bilig
GÜZ 2017/SAYI 83
121-146

Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi*

Ali Burak Darıcılı**
Barış Özdal***

Öz

Rusya Federasyonu (RF), günümüzde siber uzayı Amerika Birleşik Devletleri (ABD) ve Çin Halk Cumhuriyeti (ÇHC) ile birlikte domine eden en önemli küresel güçlerden biri konumundadır. RF'nin siber kapasitesinin mahiyetini diğer iki devletten ayıran temel fark, siber uzayın sağladığı imkânları dış politik sorunlarının çözülmesi noktasında ve özellikle de komşuları ile ilişkilerinde bir baskı / yaptırım aracı olarak kullanmasıdır. RF'nin mevcut siber saldırı kapasitesi, Sovyet döneminin teknoloji mirasının da bir sonucu olarak, özellikle 2000'li yıllar ile birlikte ortaya konulan siber güvenlik ve savunma stratejileri belgeleri kapsamında geliştirilmiştir ve geliştirilmeye de devam edilmektedir. Bu bağlamda çalışmamızda ilgili Siber Güvenlik Strateji Belgeleri ile Rus Silahlı Kuvvetleri ve Rus İstihbarat Servisleri'nin siber yapısı analiