adayı Donald Trump lehine manipüle ettiği iddiaları ile yeni bir boyuta taşınmıştır. Bu bağlamda çalışmamızda literatürde Demokrat Parti hack skandalı olarak tanımlanan olay; ABD ve RF'nin siber güvenlik stratejilerinin tarihsel gelişimi kapsamında taraflar arasında günümüze kadar meydana geldiği karşılıklı olarak iddia edilen siber saldırı vakaları çerçevesinde analiz edilecektir.

**Anahtar Kelimeler:** Amerika Birleşik Devletleri, Rusya Federasyonu, Siber Mücadele, Siber Güvenlik Stratejisi, Siber Saldırı.

* daricili@yahoo.com.

# Analysis of the USA and the RF's Cyber Strategies within the Context of Democratic Party Hacking Scandal


## ABSTRACT

The United States of America (USA) and the Russian Federation (RF) are the most important global cyber forces that dominate cyber space today. The details of the system and planning of the cyber powers of the two states are based on the technological innovations derived from the military competition between the US and the Union of Soviet Socialist Republics (USSR) during the Cold War.

As a result of the rapid development of networking technologies as well as the commercialization and widespread use of the internet by the 1990s, the USA has rapidly developed national and international cyber security strategies and has reached today's strong cyberspace capacity. In the years after 2000, RF was able to have an effective cyber capacity including espionage, counter/espionage, disinformation, electronic war capabilities, psychological warfare and propaganda and cyber attack.

The cyber struggle between the two states has been moved to a new dimension with assertions that e-mails of some of the politics and consultants involved in RF's National Committee for the Democratic Party were provided by cyber attack methods organized by RF and leaked some of these emails to the public, thus actively manipulating the US electoral process in favor of other presidential candidate Donald Trump in the direction of RF's national interests. In this context, the event defined as "Democratic Party hacking scandal" in the literature will be analyzed together with the mutually alleged cyber attacks happened between USA and RF within the context of the historical development of the cyber security strategies of two states in our study.


**Keywords:** The United States of America, The Russian Federation, Cyber Struggle, Cyber Security, Cyber Attack.

## Giriş

Siber uzay kavramının literatürde kabul görmüş bir tanımı bulunmamaktadır. Çoğunlukla interneti ifade etmek için kullanılan bir kavram olarak analizlerde sıklıkla ele alınmaktadır.[1] Gerçekte bu tabir bir bilim kurgu romanı ile oluşturulmuştur. Zira dünya'da en çok okunan bilim kurgu romanlarından biri olan Neuromancer'in yazarı William Gibson gerçeklikle hiçbir ilgisi olmayan bu kavramı, kendisi ile yapılan bir söyleşi de ilk defa kullanmıştır. Gibson'a göre siber uzay: *"milyarlarca meşru kullanıcı tarafından her gün tecrübe edilen uzlaşılmış bir halüsinasyon"* ve *"tasavvur edilemez karmaşa"* şeklindedir.[2] Bu etkileyici terim tanımı ne olursa olsun, günümüzde günlük hayattan, askeri ve ekonomik konulara kadar, ciddi ve derin anlamlara sahip bir biçimde karşımıza çıkmaktadır. Bize göre ise en kapsamlı ve doğru tanım; *"internet, iletişim ağları, dış dünyaya kapalı askeri ağlar, enerji hatları ağları, cep telefonları yazılım altyapılı telsizler, elektronik komuta sistemleri, cep teflonları, uydu sistemleri, insansız hava araçları sistemleri gibi birçok yazılım ve donanım elemanları toplamı*" şeklinde yapılabilecektir.[3]

Uluslararası ilişkiler açısından ise siber uzayı ABD ve RF'nin gerek yıllardan beri geliştirdikleri ağ teknolojileri ve bu teknolojileri kullanmak suretiyle askeri kapasitelerini ve espiyonaj imkanlarını maksimize etmek adına yaptıkları planlamaları gerekse de ülkelerinin siber güvenliklerini sağlamak adına ortaya koydukları strateji ve doktrinler çerçevesinde domine ettikleri görülmektedir. Bu çerçevede söz konusu etkileşimin ve etki-tepki ilişkisinin ortaya konması amacıyla çalışmamızda ilk olarak ABD'nin ve RF'nin siber güvenlik stratejilerini oluşturan enstrümanlar temel hatlarıyla değerlendirilecektir. Bu değerlendirme esnasında ise ABD'nin ve RF'nin siber güvenlik alanında ortaya koydukları önemli resmi stratejik belgeler ile söz konusu iki devletin siber kapasitesini kullanmada istifade ettikleri özel kuruluşlar ile askeri, güvenlik ve istihbarat örgütlenmeleri analiz edilecektir. Daha sonra literatürde **"**Demokrat Parti hack skandalı" olarak tanımlanan olay; ABD ve RF'nin siber güvenlik stratejilerinin tarihsel gelişimi kapsamında analiz edilecektir.

## ABD'nin Siber Güvenlik Stratejisini Oluşturan Enstrümanların Temelleri

ABD'nin siber gücünün evriminin başlangıcı tarihsel olarak 1930'lara dayandırılabilir. Bu kapsamda, ilk işlevsel bilgisayar örneklerinden biri olarak da görülebilecek olan ve Alman Donanması'nın 1920'lerde ilk örneğini ortaya koyduğu "ENİGMA" kripto cihazının muadili, ABD Donanması tarafından 1930'ların son yarısında "SIGIBA" adı altında üretilmiştir. Öte yandan İngiliz ve ABD'leri kökenli bilim insanlarının 2. Dünya Savaşı esnasında, "ENİGMA"cihazının gelişmiş bir versiyonunun şifresini çözmeye yönelik çabaları da ABD'nin bilgisayar yazılımı alanındaki ilk teknolojik tecrübeleri arasında önemli bir yere sahip olmuştur. 1940'ların sonu itibariyle ise ABD'de Atanasoff-Berry Computer Şirketi, ilk elektronik dijital bilgisayarı, ardından da AT&T2s Bell Labs Şirketi bilgisayarların gelişimi

[1] A. Burak Darıcılı, "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırılar", *Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Cilt 7, No 2, 2014, s. 2.
[2] William Gibson, *Neuromancer*, New York, Ace Books, 1984, s. 69.
[3] Uğur Akyazı, "Uluslararası Siber Güvenlik Stratejisi ve Doktrinler Arasında Alınabilecek Tedbirler", 6.Uluslararası Siber Güvenlik ve Kriptoloji Konferansı, http://www.iscturkey.org/s/2226/i/2013-paper105.pdf, (Erişim Tarihi 14 Nisan 2017).

açısından büyük öneme sahip ilk transistörü icat etmişlerdir.[4] 1950'ler ile birlikte International Business Machines (IBM) ilk yüksek seviye bilgisayar dili olan FORTRAN'ı geliştirmeyi başarmış, ayrıca söz konusu yıllarda ilk bilgisayar cipleri ABD'de kullanılmaya başlanmıştır.[5]

Bununla birlikte, ABD yönetimi SSCB ile bilimsel alanda rekabet edebilmek amacıyla Şubat 1958'de İleri Araştırma Projeleri Ajansı (Advanced Research Projects Agency / ARPA)'nı kurmuştur. ARPA'daki projelerin kapsamı ise uzay araştırmalarının yanı sıra balistik füze savunması, dünya üzerinde nükleer test yapılan coğrafi noktaların saptanması gibi konuları da kapsayacak biçimde düzenlenmiştir.[6] ARPA bünyesinde, proje kapsamında çalışma yürüten bilim insanlarını tek bir ağ altında toplanmasını sağlayabilecek bir teknolojinin geliştirilmesi ile birlikte, söz konusu proje internet tarihinin başlangıcını teşkil etmiştir. Bu kapsamda da ARPA projesi, ARPANET şeklinde isimlendirilmiştir.

Küba Krizi ile birlikte olası bir nükleer savaş halinde ARPANET'in bu saldırılardan etkilenmesi için ne tür önlemler alınması gerektiği şeklinde tartışmalar da yaşanmaya başlamıştır. Bu tartışmalar ise Paul Baran isimli bir bilim adamının fiziksel saldırı sonrasında kalan en büyük grupla elektrik bağlantısı sağlayarak iletişimi sürdürebilecek bir ağ yapının yaratılabileceğini ortaya koyması ile nihayetlenmiş ve farklı merkezlerde çalışan ağlar belirtilen yaklaşıma göre düzenlenmiştir. Akabinde söz konusu teknik altyapı ile birbirine bağlı olan ARPANET, ilk olarak İngiltere'deki Ulusal Fizik Laboratuvarı (National Physical Laboratory)'ndaki ticari ağ ve Fransa'daki araştırma ağı olan Cyclades ile birleştirilmiştir.[7] Böylelikle de internetin uluslararası boyutta ulaşan ilk çekirdek altyapısı oluşturulmuştur. İnternetin temelinin atılması sonrasında ise 1971 yılında *"creeper"* isimli ilk bilgisayar solucanı yazılımı tarafından ARPANET'in olumsuz bir şekilde etkilenmesi söz konusu olmuştur. Bu çerçevede anılan yazılım siber alandaki ilk olası tehdit emaresi olarak değerlendirilmiştir. Bahse konu gelişmelere rağmen sınırlı sayıda kullanıcı tarafından erişilebilen bilgisayar teknolojisi, 1970 yılında elektronik parçaları kendin yap projesi (DIY-Do it yourself), 1975 yılında kişisel bilgisayar olarak tanımlayabileceğimiz "Altair 8800"isimli bilgisayarların üretilmesi ve 1975 yılında piyasaya çıkan "IBM 5100"ler" ile birlikte, bir iletişim ve ağ kültürü olarak günlük hayatımızda yer edinmeye başlamıştır.[8]

Bu gelişmeler akabinde, internetin temel altyapısı olarak kabul edebileceğimiz, TELENET kamusal alanda servis vermeye başlamıştır. 1980'ler ile birlikte kişisel bilgisayar kullanımın artması ile birlikte ağlara katılımlar da artmaya başlamış ve sonuç olarak 1980 yılında ARPANET'e sızan bir virüs ile birlikte ARPANET'teki iletişim 72 saatliğine kesintiye uğramıştır.[9] Bu gelişmenin ardından ABD'de internet teknoloji ile birlikte gelişmekte olan ağ sistemlerinin güvenliği kavramı ilk defa tartışılmaya başlanmıştır. 1982 yılına gelindiğinde ise ARPANET'teki tehditlerin artması üzerine, ABD Savunma Bakanlığı gizli askeri verilerin

---

[4] *AFCEA Organization*, "The Evolution of US Cyberpower", http://www.afcea.org/committees/cyber/documents/TheEvolutionofUSCyberpower.pdf, (Erişim Tarihi 23 Nisan 2016), s. 7.

[5] Ian Chivers ve Jane Sleightholme, "Fortran History and Development", http://www.fortranplus.co.uk /resources/Fortran_history_and_development.pdf, (Erişim Tarihi 23 Nisan 2015), s. 5

[6] Salih Bıçakcı, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler*, Cilt 10, No 40, Kış 2014, s. 103.

[7] Salih Bıçakcı, *21. Yüzyılda Siber Güvenlik*, İstanbul, Bilgi Üniversitesi Yayınları, 2013, s. 6.

[8] A.g.e., s. 7.

[9] Janet Abbate, "Government, Business, and the Making of the Internet", *Business History Review*, Cilt 75, No 1, Bahar 2001, s. 164.

iletişimin sağlanacağı yeni bir altyapı oluşturulmasına karar vermiş ve ARPANET'e ilave olarak, Militarynet (MILNET) isimli bir altyapının oluşturulmasını tesis etmiştir.[10] Diğer yandan sanal dünyanın temelini atmış olan ARPANET, teknolojik yetersizlik nedeniyle yavaşlaması, ayrıca daha nitelikli bir altyapıya sahip Ulusal Bilim Vakfı Ağı (National Science Foundation Network / NSFNET) gibi ağların kurulması kapsamında, 1990 yılında kapatılmıştır.[11]

Tim Berners-Lee isimli bir fizikçi tarafından Avrupa Nükleer Araştırma Örgütü (European Organization for Nuclear Research / CERN )'nde çalışan bilim insanlarının farklı bilgisayarlardaki bilgiye kolayca erişebilmesi için geliştirdiği "world wide web (www)" formatı ile birlikte, internet üzerinden bilgisayarlar tarafından sunulan web sayfalarının oluşturulmasına ve ziyaret edilmesine imkân sağlanarak, internetin başta ABD olmak üzere, tüm dünya genelinde hızla gelişmesi mümkün olmuştur.[12] Bu gelişmenin bir uzantısı olarak da 15 Eylül 1997 tarihinde ise iki Stanford Üniversitesi öğrenci olan Larry Page ve Sergey Brin, ilk internet arama motoru olan Google.com'un tescilini yapmıştır.[13]

Belirtilen şekilde ağ teknolojilerinde meydana gelen yeni nesil gelişmeler ile birlikte ABD Ordusu tarafından bu teknolojiler ilk kez o güne kadar tecrübe edilemeyen bir kapasite ile 1990-1991 yılındaki 1. Körfez Savaşı esnasında kullanılmıştır. Bununla birlikte 1. Körfez Savaşı'ndaki sıcak çatışmaların dünya kamuoyuna adeta canlı olarak aktarılmasında, kitle iletişim araçlarının ortaya koyduğu imkân ve kabiliyetin anlaşılması noktasında büyük öneme sahip olmuştur. Bu kapsamda da ABD Hava Kuvvetleri bünyesinde Bilgi Savaşı Merkezi (Info War Center) isimli bir birim kurulmuş, 1995 yılında ise ABD Ulusal Savunma Üniversitesi siber savaşa komuta edecek olan ilk subaylarını mezun etmeye başlamıştır. Ayrıca konu kapsamında ABD Hükümeti tarafından, Uzay Komutanlığı (Space Command), "Stratejik Komutanlık (Strategic Command/ STRATCOM)'a dönüştürülmüş ve bu komutanlığa siber savaşa komuta etme yetkisi verilmiştir. Bu gelişmelerin devamında 2009 yılında STRATCOM'da, bir siber komutanlık kurulması emri verilmiş, 2010 yılında ise müstakil bir Siber Komutanlık (Cyber Command / CYBERCOM) tesis edilmiştir.[14]

## ABD'nin Siber Güvenlik Stratejisi ile İlgili Resmi Dokümanlar

1990'lı yıllar ile birlikte, ABD yönetimlerinin kendi ülkesinde yaşanmakta olan siber uzay teknolojileri alanındaki gelişmeleri, askeri kapasitesini geliştirme yönünde bir fırsat olarak okuduğu ve bu konuda kurumsal altyapılar oluşturma sürecine bu yıllarda ciddi hız verdiği görülmektedir. Bu noktada ABD'nin siber güvenlik stratejisini belirleyen temel belgelerin, RF'de analiz edilen süreçlerin aksine, sadece ilgili ABD kurumlar tarafından yayımlanmış olan strateji belgeleri, askeri ve güvenlik doktrinlerinden ibaret olmadığı da ifade edilmelidir. Zira federal sisteminin bir sonucu olarak, ABD'nin siber güvenlik stratejisinin şekillenmesinde, ABD başkanlık direktifleri; ilgi kurumların kendi güvenlik alanlarına yönelik olarak ortaya koydukları stratejiler ve eyalet bazında yapılan siber stratejik planlamalar da ciddi önem sahiptir.

[10] Bıçakcı, "NATO'nun Gelişen Tehdit …", a.g.e., s. 107.
[11] Bıçakcı, "21. Yüzyılda Siber…", a.g.e., s. 25.
[12] A.g.e., s. 26.
[13] *AFCEA Organization*, a.g.e., s. 10.
[14] Ayrıntılı bilgi için bkz. Mehmet Yayla, "Hukuki Bir Terim Olarak Siber Savaş", http://portal.ubap.org.tr/App_Themes/ Dergi/2013-104-1247.pdf, (Erişim Tarihi 17 Şubat 2017), s. 186-187.

Söz konusu direktiflerden ilki olan ve Temmuz 1995'de yayımlanan *"13010 No'lu Başkanlık Direktifi (Presidential Directive-13010)*'nin ABD'nin siber güvenlik alanındaki gelişmelere doğrudan vurgu yapan ilk resmi belge olması bakımından önemi büyüktür.[15] Bu belgenin önemli bir bölümü gizli niteliği haiz olmakla birlikte, anılan belgede dönemin ABD Başkanı Bill Clinton, başsavcılık makamını ülkenin kritik altyapılarına yönelik olası bir siber saldırıya karşı hazırlık durumunu araştıran bir çalışma yapması konusunda görevlendirmiştir.[16]

Mayıs 1997 tarihinde yayımlanan "*63 Nolu Başkanlık Direktifi (Presidential Directive-63)"* ise ABD'nin kritik altyapılarını tanımlayan ilk resmi dokümandır. Bu belgeye göre ABD kritik altyapıları; *"enformasyon, iletişim, enerji, bankacılık ve finans, ulaşım sektörleri ile içme suyu ve acil müdahale altyapısı (911) ve kamu sağlığı alanı"* şeklindedir.[17]Ayrıca bu direktif, gelecek dönemde ABD resmi kurumları tarafından hazırlanacak olan stratejik belge, planlama ve doktrinlere kaynaklık teşkil etmiş olması bakımından da öneme sahiptir.[18]

*"The National Strategy to Secure Cyberspace / Siber Uzay'ın Korunmasına Yönelik Ulusal Strateji"* belgesi, Şubat 2003'de yayımlanmıştır. Bu belge, ABD'nin siber uzay alanını tanımlayan, bu alandaki hedef ve planlamalarını ortaya koyan, ulusal siber uzayın nasıl korunacağına dair planlanan sistemi belirleyen, siber uzay kaynaklı tehditleri tarif eden ilk geniş kapsamlı dokümandır. Bu belgede, 2003 stratejisinin amaçları: *"ABD kritik altyapısını siber ataklara karşı korumak, ABD siber savunma sistemindeki açıkları tespit etmek ve gidermek, olası saldırılar karşısında uğranılabilecek zararı minimize etmek"* şeklinde ifade edilmiştir.[19]

*"Cyberspace Policy Review / Siber Uzay Politika Revizyonu"*, Başkan Obama'nın talimatıyla 2009 yılında hazırlanmış olan bir belge niteliğindedir. Bu belgede temel olarak, ABD siber savunma sisteminde görev alan resmi kurum ve kuruluşların, federal ve yerel düzeyde çok başlı yapısına eleştiride bulunularak, bu durumun giderilmesi için bazı tedbirlerin alınması gerektiği ve ulusal siber güvenlik sistematiğinin ancak bu kuruluşların birlikte ve eşgüdüm halinde hareket etmesi ile etkili olabileceği belirtilmektedir.

"*International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World / Siber Uzay İçin Uluslararası Strateji: Ağlanmış Bir Dünya'da Refah, Güvenlik ve Açıklık"* isimli doküman, dönemin ABD Başkan Obama'nın talimatıyla Mayıs 2011'de ABD ve dünya kamuoyuna ilan edilmiş olan ve ABD'nin uluslararası düzeyde ülkenin siber uzay alanındaki amaç ve hedeflerini ortaya koyan bir siber güvenlik strateji belgesidir.

Şubat 2015 tarihli *"National Security Strategy / Ulusal Güvenlik Stratejisi"* genel olarak ABD'nin gelecek dönem tehdit algılamaları ile güvenlik stratejisi kapsamında alacağı tedbirler hakkında bilgiler sunmakla birlikte, belgenin birçok bölümünde siber güvenlik kavramına ilişkin

---

[15] K. William Tirrell, *United States Cyber Security Strategy, Policy and Organization: Poorly Postured to Cope With a Post-9/11 Security Environment*, Master Thesis, Washington University, 2012, https://www.hsdl.org/?view&did=729810, (Erişim Tarihi 10 Şubat 2017), s. 20. Ayrıntılı bilgi için bkz. https://www.federalregister.gov/executive-orders/william-j-clinton/1997, (Erişim Tarihi 15 Ocak 2017).

[16] Ayrıntılı bilgi için bkz. "Presidency Of USA, Executive Order 13010—Critical InfrastructureProtection", http://www.presidency.ucsb.edu/ws/?pid=53066, (Erişim Tarihi 17 Şubat 2017).

[17] "White House, Presidential Decision Directive (PDD)-63, Critical Infrastructure Protection", http://fas.org/irp/offdocs/pdd/pdd-63.htm, (Erişim Tarihi 24 Mayıs 2016).

[18] Tirrell, a.g.e., s. 24.

[19] Ayrıntılı bilgi için bkz. https://www.us cert.gov/sites/default/ files/publications/ cyberspace _strategy .pdf, (Erişim Tarihi 16 Ocak 2017).

değerlendirme ve öneriler de mevcuttur. Bu değerlendirme ve öneriler ise özetle:[20] RF'nin artan siber gücünün ve siber meydan okumalarının ABD'nin güvenliği için ciddi tehdit oluşturduğu, Çin Halk Cumhuriyeti (ÇHC)'nin özellikle siber casusluk faaliyetleri noktasında ABD için tehdit yarattığı, bu nedenle de ABD'nin teknolojik yeniliklerini ve özel sektörünün ticari çıkarlarını korumak için gerekli tedbirleri alacağı, ABD'nin müttefik ülkelerin istikrarını bozmayı hedefleyen siber saldırılara karşı, ilgili ülkelere tam destek vereceği hususları belirtilmektedir.

Bahse konu değerlendirme ve öneriler arasında, ABD'nin RF'nin ve ÇHC'nin siber tehdit yaratma kapasitesine yaptığı vurgu, ABD'nin gelecek dönem siber güvenlik stratejisinin şekillenmesi bakımından oldukça önemli görülmelidir. Bu noktada ilgili belgede, ABD, ÇHC'yi dar bir kapsamda siber casusluk açısından hedef göstermekte, RF'yi ise çok daha geniş bir değerlendirme ile birlikte ülkesi için açık bir siber tehdit olarak kabul etmektedir. Bu itibarla da söz konusu belgede yer alan *"Rusya'nın artan siber gücünün ve siber meydan okumalarının ABD'nin güvenliği karşısında ciddi tehdit oluşturduğu*" ve Rusya'nın komşusu ülkelere yönelik olarak yaptığı siber saldırıları da işaret edecek şekilde, *"ABD'nin müttefik ülkelerin istikrarını bozmayı hedefleyen siber saldırlara karşı, ilgili ülkelere her türlü desteği vereceği*", ifadelerinin dikkat çekici olduğu belirtilmelidir.[21]

*"The Department of Defence Cyber Strategy / ABD Savunma Bakanlığı Siber Strateji*" isimli belge, 23 Nisan 2015 tarihinde kabul edilmiştir. Söz konusu belge ile ABD Silahlı Kuvvetleri'ne, ABD ağ teknoloji ve sistemleri ile gizli siber bilgilerini savunma, siber ataklara karşı ABD çıkarlarını koruma, askeri ve gizli siber operasyonları planlama ve bu tür operasyonlara rehberlik etme, görevleri verilmiştir.[22] Bu belgenin kabul edilmiş olması, ABD'nin operasyonel bir siber güç olma yönündeki iradesini dünya kamuoyuna ilan etmesi bakımından oldukça önemlidir. Bu nedenle de bahse konu stratejinin geniş bir perspektif ile hazırlandığı ileri sürülebilir. Zira söz konusu strateji belgesinde, RF ve ÇHC'nin oldukça ileri bir siber kapasite ve strateji geliştirmiş oldukları vurgulanmaktadır. Bu kapsamda, RF'nin siber gücü: *"tespiti ve deşifresi oldukça zor"* şeklinde bir ifade ile tanımlanmaktadır.

## ABD'nin Siber Güvenlik Alanında Faaliyet Gösteren Resmi Kurum ve Kuruluşları

ABD'nin resmi siber organizasyonu oldukça karmaşık bir yapıya sahiptir. Daha önce belirtildiği üzere bu karmaşık yapı ABD'nin federatif yönetim anlayışı ile şekillenen adem-i merkeziyetçi idare şekliyle doğrudan ilintilidir. ABD'nin resmi siber organizasyonu temelde: "ABD Savunma Bakanlığı (United States Department of Defense), ABD İç Güvenlik Bakanlığı (The Department of Homeland Security) ve ABD Gizli Servisleri (FBI / CIA)" şeklinde üçlü bir yapıya sahiptir. Bunun dışında, bazı resmi kurumların kendi görev sahalarına yönelik olarak yetki ve sorumlulukları da bulunmaktadır. Ayrıca, eyalet yönetimleri, ulusal siber güvenlik ağı haricinde,

[20] Ayrıntılı bilgi için bkz. "NATO Cooperative Cyber Defense Centre of Excellence, National Security Strategy", https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf, (Erişim Tarihi 25 Mayıs 2016).
[21] A.g.e.
[22] The Department of Defence Cyber Strategy, "NATO Cooperative Cyber Defense Centre of Excellence", http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, (Erişim Tarihi 25 Mayıs 2016). Ayrıntılı bilgi için bkz. http://www.dtic.mil/doctrine/doctrine/other/dod _cyber_ 2015.pdf, (Erişim Tarihi 15 Nisan 2017).

kendi siber güvenliklerini sağlamak amacıyla çeşitli yapılanmalar da kurarak, bu yapılardan aktif olarak istifade etmeyi de tercih etmektedirler.[23]

Bu kapsamda ABD Savunma Bakanlığı, ABD Silahlı Kuvvetleri'nden sorumlu olan bakanlıktır. 18 Eylül 1947 tarihinde oluşturulmuştur ve karargâhı ABD'nin başkenti Washington DC'de bulunan Pentagon'dur.[24] Savunma Bakanlığı, ABD'nin siber güvenlik stratejisinin uygulanmasında etkin bir role sahiptir. Savunma Bakanlığı bünyesinde siber güvenlik alanında en etkili rolü, STRATCOM bünyesinde faaliyet gösteren ve 2010 yılında kurulan CYBERCOM üstlenmektedir.[25] CYBERCOM, mevcut siber kaynaklarını düzenler ve ABD askeri bilgisayar ağları müdafaasını eşzamanlı bir hale getirir. Bünyesinde: *"24. Hava Kuvvetleri, Ordu Siber Savaş Birimi, Donanma Siber Savaş Birimi, Deniz Kuvvetleri Siber Savaş Birimi*"[26] şeklinde yapılanmalar mevcuttur.

ABD Savunma Bakanlığı bünyesinde siber güvenlik alanında faaliyet gösteren bir diğer kuruluş ise adı "Edward Snowden Olayı" kapsamında dünya kamuoyunda oldukça sık gündeme gelen Ulusal Güvenlik Ajansı (National Security Agency / NSA)'dır. NSA, 04 Kasım 1952 tarihinde kurulmuştur. NSA, ABD'nin küresel izleme, şifre çözme, veri toplama, veri analizi, sinyal toplama, çeviri ve yabancı istihbaratlara karşı istihbarat yapma amaçları için tesis ettiği istihbarat kuruluşu ve örgütüdür. NSA, ABD'nin ağ savaşları kapsamındaki haberleşme ve bilgi veri sistemlerinin korunmasından da sorumludur.[27]

Söz konusu kuruluşların yanı sıra, Savunma Bakanlığı bünyesindeki Kara, Deniz ve Hava Kuvvetleri Daireleri'nde her biri kendi görev ve sorumluluk alanı ile ilgili olarak faaliyet ve eşgüdüm görevi ifa eden birer Birleşik Siber Merkezi (Joint Cyber Center/ JCC) isimli organizasyonları da mevcuttur.[28]

ABD İç Güvenlik Bakanlığı (United States Department of Homeland Security / DHS), 11 Eylül 2001 saldırılarından sonra kurulan ve ülkede terörle mücadele konusunda asıl görevli olan devlet kurumudur. ABD Kongresi tarafından 2002 yılında çıkartılan "Kamu Güvenlik Yasası" ile kurulmuştur. Bu kanun, ABD İç Güvenlik Bakanlığı'nın da kurucu belgesidir.[29] ABD İç Güvenlik Bakanı (The Secretary), Bakanlığın başı olup (Head Of Department), Bakanlık üzerinde yönetim, yetki ve denetim gücünü elinde bulundurmaktadır. Bakanlığın bütün örgütsel birimlerinin, yöneticilerinin ve çalışanlarının, bütün işlevleri Bakan'ın himayesindedir.

ABD İç Güvenlik Bakanlığı'nın siber güvenlik alanındaki amaçları ise: *"kritik altyapıları korumak, kritik öneme haiz altyapı yatırımlarını ve hayati öneme haiz kaynaklarının direncini güçlendirmek, hükümetin iletişimini ve operasyonel gücünün devamlılığının sağlamak, ulusal siber güvenlik şartlarını ilerletmek"* olarak belirlenmiştir.[30]

---

[23] Tirrell, a.g.e., s.55.
[24] United States Department of Defense, "About the Department of Defense (DoD)", http://www. defense. gov/About-DoD, (Erişim Tarihi 30 Mayıs 2016).
[25] Yayla, a.g.e., s. 186.
[26] Tirrell,a.g.e., s. 57.
[27] National Security Agency, "60 Years of Defending Our Nation", http://www.nsa.gov/public _info/_files/cryptologic_histories/origins_of_nsa.pdf, (Erişim Tarihi 30 Mayıs 2016).
[28] Tirrell, a.g.e., s. 57.
[29] Şafak Başa, "ABD İç Güvenlik Bakanlığı", https://www.academia.edu /9830086/ ABD_%C4% B0%C3 %87_G%C3%9CVENL%C4%B0K_BAKANLI%C4%9EI_SUNUM_, (Erişim Tarihi 31 Nisan 2017).
[30] A.g.e.

ABD İç Güvenlik Bakanlığı organizasyon şeması ele alındığında, ülke genelinde 7/24 esasına göre bir füzyon merkezi olarak görev ifa eden Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (National Cybersecurity and Communications Integration Center / NICIC)'nin siber güvenlik alanındaki temel sorumlu birim olduğu görülmektedir. Bu merkez federal, eyalet ve diğer yerel birimler nezdinde ülke genelinde meydana gelen siber olayları izleyerek, bu olaylara anında cevap vermekten sorumludur. Ayrıca NICIC görevi kapsamında, ilgili güvenlik ve istihbarat birimleri ile özel sektör arasında eşgüdüm ve uyumu tesis eder.[31]

ABD İç Güvenlik Bakanlığı bünyesinde siber güvenlik alanında görev yürüten diğer birimler ise Bilgisayar Acil Müdahale Hazır Ekibi (Computer Emergency Readiness Team / US-CERT) ve Sanayi Kontrol Sistemleri Bilgisayar Acil Müdahale Hazır Ekibi (Industrial Control System Computer Readiness Team / ICS-CERT)'dir. Bu takımlar ve servisler 7/24 esasına göre, ülke genelindeki siber saldırıları takip eden operasyonel birimler şeklinde organize edilmiştir ve görevleri ile ilgili olarak "Ulusal Siber Güvenlik Birimi (National Cyber Security Division/ NCSD)'ne karşı sorumludur. Ayrıca ABD İç Güvenlik Bakanlığı bünyesinde "Gelişmiş Siber Güvenlik Servisleri (Enhanced Cybersecurity Services / ECS) şeklinde örgütlenmiş birimler de bulunmaktadır ve bu birimler siber güvenlik alanında özel sektör ile bilgi paylaşımı süreçlerini koordine etmekten sorumlu olacak şekilde planlanmışlardır.[32]

ABD İç Güvenlik Bakanlığı, ABD siber savunma planlamasının şekillenmesinde, önemli bir eşgüdüm merkezi olarak da görev yapar. Bu itibarla ABD İç Güvenlik Bakanlığı, istihbarat ve güvenlik servisleri ile gelecek dönemde meydana gelmesi muhtemel siber saldırıların mahiyeti, kaynağı ve organizasyonu ile ilgili duyumlarını paylaşmak, ABD Savunma Bakanlığı ile ülkenin ulusal siber güvenlik savunma sistematiğini geliştirmek, ABD Adalet Bakanlığı (United States Department of Justice) ile ABD'ye yönelik siber saldırıların faillerinin tespiti ve yargılanması sürecinde hukuki destek sağlamak ile sorumludur.[33]

ABD İç Güvenlik Bakanlığı'nın ülke genelinde siber güvenliğin sağlanması amacına yönelik olarak etkin bir şekilde kullandığı sistemin adı ise Ulusal Siber Güvenlik Koruma Sistemi (National Cybersecurity Protection System/ NCPS)'dir.[34] NCPS, bir zorlama uygulama olarak, federal ağ sistemindeki siber saldırıları tespit ederek, etkisizleştirmek amacıyla sistemin partnerlerine NICIC ve NCSD uzmanları ile bilgi paylaşımı ve koordinasyon noktasında kanuni sorumluluklar yüklemektedir. NCPS'nin etkinleştirilmesini sağlamak amacıyla da "EINSTEIN" adı verilen bir yazılım kullanılmaktadır ve bu yazılım eksikleri ortaya çıkan yeni durumlar kapsamında sürekli olarak teste tabi tutulmaktadır. Böylelikle de bu yazılımın her seferinde daha sıkı kontrol unsurları getiren ve yenilenen üç yeni versiyonu bugüne kadar geliştirilmiştir.[35]

---

[31] Tirrell, a.g.e., s. 58.

[32] A.g.e., s. 60.

[33] Department of Homeland Security, National Cybersecurity and Communications Integration Center, https://www.isaca.org/chapters2/New-York-Metropolitan/membership/Documents/2012-04-30%20Spring%20Conference-Meeting/2%20Lichtenfels%20DHS%20NCCIC%202.pdf, (Erişim Tarihi 31 Mayıs 2016).

[34] Ayrıntılı bilgi için bkz. Committee on Homeland Security and Governmental Affairs, A Review of the Department of Homeland Security's Missions and Performance, file:///C:/Users/tk44655/Downloads /Senator%20Coburn%20DHS%20Report%20FINAL%20(3).pdf (yerel bilgisayardan kaynak gösterilmez), (Erişim Tarihi 31 Mayıs 2016), s . 82-85.

[35] Ayrıntılı bilgi için bkz. A.g.e.., s . 85-87.

ABD istihbarat topluluğu ise bünyesinde çeşitli örgütlenmeleri barındıran bir yapı olup, bu örgütlenmeler arasındaki koordinasyon ise Ulusal istihbarat Direktörü / Director of National Intelligence (DNI) tarafından sağlanmaktadır. Bu kapsamda DNI'ya bağlı 17 ajans ve örgüt bulunmaktadır.[36] Söz konusu örgütlerin siber güvenlik alanına ilişkin faaliyetleri ile ilgili koordinasyonu da DNI'nın görevleri arasında yer almaktadır.

Bu örgütlenmelerin en önemlileri arasında yer alan Federal Araştırma Bürosu (The Federal Bureau of Investigation / FBI), ABD'nin iç istihbarat ihtiyaçlarını karşılayan ve diğer devletlerin ABD'ye yönelik casusluk operasyonları ile subversif (yıkıcı) faaliyetlerine karşı koyan istihbarat organizasyonudur. FBI'ın ABD'nin siber güvenlik stratejisinin uygulanmasında, siber suçlulardan, devlet destekli unsurlardan ve terörist gruplardan kaynaklanan siber ataklara karşı koyma görev ve yetkisi kapsamında önemli rolü bulunmaktadır. Bu çerçevede, FBI siber güvenlik ile ilgili yetki ve sorumluluklarını sürdürmek amacıyla, Siber Ulusal Güvenlik Bölümü (Cyber National Security Section / CNSS) ve Siber Suç Bölümü (Cyber Criminal Section / CCS) şeklinde örgütlenmeler tesis etmiştir. Bu örgütlemelerden CNSS, terörist gruplardan ve hasım devletlerden kaynaklanan siber saldırıları takip etmek, izlemek ve deşifre etmekten sorumluyken, CCS ise adı suç kapsamında olan, ancak federal güvenliği tehlikeye düşüren siber suçlar ile mücadele etmektedir.[37] CCS ve CNSS'nin, söz konusu görevleri kapsamında diğer hükümet kurumları ile olan koordinasyonu ise Ulusal Siber Araştırma Birleşik Görev Gücü (National Cyber Investigative Joint Task Force / NCIJTF)" aracılığıyla sağlanır. CNSS direktörü ise aynı zamanda NCIJTF'nin de başkanıdır ve siber güvenlik faaliyetlerinden sorumlu FBI direktör Yardımcısı'nın emrinde çalışır.[38]

## RF'nin Siber Güvenlik Stratejisini Oluşturan Enstrümanların Temelleri

RF, siber güç olarak günümüzde siber uzayı domine eden en önemli devletlerden biri konumundadır. RF, internetin genişleyip yayılmaya ve günlük hayatımızın hemen her alanını etkilemeye başladığı 2000'li yılların başından itibaren, siber uzay olarak adlandırılan alanda etkinlik sağlamak amacıyla planlama ve stratejiler geliştirmektedir. Tarihsel olarak SSCB döneminden günümüze kadar ulaşan stratejik ve teknolojik aklın da etkisiyle, RF'nu siber kapasitesini saldırı ve savunma yönünde genişletme eğilimindedir. Örneğin, SSCB döneminde, Komitet Gosudarstvennoy Bezopasnosti (KGB)'nin dış operasyonlarının önemli bir bölümünün, Batı bloğundaki teknolojik gelişmeleri yakından takip ederek teknolojik casusluk yoluyla bu buluşları SSCB'ye aktardığı bilinmektedir.

Bu geleneksel yöntem, Soğuk Savaş dönemi sonrasında da Rus İstihbarat Servisleri (RİS)'nin dış operasyonlarında belirleyici bir etken olmuştur.[39] Diğer yandan SSCB Ordusu'nda teknolojik gelişmeleri askeri doktrinlere adapte eden fikirlerin daima teşvik edildiği, söz konusu

[36] NATO Cooperative Cyber Defense Centre of Excellence, National Cyber Security Organisation in United States, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf, (Erişim Tarihi 01 Haziran 2019), s. 23.

[37] Ayrıntılı bilgi için bkz. Tirrell, a.g.e., s . 60-62.

[38] Ayrıntılı bilgi için bkz. Federal Bureau of Investigation, Cyber Crime, https://www.fbi.gov/about-us/investigate/cyber/ncijtf, (01 Haziran 2017).

[39] J. James Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy", NATO CCD COE Publications, Tallinn 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf, (Erişim Tarihi 05 Mart 2016), s. 30.

geleneğin ise günümüz RF Silahlı Kuvvetleri (RSK)'nde de devam ettiği genel kabul görmüştür. Böyle bir uygulamanın neticesi olarak, 1920'li yıllarda Sovyet yazarları tarafından uzayda savaş uçaklarının it dalaşı yapabileceği fikirlerinin ortaya konduğu da bilinmektedir.[40] Diğer yandan 1920'ler için bir hayal olan bahse konu fikirlerin, 1980'lerin başı ile birlikte ABD'nin "Yıldız Savaşları Projesi" ile gerçeğe dönüştüğü de görülecektir.

1980'lerde Sovyet Ordusu'nda üst düzey görev yapan Mareşal Nikolai Orgakov tarafından başlatılan Revoluation in Military Affairs (RMA) Programı, günümüz Rus Siber Stratejisi'nin temeli olarak kabul edilebilir.[41] Orgakov, bu program ile birlikte kitlesel ve hantal bir yapıya sahip Sovyet Silahlı Kuvvetleri'ni ağ teknolojileri ve teknik operasyonlar ile takviye edilen ve yönetilen, daha etkin bir yapılanmaya kavuşturmayı hedeflemiştir. Orgakov'un bu misyonu ile birlikte, 1980'ler boyunca kimi Sovyet askeri stratejistleri, enformasyon teknolojilerindeki önemli gelişmelerin orduların kapasitelerinin artırılması noktasında kullanılabileceğini değerlendirmişlerdir.

1979-1989 arasında devam eden Afganistan Savaşı esnasında, Sovyet Ordusu'nun psikolojik savaş tekniklerini uygulamada ve Afganistan'daki saha birlikler ile Moskova Riyaseti arasında etkili bir iletişim sağlama noktasında yeterince başarılı olamadığı ortadadır.[42] Benzer şekilde 1994-1996 yıllarındaki Çeçen Savaşı sırasında, internet haberleşmesi ve internet haberleşmesinin ortaya koyduğu imkânlar, savaş esnasındaki olayların RF aleyhine yansıtılması kapsamında oldukça başarılı olmuştur.[43] Bu kapsamda RF, uluslararası kamuoyu nezdinde Çeçen Savaşı'nda insanlık dışı yöntemlere başvuran, savaş suçu işleyen bir devlet olarak kabul edilmiştir.[44] Söz konusu iki olayın olumsuz etkisiyle, Rus güvenlik ve askeri bürokrasisinin "*askeri ağ teknolojileri*" ve "*enformasyon savaşı*" alanındaki planlamaları ve hazırlıkları hızla gelişmeye başlamıştır. Bu planlamanın bir sonucu olarak, NATO güçlerinin 1999 yılında eski Yugoslavya'daki Sırp güçlerini bombalamaya başlaması ile birlikte, Sırp ve Rus hackerlar tarafından NATO'ya, üye ülkelerin askeri haberleşme sistemlerine, ABD Savunma Bakanlığı'nın alt yapılarına siber saldırılar gerçekleştirilmiştir.[45]

## RF'nin Siber Güvenlik Stratejisi ile İlgili Resmi Dokümanlar

Siber uzay ve siber güvenlik ile ilgili analizlerin uluslararası literatürde yoğun olarak tartışılmaya başlandığı 2000'li yıllar ile birlikte, RF'nin "*bilgi güvenliği*" kelimesinin ilk kez kullanıldığı resmi belgesi, 24 Ocak 2000 tarihinde yürürlüğe giren "*National Security Concept of Russian Federation / RF Ulusal Güvenlik Konsepti"* isimli dokümandır. Bahse konu belge temel

[40] Ayrıntılı bilgi için bkz. A.g.e., s. 33-34.
[41] Ayrıntılı bilgi için bkz. Matthew Mowthorpe, "The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views", file:///C:/Users/tk44655/Downloads/2011.06.02-Maturing-Revolution-In-Military-Affairs1.pdf (yerel bilgisayardan kaynak gösterilmez), (Erişim Tarihi 05 Mart 2017), s. 1-5.
[42] A. Burak Darıcılı ve Barış Özdal, "Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi", *Gelişim Üniversitesi Sosyal Bilimler Dergisi*, Cilt 4, No 1, 2017, s. 20.
[43] Bıçakcı, "21. Yüzyılda Siber …", a.g.e, s. 30.
[44] Roland Heickerö, Emerging Cyber Threats and Russian Views on Information Warfare and Operation, Swedish Defense Research Agency Press, Mart 2010, http://www.foi.se/rapport?rNo=FOI-R--2970--SE, (Erişim Tarihi 23 Haziran 2016), s. 5.
[45] Bıçakcı, "21. Yüzyılda Siber …", a.g.e.

olarak, enformasyon güvenliğinin öneminden, bu alanda Rus çıkarlarına yönelik iç ve dış tehditlerin varlığından ve bu tehditlere yönelik tedbirler alınmasından bahsetmektedir.

9 Eylül 2000 tarihli *"Information Security Doctrine of the Russian Federation / RF Enformasyon Güvenliği Doktrini"*, RF'nin siber güç olma hedefi yolundaki ilk temel belge olduğu belirtilebilecektir. Bu belge, RF'nin enformasyon güvenliği konusundaki yol haritasını, prensiplerini, amaçlarını ve konu kapsamındaki resmi görüşlerini genel hatlarıyla ortaya koymaktadır.[46] Belgede, RF'nin enformasyon güvenliğinin sağlanması konusundaki ulusal çıkarlarının temelde ekonomik yapının, sivil toplumun ve politik sistemin korunması ile sağlanabildiğine işaret edilmektedir.[47] Belgede RF'nin enformasyon savaşı konsepti 2000'li yılların ilk bölümü için potansiyel iki tehdit kaynağına odaklanmıştır. Söz konusu tehdit kaynaklarının ilki; RF'nin siyasi ve kültürel yapısını etkileyebilecek olan psikolojik savaş yöntemleri, diğeri ise RF'nin enformasyon ve teknoloji güvenliğini tehlikeye atabilecek olan siber savaş teknikleridir.[48]

*"Russia's National Security Strategy to 2020 / 2020'ye doğru Rus Ulusal Güvenlik Stratejisi"* tüm açıklığı ile güvenlik meselesine odaklanması bakımından dikkat çekici bir belge olarak karşımıza çıkmaktadır.[49] Söz konusu belgede, başta ekonomi olmak üzere, sağlık ve güvenlik stratejine ilişkin görüş ve planlamalara yer verilirken, enformasyon güvenliği konusu dolaylı olarak gündeme getirilmiştir. Bu belgede temel olarak güven artırıcı ve işbirliğini hedefleyen bir üslubun hâkim olduğu söylenebilecektir.

2011 yılında RF Savunma Bakanlığı tarafından yayımlanan*"Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space / Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler"* isimli belge, siber güvenlik analisti Keir Giles tarafından: *"Rus Ordusu'nun Ön Siber Savaş Doktrini"* şeklinde tanımlanmaktadır.[50] Bu kapsamda, belgenin siber uzayda Rus askeri varlığını ve hareketliliğini kabul eden ilk açık belge olduğu da ileri sürülebilir.[51] Bu dokümanda, diğer resmi RF stratejilerinin aksine bilgiyi merkeze alan bir bakış açısıyla siber faaliyetleri operasyonel bir mantık ve çatışma konsepti ile değerlendirme söz konusudur.

---

[46] A. Sergei Medvedev, Offence-Defence Theory Analysis of Russian Cyber Capability, Master Thesis, Naval Post-Graduate School, Monterey, California, https://www.google.com.tr/?gfe_rd=cr&ei=qzHZVrreN7Go8wfMuYegDw#q=this+thesis+represent+mikhail+tsypkin (alıntılama yanlış; doğrusu: http://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf?sequence=1), (Erişim Tarihi 05 Mart 2017), s. 55.

[47] Ministry of Foreign Affairs of the Russian Federation, Information Security Doctrine of Russian Federation, http://archive.mid.ru//bdomp/nsosndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument, (Erişim Tarihi 23 Mart 2016). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/ 99.html, (Erişim Tarihi 23 Haziran 2016).

[48] Thomas L. Timothy, "Russia's Information Warfare Strategy: Can the Nation Cope inFuture Conflicts?", *The Journal of Slavic Military Studies*, Cilt 27, No 1, 2014, s. 275.

[49] Ayrıntılı bilgi için bkz. Rustrans Useful Translations, "Russia's National Security Strategy to 2020", http://rustrans.wikidot. com/russia-s-national-security-strategy-to-2020, (Erişim Tarihi 23 Mart 2016).

[50] A.g.e..

[51] Ayrıntılı bili için bkz. The Russian Ministry of Defense, "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space", https://ccdcoe.org/strategies/ Russian_Federation_ unofficial_translation.pdf, (Erişim Tarihi 23 Mart 2016).

9 Kasım 2012 tarihinde RF Genelkurmay Başkanlığı görevine atanan Valery Gerasimov'un 27 Şubat 2013 tarihinde *"Military Industrial Kurier Dergisi'nde"* yayınlanan *"The Value of Science in Prediction"* adlı makalesinde ortaya koyduğu askeri yaklaşım, uluslararası ilişkiler alanında geniş yankı bulmuş ve "*Gerasimov Doktrini*" olarak tanımlanarak, tartışmaya başlanmıştır.[52] Diğer yandan, bahse konu makale hakkındaki tartışmaları mezkur dönemden günümüze kadar hararetli bir şekilde sürdüren temel neden ise Gerasimov'un yaklaşımına uygun bir tarzda, RSK'nın 2014 yılındaki Ukrayna müdahalesi esnasında gösterdiği çok yönlü sıcak çatışma performans ile ilgilidir.[53] Bu kapsamda, RSK, Ukrayna müdahalesi sırasında, organize bir şekilde yönlendirilen ekonomik tedbirleri, siber saldırı yöntemlerini, yerel Rus azınlıkla koordineli bir şekilde gerilla faaliyeti gerçekleştiren özel piyade kuvvetlerinin operasyonlarını ve psikolojik savaş yöntemlerini kullanmıştır.[54]

*"Concept of the Foreign Policy of the Russian Federation / RF Dış Politika Konsepti"*, 12 Şubat 2013 tarihinde RF Devlet başkanı Vladimir Putin'in onayı ile kabul edilmiş bir belgedir. Esas itibariyle RF'nin dış politikasının gelecek dönem hedefleri ile ilgili temel yaklaşım ve prensipleri ele alan bu belgede, enformasyon ve siber güvenlik alanında da bazı tespit ve değerlendirmeler mevcuttur.[55] Bu kapsamda belgede enformasyon alanında yaşanmakta olan yeni teknolojilerin ulusal güvenlik için tehdit olduğu vurgusu yapılarak, geleneksel uluslararası ilişkiler disiplini yaklaşımlarının ötesinde yeni enformasyon teknikleri ve kültürel metotların modern dış politika enstrümanları arasında kabul edilmesi gerektiği ifade edilmektedir.

2013 yılında kabul edilen *"Basic Principles for State Policy of the Russian Federation in the Field of International Information Security / RF Devlet Politikasının Uluslararası Enformasyon Güvenliği Alanındaki Temel Prensipleri"* isimli belge, RF'nin siber güvenlik kapsamındaki uluslararası girişim ve planlamalarının devamı kapsamında görülebilecektir. Bu itibarla söz konusu belge ile RF'nin uluslararası enformasyon güvenliği alanındaki temel prensiplerini tespit edilerek, uluslararası kamuoyuna ilan edilmiştir. Söz konusu belgede hedeflenen temel amacın; *"RF'nin bilgi ve telekomünikasyon teknolojileri alanında dünyanın diğer önemli güçleri ile eşitliği sağlayabileceği şartların oluşturulması"* olduğu ifade edilmiştir.[56]

*"RF Bilgi Güvenliği Doktrini / Information Security Doctrine of the Russian Federation"* isimli doküman,9 Eylül 2000 tarihli RF Enformasyon Güvenliği Doktrini'nin yerine yürürlüğe konulmak üzere hazırlanmıştır.6 Aralık 2016 tarihinde kabul edilenbelge, RF'nin siber savunma ve bilgi güvenliği alanındaki ulusal çıkarlarını belirlemekte ve bu alanlar kaynaklı olarak Rus çıkarlarını hedef alan tehdit unsurlarına işaret etmektedir. [57]

---

[52] Medvedev, a.g.e, s. 56.
[53] Darıcılı ve Özdal, "Enformasyon Savaşı Bağlamında…", a.g.e., s. 23.
[54] Ayrıntılı bilgi için bkz. Darıcılı ve Özdal, "Enformasyon Savaşı Bağlamında…", a.g.e., s .23-24.
[55] Ayrıntılı bilgi için bkz. The Russian Ministry of Defense, "Concept of the Foreign Policy of the Russian Federation", http://archive.mid.ru//brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D, (Erişim Tarihi 24 Mart 2016). Ayrıntılı bilgi için: http://archive.mid.ru//brp_4.nsf/0/6D84DDEDEDBF7DA644257 B160051BF7F, (Erişim Tarihi 26 Haziran 2016).
[56] NATO Cooperative Cyber Defense Centre of Excellence, "Basic Principles for State Policy of the Russian Federation in the Field of International Information Security", https://ccdcoe.org /sites/default /files/strategy/RU_state-policy.pdf, (Erişim Tarihi 24 Mart 2017). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/6/114.html, (Erişim Tarihi 26 Haziran 2016).
[57] "New Kremlin Information-Security Doctrine Calls For 'Managing' Internet In Russia", *RIA Novosti ve Mir24.Tv*, http://www.rferl.org/a/russia-informaiton-security-internet-freedomeconcerns/28159130

**RF'nin Siber Güvenlik Alanında Faaliyet Gösteren Resmi Kurum ve Kuruluşları**

Rus Federal Güvenlik Servisi (Federalnaya Slujba Bezopasnosti / FSB), Rus İstihbarat Servisi (Sluzhba Vneshney Razvedki / SVR) ve Rus Askeri İstihbarat Direktörlüğü'nin (Glavnoye Razvedyvatel'noye Upravleniye / GRU) gerek tek başlarına sahip oldukları siber kapasiteleri gerekse de Rus kriminal örgütleri ile olan illegal bağlantıları kapsamında RF'nin siber savunma ve saldırı kapasitesini belirleyen temel aktörlerdendir. Bu servislerden FSB ve SVR, RF Devlet Başkanı'na doğrudan bağlı durumdayken GRU, Savunma Bakanlığı'nın bir parçası konumunda ve RSK emrinde görev yapmaktadır.[58]

RF'ye yönelik siber saldırılara karşı koymak ve temelde ülkenin siber güvenliğini sağlamak, iç istihbarat servisi FSB'nin görevidir.[59] FSB'nin siber güvenlik operasyonlarına doğrudan yöneldiği tarih ise 2008'dir. 2008 yılında, 1978 yılında teknik operasyonları yürütmek amacıyla KGB bünyesinde kurulan "Kvant" isimli departman, FSB'nin adeta siber güvenlik operasyon merkezi haline dönüştürülmüştür.[60] FSB'nin siber güvenlik alanındaki diğer bir sorumluluğu, ülke genelindeki Rus vatandaşlarının ve yabancıların telekomünikasyon iletişim bilgilerinin istihbar olunan bilgiler kapsamında takip edilmesidir. FSB, Rus GSM ve telekom şirketlerinin yasal bir zorunluluk olarak kurmak zorunda oldukları, RF'deki internet ve anolog haberleşmesini takip eden ve bir nevi denetleme sistemi şeklinde tesis edilmiş olan "Operatif Denetleme Faaliyetleri Sistemi" (System for Operative Investigative Activities / SORM)'nin kontrolü görevini de üstlenmiştir.

FSB'nin sanayi, teknoloji ve bilişim sektörlerine yönelik espiyonaj faaliyetlerinin engellenmesi noktasında Rusya Teknik ve İhracat Kontrol Servisi (Federal Service for Technical and Export Control of Russia / FSTEC) ile de yakın işbirliği bulunmaktadır. Bu kapsamda 2004 yılında kurulan ve RF Savunma Bakanlığı bünyesinde faaliyet göstermekte olan FSTEC'nin ihracat denetim rejimini kontrol etmek suretiyle sanayi, teknoloji ve bilişim sektörlerini hedef alan espiyonaj operasyonlarına karşı koymada önemli bir rolü bulunduğu belirtilebilir.[61] FSB, siber güvenlik alanındaki çalışmalarının yanı sıra diğer tüm faaliyetlerinde SVR ile koordinasyon içinde sürdürmektedir.[62]

Siber güvenlik stratejisi kapsamında RF'nin bir ülkenin bilim ve teknoloji kapasitesi hedef alan siber casusluk operasyonlarını planlamak, dış istihbarat SVR'nin görevleri arasındadır. SVR'nin yurt dışında Belarus, Kazakistan,Tacikistan, Ermenistan, Kırgızistan, Suriye, Küba, Vietnam ile Güney Osetya, Abhazya, Kırım ve Transdinyester bölgelerinde GRU ile birlikte ortak kullandığı elektronik ve sinyal istihbaratı toplama merkezleri de mevcuttur.[63]

---

.html, (Erişim Tarihi 02 Ocak 2017). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/ documents/6/135.html, (Erişim Tarihi 02 Ocak 2017).

[58] Heickerö, a.g.e, s. 27.

[59] Ayrıntılı bilgi için bkz. The Centre For Counterintelligence and Security Studies, "Russia's SVR/FSB/GRU Intelligence Services", http://www.cicentre.com/?page=191, (Erişim Tarihi 27 Mart 2016).

[60] Ayrıntılı bilgi için bkz. Jeffrey Carr, "Intelligence on Russian Information Warfare Activities", http://jeffreycarr.blogspot.com/2012/01/intelligence-on-russian-information.html, (Erişim Tarihi04 Ocak 2017).

[61] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld,* O'Reilly Media Inc., USA, 2011, s. 318.

[62] Ayrıntılı bilgi için bkz. R. Tocaso Staar, "Russia's Security Services", *Mediterranean Quarterly*, Cilt 15, Sayı 1, 2010, s. 1-10.

[63] Heickerö, a.g.e., s. 30

Askeri istihbarat servisi GRU'nun siber güvenlik açısından temel görevleri, Rus askeri kapasitesini hedef alan dış servis kaynaklı siber operasyonlara karşı kontr/espiyonaj faaliyeti yürütmek ve imkan bulunması halinde hedef ülkenin askeri kapasitesine yönelik siber casusluk operasyonları planlamaktır. Stratejik Füze Birlikleri'nin faaliyetlerinin sürdürülmesi ayrıca ülkeye yönelik siber saldırılara karşı koymak üzere kurulmuş olan "Computer Emergency Response Team" (RE-CURT)'lerin kontrolü de GRU'nun diğer Rus istihbarat ve güvenlik kuruluşları ile koordineli olarak gerçekleştirdiği görevleri arasındadır.[64]

Öte yandan, SVR, FSB ve GRU'nun faaliyetlerinin yanı sıra diğer istihbarat ve güvenlik servislerinin yetkilerinin ve görev alanlarının yeniden planlanması kapsamında, 2000'li yılların başı itibariyle RF'nin siber kapasitesini geliştirme yönünde ciddi adımlar attığı da bilinmektedir. Bu bağlamda, RF 1993 yılında kurulmuş olan, elektronik ve sinyal istihbaratı ile kriptoloji alanlarında faaliyet gösteren FABSİ (Federal Agency of Government Communications and Information / Federal İletişim ve Enformasyon Ajansı)'yi 2003 yılında lağvederek, bu kuruluşun yetki ve sorumluluklarını FSB, SVR, RF Savunma Bakanlığı ve Federal Koruma Servisi'ne (Federalnaya Sluzhba Okhrany / FSO) arasında dağıtmıştır. FABSİ'nin kapatılmasının en önemli nedeni ise kurum içerisindeki yolsuzluk ve organize suç örgütleri ile bağlantılı yapılanmalardır.[65] FSO'nun siber güvenlik alanındaki temel görevi ise RF'nin ilgili kurumları ve yöneticileri arasındaki üst düzey ve gizlilik içeren iletişimin güvenli bir şekilde sürdürülmesini denetlemek ve yönetmektir. Doğrudan RF Devlet Başkanı'na bağlı olarak faaliyet yürütür. FSO'nun, ülke genelindeki telgraf, kablolu telefon hatlarının, internet ve iletişim haberleşmesinin kontrolü ve denetimi, ayrıca Rus uyduları üzerinden toplanan sinyal istihbaratının değerlendirilmesi ve raporlanması, son olarak Rus nükleer silah sisteminin güvenliğin sağlanması şeklinde görevleri de bulunmaktadır.[66]

RF 2010 yılında enformasyon ve bilgi teknolojileri alanında çalışma yürütmek amacıyla Savunma Bakanlığı bünyesinde bir "bakan yardımcılığı" pozisyonunu da tesis etmiştir.[67] RF, 2013 yılında aldığı bir karar ile RSK bünyesinde bağımsız bir siber savaş birimi kurmayı planlama kapsamına almıştır.[68]

Yukarıda aktardığımız bilgilerden de anlaşıldığı üzere Rus sivil ve askeri istihbarat servisleri, haber toplama yöntemi olarak geleneksel HUMINT (Human Intelligence / İnsan Kaynaklı İstihbarat), SIGINT (Signal Intelligence / Sinyal İstihbaratı), ELINT (Electronic Intelligence / Elektronik İstihbarat) ve diğer istihbarat toplam tekniklerinin yanı sıra siber saldırı şeklinde düzenlenmiş espiyonaj operasyonlarına dayanan geniş ve sistematik bir yapıya sahip olmayı hedeflemektedir. Böyle bir yapılanma ile RF, Rus toplumunun ekonomik kalkınmasını ve enerji güvenliği açısından hayati öneme sahip ekonomik, finansal ve teknolojik istihbarat ihtiyaçlarını karşılamaya ve ülke güvenliğini sağlamaya çalışmaktadır. Son yıllarda

[64] A.g.e., s. 27
[65] Heickerö, a.g.e., s. 28.
[66] A.g.e, s. 29
[67] EastWest Instıtute, "The American and Russian Approaches to Cyber Challenges", http://www.omicsgroup.org/journals/the-american-and-russian-approaches-to-cyber-challenges-2167-0374.1000110.pdf, (Erişim Tarihi 14 Nisan 2017).
[68] "Russia Announces Development of Cyber Military Unit", *State Security Magazine*, http://www.tripwire.com/state-of-security/latest-security-news/russia-announces-development-cyberwar-military-unit/, (Erişim Tarihi 26 Mart 2017).

yapılan yatırımlar ile RF'nin bu amaca hizmet eden siber kapasitesinde ciddi bir artış söz konusu olmuştur.[69]

Rus istihbarat servislerinin çalışma alanları, operasyonları, imkân ve kabiliyetleri ile siber kapasiteleri sıklıkla dünya kamuoyunda tartışılmasına rağmen, bu servislerin örtülü siber faaliyetleri ile ilgili olarak sınırlı açık kaynak bilgisi mevcuttur. Konu kapsamında hâkim olan kanı, FSB, GRU, SVR ve FSO'nun siber uzay alanında kendi faaliyet alanları ile ilgili olarak, öz kaynaklarını ve uzman personelini kullanmak suretiyle özel operasyonlar sürdürmekte oldukları şeklindedir. Bu servislerin ihtiyaç hissettikleri faaliyetleri için ise siber kabiliyete sahip kriminal şahıslardan da istifade ederek, özel operasyonlar planlayabildikleri de iddia edilmektedir.

Genel hatlarıyla izah edilmeye çalışıldığı üzere ABD ve RF'nin siber uzayda 2000'li yıllar sonrasında ortaya koyduğu siber güvenlik strateji belgelerinde belirlediği hedefler kapsamında ulusal ve uluslararası siber savunma ve saldırı kapasitelerini geliştirme noktasında diğer devletlere kıyasla önemli mesafe aldıkları ortadadır. Bununla birlikte iki devlet arasında 2015 yılına kadar örtülü bir şekilde yaşanmakta olan siber mücadele, 2015 yılından itibaren RF'nin ABD'nin başkanlık seçim sürecine siber saldırı yöntemleri ile manipüle ettiği yönündeki iddialar ile birlikte günümüzde adeta açık bir siber çatışma haline evrilmiştir.

## RF'nin Siber Saldırı Yöntemleri ile ABD Başkanlık Seçimine Müdahale Ettiğine Yönelik İddialar

İlk olarak Demokrat Parti yönetimi, sonrasında ise ABD'nin siber güvenlik alanında faaliyet gösteren kuruluşları tarafından, RF'nin 2016 yılı içerisinde Demokrat Parti Ulusal Komitesi (DUK)'nin, Clinton'ın seçim kampanyası direktörü olan John Podesta ile ABD eski Dışişleri Bakanı ve aynı zamanda Demokrat Parti'nin seçim çalışmalarına aktif olarak destek veren Colin Powell'ın e-postalarını siber saldırı yöntemleri ile temin ettiği ve bu e-postalardan bazılarını kamuoyuna sızdırdığı, böylelikle de RF'nin aktif bir şekilde ABD seçim sürecini kendi ulusal çıkarları kapsamında manipüle ettiği iddia edilmiştir.[70]

Söz konusu siber saldırılar ile ilgili olarak ise açık kaynaklarda yer alan haberlerde, RF istihbarat örgütlerinin bizzat Putin'in talimatıyla bu saldırıları organize ettiği, bahse konu saldırıların nedeninin ise 2012 yılında RF başkanlık seçimlerine yönelik olarak Clinton'ın da dışişleri bakanı olarak yer aldığı ABD yönetiminin Putin karşıtı açık ve örtülü faaliyetleri olduğu hususları da gündeme getirilmiştir.[71]

RF tarafından gerçekleştirildiği iddia edilen siber saldırılar, 2015 yaz ayları içinde başlayacak şekilde RF iç istihbarat örgütü FSB, RF askeri istihbarat örgütü GRU tarafından bizzat veya bu örgütler tarafından desteklenen hacker grupları vasıtasıyla gerçekleşmiştir. Söz konusu

[69] Ayrıntılı bilgi için bkz. William Hagestad II, "Comparative Study: Iran, Russia and PRC Cyber War", RSA Conference, 2013 Europe, http://www.rsaconference.com/writable/presentations/file_upload/hta-w01-comparative-study-iran-russia-prc-cyber-war_copy1.pdf, (Erişim Tarihi05 Mart 2017), s. 18-25.

[70] "Clinton'a 4 ay Boyunca Yapılan Siber Saldırılar, Seçimleri Manipule Etti", *Türk İnternet Haber Sitesi*, http://www.turk-internet.com/portal/yazigoster.php?yaziid=55005, (Erişim Tarihi 20 Şubat 2017).

[71] NY Times, "Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says", https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html, (Erişim Tarihi 20 Şubat 2017).

hacker grupları arasında yer alan ve FSB tarafından desteklendiği iddia edilen yapılanmaların adları, Cozy Bear, the Dukes ve APT 29'dur. GRU tarafından desteklendiği iddia edilen grup ise Fancy Bear veya APT 28 olarak isimlendirilmektedir. Ayrıca "Guccifer 2.0" adıyla bireysel olarak faaliyet gösteren bir hacker yapılanması da bahse konu saldırılarda rol oynamıştır. Saldırılar, "spread phishing" şeklinde ifade edilen hedef odaklı ve yemleme yöntemleri ile gerçekleştirilmiştir. Bu yöntemle, hedef kurum ve şahısların e-postaları (50-60 bin civarı) siber casusluk amaçlı kötü yazılımlar ile temin edilerek, manipülasyonun amacına uygun olanları çeşitli internet sayfaları ve medya kuruluşları (WikiLeaks, The New York Times, DC Leaks, The Washington Post, The Wall Street Journal) tarafından kamuoyuna ifşa ettirilmiştir.[72]

Söz konusu ifşalar neticesinde ise ABD Demokrat Parti seçim propaganda sürecinin kısmen etkilendiği ileri sürülebilir. Bu kapsamda, DUK Başkanı Debbie Wasserman Schultz ve bazı üst düzey görevliler istifa etmiş, Demokrat Parti'nin diğer başkan adayı Senatör Bernie Sanders'in pozisyonu güçlenmiş ve adaylık yarışına bir süre daha devam etmesi sağlanmış, Cumhuriyetçi Parti'nin eline Demokrat Parti'nin aleyhine kullanabileceği bir koz verilmiş, Clinton ismi tartışmalı hale gelerek, yıpratılmıştır.[73]

Bununla birlikte, söz konusu siber saldırılar neticesinde ifşa edilen e-postaların yarattığı olumsuz etkinin, Clinton karşısında Trump'un zaferini sağlayan en önemli faktör olduğunu gündeme getirmenin de iddialı bir değerlendirme olduğu da ileri sürülebilecektir. Bu noktada, Trump'ın seçim zaferi sonrasında anılanı yıpratmak ve baskı altına almak amacıyla ABD'deki bazı çevrelerin söz konusu siber saldırıları sürekli gündemde tutarak, Trump aleyhine kullanmakta olduğu da bizce dikkate alınması gereken bir durumdur.

Söz konusu siber saldırılar ile ilgili olarak FBI ve DHS tarafından ortak olarak hazırlanmış olan bir raporda ise RF, bu siber saldırıların planlayıcısı olarak doğrudan suçlanmıştır. Ayrıca, bahse konu raporla birlikte yayımlanan 29 Aralık 2016 tarihli medya bildirisinde, belirtilen raporda gündeme gelen siber saldırıların da ötesinde, Rus istihbarat unsurlarının ABD hükümet kuruluşlarını, sivil toplum örgütlerini, üniversiteleri, ABD kritik altyapılarını, düşünce kuruluşlarını, teknoloji üreten şirketlerini hedef alan siber saldırılar planlamakta olduğu da gündeme getirilmiştir.[74]

Bununla birlikte DHS tarafından 30 Aralık 2016 tarihinde yapılan bir başka medya açıklamasında,[75] RF sivil ve askeri istihbarat yapılarının son dönemlerde ABD hükümetini ve vatandaşlarını hedef alan sofistike ve agresif siber operasyonlar düzenlediği, ABD güvenlik ve istihbarat kurumlarının bu saldırıları "Grizlly Steppe" takma adıyla tanımladığı, "Grizlly Steppe" faaliyeti ile RF'nin ABD'nin hükümet kuruluşlarına, üniversitelerine sivil toplum ve düşünce kuruluşlarına, siyasi partilerine "spread phishing" şeklinde ifade edilen hedef odaklı ve yemleme

---

[72] NY Times, "Hackers to the U.S. Election", https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html, (Erişim Tarihi 20 Şubat 2016).

[73] "Beyaz Saray, Rusya'nın Hackleme Operasyonuna Cevap Verileceğini Açıkladı", *Türk İnternet Haber Sitesi*, http://www.turk-internet.com/portal/yazigoster.php?yaziid=54247, (Erişim Tarihi 20 Şubat 2017).

[74] Department of Homeland Security, "Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity", https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity, (Erişim Tarihi 20 Şubat 2017).

[75] Department of Homeland Security, "Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale", https://www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary, (Erişim Tarihi 20 Şubat 2017).

yöntemleri ile siber casusluk operasyonları düzenlediği ve elde ettiği gizli bilgileri üçüncü ortaklar vasıtasıyla kamuoyuna ifşa ettiği, belirtilerek, söz konusu "spread phishing" operasyonlarının yazılımlarına ve uygulanma şekillerine ait bazı teknik detaylar kamuoyuyla paylaşılmıştır.

Ayrıca konuya ilişkin olarak Federal Araştırma Bürosu (Federal Bureau of Investigation / FBI), Merkezi Haber Alma Servisi (Central Intelligence Service / CIA) ve Ulusal Güvenlik Ajansı ( National Security Agency / NSA) tarafından 7 Ocak 2017 tarihinde kamuoyuna açıklanan ortak raporda; "*Putin'in 2016 ABD Başkanlık seçim sürecinin manipülasyonu emrini bizzat verdiği, bu manipülasyonun temel amacının Demokrat Parti'ye olan kamuoyu güvenini sarsmak olduğu, süreçten Demokrat Parti adayı Clinton'un açıkça zarar gördüğü ve bu durumdan diğer başkan adayı Donald Trump'ın da istifade ettiği*" belirtilmiştir.[76]

ABD resmi kurumlarınca RF hükümetine yapılan söz konusu açık suçlamalar sonrasında, Obama yönetimi tarafından çoğunluğu GRU mensubu olduğu iddia edilen 35 Rus diplomatın, ABD başkanlık seçimlerini hedef alan siber saldırılarda görev yaptıkları iddiasıyla sınır dışı edilmesi ile Maryland ve New York'taki Rus diplomatik temsilciliklerinin kapatılması kararı alınmıştır.[77] Söz konusu sınır dışı kararı karşısında ise RF tarafı belirtilen suçlamaları kabul etmediğini açıklamıştır. Putin tarafından konuyla ilgili olarak yapılan açıklama ise "*gelişmelerin kendileri tarafından Washington yönetiminin attığı yeni düşmanca adımlar ve provokasyon olarak nitelendirildiği, hiç kimseyi sınır dışı etmeyecekleri ve ABD'ye verilecek yanıtı Trump yönetiminin tutumuna göre belirleyecekleri*" ifade edilmiştir.[78]

Konu kapsamında ilerleyen süreçte Putin tarafından 1 Haziran 2017'de yapılan "*Vatansever Rus Hackerler*" şeklindeki açıklamada dünya kamuoyunda geniş yankı bulmuştur. Bu itibarla Demokrat Parti Hack Skandalı kapsamındaki bir soruya cevaben Putin; "*RF'nin hiçbir zaman böyle bir şeye dahil olmadığını, belki vatansever Rus hackerların siber saldırı düzenlemiş olabileceğini, eğer hackerların vatansever düşüncedeyse, Rusya hakkında kötü konuşanlara karşı iyi bir savaş açma konusunda kendi katkılarını yapmaya başlayabileceğini, bunun teorik olarak mümkün olduğunu, devlet düzeyinde hiçbir zaman hackleme olaylara dahil olmadıklarını ve olmayı da planlamadıklarını*" belirtmiştir.[79]

Bu gelişmelere ilave olarak FBI eski direktörü James Comey'in ABD Kongresi'nde konu kapsamında açılan soruşturma dâhilinde 6 Haziran 2017 tarihinde verdiği ifade de oldukça önemlidir. Bu ifadesinde gelen sorulara karşılık olarak anılan tarafından; "*Rusya'nın seçimlerle ilgili siber saldırı yaptığı konusunda şüphe duymadığı, Trump'ın kendisinden konuyla ilgili yapılan 'FBI soruşturmasını durdurmasını istediği, bu kapsamda Trump'a*

[76] Office of the Director of National Intelligence, "Background to "Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution", https://www.dni.gov/files/documents/ICA_2017_01.pdf, (Erişim Tarihi 10 Temmuz 2017).

[77]"Beyaz Saray ABD, 35 Rus diplomatı 72 saat içerisinde sınır dışı edecek", *Sputniknews Haber Portalı*, https://tr.sputniknews.com/abd/201612291026553306-abd-rusya-yaptirim-diplomat-sinir-disi/, (Erişim Tarihi 20 Şubat 2017).

[78] "Putin'den ABD'ye yanıt: Biz hiç kimseyi sınır dışı etmeyeceğiz.", *Sputniknews Haber Portalı*, https://tr.sputniknews.com/rusya/201612301026565257-putin-abdye-yanit-biz-hic-kimseyi-sinir-disi-etmeyecegiz/, (Erişim Tarihi 20 Şubat 2017).

[79] "Putin: 'Patriotic' Russian hackers may have targeted US election", *CNN International*, http://edition.cnn.com/2017/ 06/01/politics/russia-putin-hackers-election/index.html, (Erişim Tarihi 10 Temmuz 2017).

*güvenmediği için adı geçen ile yaptığı her görüşmeyi kayıt altına alma ihtiyacı hissettiği*" beyan edilmiştir.[80]

## Sonuç

İtici gücü internet ve ağ teknolojileri temelli gelişmeler olan siber uzay, artık devletler tarafından yeni bir mücadele alanı olarak görülmeye başlanmıştır. Mevcut siyasi, ekonomik ve askeri güçleri kapsamında küresel sistemde hegemon güç konumunda olan ABD ve RF, söz konusu güçlerini kaybetmemek ve hatta daha da artırmak amacıyla siber uzay kaynaklı gelişmeleri askeri kapasitelerini geliştirmek adına yeni bir imkan olarak değerlendirmişlerdir. Soğuk Savaş dönemindeki rekabet sürecinin bir sonucu olan teknolojik miraslarının da katkısıyla, ABD ve RF ağ teknolojileri merkezli gelişmeleri kullanmak suretiyle etkili bir siber saldırı ve savunma kapasiteyi geliştirmeye yönelik planlamalarına hız vermişlerdir.

Bu kapsamda öncelikle ABD, özellikle 1990'lı yılların ikinci yarısından sonra teknolojik imkânları, ekonomik gelişmişlik düzeyi ve kurumsal örgütlenmeleri ile birlikte siber uzay alanında etkili rol oynayan ilk hegemon güç olmuştur. SSCB'nin dağılması sonrasında bir süre siyasi ve ekonomik toparlanma süreci yaşayan RF ise 2000'li yıllar ile birlikte ortaya koyduğu strateji ve planlamalar ile birlikte, günümüzde siber uzayda ABD karşıtlığını ve çıkarlarını hedef alan güçlü ve agresif bir etkinliğe ulaşmıştır.

Bir başka ifadeyle de 2000'li yılların ikinci yarısından sonra RF'nin siber uzay alanında ortaya koyduğu yenilikler ile geliştirdiği saldırı kapasitesi, bu hamlelere yönelik ABD'nin ortaya koyduğu tedbirler ve karşı girişimler günümüzde uluslararası ilişkilerde etkisini süratle hissettirmiştir. Bu nedenle de süreç içinde, ABD ve RF tarafından karşılıklı etkileşim ve etki-tepki ilişkisi kapsamında geliştirdikleri siber savunma ve saldırı kapasiteleri, özellikle de 2010 yılı sonrasında devletlerin klasik güvenlik anlayışlarında, ortaya çıkan bu yeni duruma göre revizyona gitmelerine neden olmuştur. Bu çerçevede, ABD ve RF kaynaklı olarak bugüne kadar gerçekleşen siber saldırıların ve espiyonaj faaliyetlerinin siber uzayın anonim doğası gereği kolay ve arkada iz bırakmadan planlanabilir oluşu, uluslararası ilişkilerde tehdit, güvenlik ve caydırıcılık konularındaki güncel yaklaşımların uygulanabilirliği noktasındaki yeni nesil sorunlar olarak ele alınmaya başlanmıştır.

Çalışmamızda analiz edilmeye çalışıldığı şekilde ABD ve RF arasında önceleri örtülü siber operasyon ve saldırılar ile birlikte süregelmekte olduğu iddia edilebilecek olan siber mücadele, RF'nin siber saldırı yöntemleri ile ABD başkanlık seçimine müdahale ettiğine yönelik iddialar ile birlikte çok daha belirgin hale gelmiştir. Bu kapsamda ABD yönetimindeki üst düzey isimlerin de açıkça beyan ettiği üzere, kısa ve orta vadede ABD'nin RF'nin söz konusu siber saldırısına karşı aktif tedbirler alacağı, bu tedbirlerin ise Rus çıkarlarını küresel düzeyde tehdit eden siber operasyonlar kapsamında gerçekleşeceği açıktır. Ayrıca bu tahminlerin de ötesinde, ABD'nin 2018 yılında yapılacak olan RF başkanlık seçimlerini etkilemeye yönelik kapsamlı enformasyon savaşı stratejileri ve siber saldırıları şimdiden planlamakta olduğu da rahatlıkla öngörülebilecektir.

[80] "Eski FBI Başkanı Comey: Trump yönetimi yalan söyledi.", *BBC*, http://www.bbc.com/turkce/haberler-dunya-40199389, (Erişim Tarihi 10 Temmuz 2017).

RF'nin ise kendi ülkesine yönelik olası siber saldırıları bertaraf etme konusundaki çalışmaları da yoğun bir şekilde sürmektedir. Bu kapsamda önümüzdeki süreçte RF hükümetinin milli yazılımların kullanılması, milli sosyal medya uygulamalarının yaygınlaştırılması, ulusal internet sisteminin denetim ve kontrolünün sıkılaştırılması, silahlı kuvvetleri ve istihbarat servisleri bünyesinde etkili, aktif ve merkezi denetime sahip yeni siber birimlerin tesis edilmesine yönelik planlamaları artacaktır. RF'nin söz konusu siber savunma imkânlarının geliştirilmesine yönelik çabalarını etkili bir enformasyon savaşı stratejisiyle destekleyeceği de ortadadır. Bu kapsamda, küresel düzeyde faaliyet gösteren medya kuruluşları ile sosyal medyada aktif olarak hâlihazırda faaliyet gösteren troll ağı ile birlikte, RF'nin yeni nesil enformasyon stratejisi geliştirme konusunda yakın gelecekte çok daha etkili olacağı öngörülebilecektir. Bu durumda ise RF'nin etkili siber saldırı ve savunma kapasitesiyle birlikte, gelişmiş bir küresel siber propaganda sistematiği sayesinde siber uzayda ABD ile ciddi bir rekabete girmekten çekinmeyeceği de ileri sürülebilecektir.

Tüm bu rekabet süreçlerinin ise insan eliyle yapılmış, birbiriyle eklemlenmiş ağ teknolojileri vasıtasıyla oluşturulmuş ve beşinci boyut olarak adlandırılan siber uzay alanının şekillenmesine doğrudan tesir edeceği ve bu kapsamda da siber uzayın devletlerarası mücadelenin yoğun bir şekilde yaşanacağı yeni bir mecra olarak uluslararası ilişkiler analizlerinde daha detaylı bir şekilde değerlendirilmesine yol açacağı da ortadadır.

## Kaynakça

Abbate, Janet, "Government, Business, and the Making of the Internet", *Business History Review*, Cilt 75, No 1, Bahar 2001, s.147-176.

*AFCEA Organization*, The Evolution of US Cyberpower, http://www.afcea. org/committees /cyber/documents/TheEvolutionofUSCyberpower.pdf, (Erişim Tarihi 23 Nisan 2016).

Akyazı, Uğur, "Uluslararası Siber Güvenlik Stratejisi ve Doktrinler Arasında Alınabilecek Tedbirler", 6.Uluslararası Siber Güvenlik ve Kriptoloji Konferansı, http://www.iscturkey. org/s/2226/i/ 2013-paper105.pdf, (Erişim Tarihi 14 Nisan 2017).

Başa, Şafak, "ABD İç Güvenlik Bakanlığı", https://www.academia.edu/9830086/ ABD_%C4% B0%C3 %87_G%C3%9CVENL%C4%B0K_BAKANLI%C4%9EI_SUNUM_, (Erişim Tarihi 31 Nisan 2017).

"Beyaz Saray ABD, 35 Rus diplomatı 72 saat içerisinde sınır dışı edecek", *Sputniknews Haber Portalı*, https://tr.sputniknews.com/abd/201612291026553306-abd-rusya-yaptirim-diplomat-sinir-disi/, (Erişim Tarihi 20 Şubat 2017).

"Beyaz Saray, Rusya'nın Hackleme Operasyonuna Cevap Verileceğini Açıkladı", *Türk İnternet Haber Sitesi*, http://www.turk-internet.com/portal/yazigoster.php?yaziid=54247, (Erişim Tarihi 20 Şubat 2017).

Bıçakcı, Salih, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler*, Cilt 10, No 40, Kış 2014, s. 101-130.

Bıçakcı, Salih, *21. Yüzyılda Siber Güvenlik*, İstanbul, Bilgi Üniversitesi Yayınları, Ağustos 2013.

Carr, Jeffry, "Intelligence on Russian Information Warfare Activities", http://jeffreycarr.blogspot.com/2012/01/intelligence-on-russian-information.html, (Erişim Tarihi 04 Ocak 2017).

Carr, Jeffrey, *Inside Cyber Warfare: Mapping the Cyber Underworld,* O'Reilly Media Inc., USA, 2011.

*Committee on Homeland Security and Governmental Affairs*, A Review of the Department of Homeland Security's Missions and Performance, file:///C:/Users/tk44655/Downloads /Senator%20Coburn%20DHS%20Report%20FINAL%20(3).pdf, (Erişim Tarihi 31 Mayıs 2016).

Chivers, Ian ve Jane Sleightholme, "Fortran History and Development", http://www.fortranplus .co.uk/resources/Fortran_history_and_development.pdf, (Erişim Tarihi 23 Nisan 2015).

"Cyberspace Becomes Second Front in Russia's Clash With NATO", *Bloomberg Tecnology News Portal*, http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato, (Erişim Tarihi 01 Nisan 2017).

"Clinton'a 4 ay Boyunca Yapılan Siber Saldırılar, Seçimleri Manipule Etti", *Türk İnternet Haber Sitesi*, http://www.turk-internet.com/portal/yazigoster.php?yaziid=55005, (Erişim Tarihi 20 Şubat 2017).

Darıcılı, A. Burak, "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırılar", *Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Cilt 7, No 2, 2014, s.1-16.

Darıcılı, A. Burak ve Barış Özdal, "Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi", *Gelişim Üniversitesi Sosyal Bilimler Dergisi*, Cilt 4, Sayı 1, Nisan 2017, s.19-40.

*Department of Homeland Security*, Executive Summary of Grizzly Steppe Findings from Homeland Security Assistant Secretary for Public Affairs Todd Breasseale, https://www.dhs.gov/news/2016/12/30/executive-summary-grizzly-steppe-findings-homeland-security-assistant-secretary, (Erişim Tarihi 20 Şubat 2017).

*Department of Homeland Security*, Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity, https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber -activity, (Erişim Tarihi 20 Şubat 2017).

*Department of Homeland Security*, National Cybersecurity and Communications Integration Center, https://www.isaca.org/chapters2/New-York-Metropolitan/membership/Documents/2012-04-30%20Spring%20Conference-Meeting/2%20Lichtenfels%20DHS%20NCCIC%202.pdf, (Erişim Tarihi 31 Mayıs 2016).

*EastWest Instıtute*, The American and Russian Approaches to Cyber Challenges, http://www.omicsgroup.org/journals/the-american-and-russian-approaches-to-cyber-challenges-2167-0374.1000110.pdf, (Erişim Tarihi 14 Nisan 2017).

"Eski FBI Başkanı Comey: Trump yönetimi yalan söyledi.", *BBC*, http://www.bbc.com/turkce/haberler-dunya-40199389, (Erişim Tarihi 10 Temmuz 2017).

*Federal Bureau of Investigation, Cyber Crime*, https://www.fbi.gov/about-us/investigate /cyber/ncijtf, (01 Haziran 2017).

Gerden, Eugene, "$500 Million for New Russian Cyber Army", Security Magazine UK, http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/, (Erişim Tarihi 26 Mart 2016).

Gibson, William, *Neuromancer*, Ace Books, New York, 1984.

"Hackers to the U.S. Election", *NY Times*https://www.nytimes.com/interactive /2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html, (Erişim Tarihi 20 Şubat 2016).

Hagestad II, William, "Comparative Study: Iran, Russia and PRC Cyber War", RSA Conference, 2013 Europe, http://www.rsaconference.com/writable/presentations/file_upload/hta-w01-comparative-study-iran-russia-prc-cyber-war_copy1.pdf, (Erişim Tarihi05 Mart 2017).

Heickerö, Roland, Emerging Cyber Threats and Russian Views on Information Warfare and Operation, Swedish Defense Research Agency Press, Mart, http://www.foi.se/rapport?rNo=FOI-R--2970--SE, (Erişim Tarihi 23 Haziran 2016).

Medvedev, A. Sergei, *Offence-Defence Theory Analysis of Russian Cyber Capability*, Master Thesis, Naval Post-Graduate School, Monterey, Colifornia, https://www.google.com.tr/?gfe_rd=cr&ei=qzHZVrreN7Go8wfMuYegDw#q=this+thesis+represent+mikhail+tsypkin, (Erişim Tarihi 05 Mart 2017).

*Ministry of Foreign Affairs of the Russian Federation*, Information Security Doctrine of Russian Federation,http://archive.mid.ru//bdomp/nsosndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument, (Erişim Tarihi 23 Mart 2016).

Mowthorpe, Matthew, "The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views", file:///C:/Users/tk44655/Downloads/2011.06.02-Maturing-Revolution-In-Military-Affairs1.pdf, (Erişim Tarihi 05 Mart 2017).

*National Security Agency*, 60 Years of Defending Our Nation, http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf, (Erişim Tarihi 30 Mayıs 2016).

*NATO Cooperative Cyber Defense Centre of Excellence*, National Security Strategy, https://ccdcoe.org/sites/default/files/strategy/USA_NSS2015.pdf, (Erişim Tarihi 25 Mayıs 2016).

*NATO Cooperative Cyber Defense Centre of Excellence*, National Cyber Security Organisation in United States, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf, (Erişim Tarihi 01 Haziran 2019).

*NATO Cooperative Cyber Defense Centre of Excellence*, The Department of Defence Cyber Strategy,http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, (Erişim Tarihi 25 Mayıs 2016).

*NATO Cooperative Cyber Defense Centre of Excellence*, Basic Principles for State Policy of the Russian Federation in the Field of International Information Security, https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf, (Erişim Tarihi 24 Mart 2017).

"New Kremlin Information-Security Doctrine Calls For 'Managing' Internet In Russia", *RIA Novosti ve Mir24.Tv*, http://www.rferl.org/a/russia-informaiton-security-internet-freedome concerns/28159130.html, (Erişim Tarihi 02 Ocak 2017).

*Office of the Director of National Intelligence*, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, https://www.dni.gov/files/documents/ICA_2017_01.pdf, (Erişim Tarihi 10 Temmuz 2017).

*Presidency Of USA*, Executive Order 13010—Critical Infrastructure Protection, http://www.presidency.ucsb.edu/ws/?pid=53066, (Erişim Tarihi 17 Şubat 2017).

"Putin'den ABD'ye yanıt: Biz hiç kimseyi sınır dışı etmeyeceğiz.", *Sputniknews Haber Portalı*, https://tr.sputniknews.com/rusya/201612301026565257-putin-abdye-yanit-biz-hic-kimseyi-sinir-disi-etmeyecegiz/, (Erişim Tarihi 20 Şubat 2017).

"Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says", *NY Times*, https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html, (Erişim Tarihi 20 Şubat 2017).

**"**Putin: 'Patriotic' Russian hackers may have targeted US election**"**, *CNN International*, http://edition.cnn.com/2017/ 06/01/politics/russia-putin-hackers-election/index.html, (Erişim Tarihi 10 Temmuz 2017).

"Russia Announces Development of Cyber Military Unit", *State Security Magazine*, http://www.tripwire.com/state-of-security/latest-security-news/russia-announces-developme nt -cyberwar-military-unit/, (Erişim Tarihi 26 Mart 2017).

*Rustrans Useful Translations*, Russia's National Security Strategy to 2020, http://rustrans.wikidot. com/russia-s-national-security-strategy-to-2020, (Erişim Tarihi 23 Mart 2016).

Staar, R. Tocaso, "Russia's Security Services", *Mediterranean Quarterly*, Vol 15, Issue 1, 2010, ss.1- 10.

Stewart, Phil ve Jim Wolf, "Old Worm Won't Die after 2008 Attack on Military", *Reuters*, June 16 2011, http://www.reuters.com/article/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617, (Erişim Tarihi16 Haziran 2016).

*The Centre For Counterintelligence and Security Studies*, Russia's SVR/FSB/GRU Intelligence Services, http://www.cicentre.com/?page=191, (Erişim Tarihi 27 Mart 2016).

*The Russian Ministry of Defense*, Concept of the Foreign Policy of the Russian Federation,http://archive.mid.ru//brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D, (Erişim Tarihi 24 Mart 2016).

*The Russian Ministry of Defense*, Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space, https://ccdcoe.org /strategies/ Russian_Federation_unofficial_translation.pdf, (Erişim Tarihi 23 Mart 2016).

Tirrell, K. William, *United States Cybwer Security Strategy, Policy and Organization: Poorly Postured to Cope With a Post-9/11 Security Environment*, Master Thesis, Washington University, 2012, https://www.hsdl.org/?view&did=729810, (Erişim Tarihi 10 Şubat 2017).

Thomas, L. Timothy, "Russia's Information Warfare Strategy: Can the Nation Cope inFuture Conflicts?", *The Journal of Slavic Military Studies*, Cilt 27, No 1, 2014, s. 20-42

*White House, Presidential Decision Directive (PDD)-63*, Critical Infrastructure Protection, http://fas.org/irp/offdocs/pdd/pdd-63.htm, (Erişim Tarihi 24 Mayıs 2016).

Wirtz, J. James, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy", NATO CCD COE Publications, Tallinn 2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf, (Erişim Tarihi 05 Mart 2016).

*United States Department of Defense*, About the Department of Defense (DoD)", http://www.defense.gov/About-DoD, (Erişim Tarihi 30 Mayıs 2016).

Yayla, Mehmet, "Hukuki Bir Terim Olarak Siber Savaş", http://portal.ubap.org.tr/App_Themes/Dergi/2013-104-1247.pdf, (Erişim Tarihi 17 Şubat 2017).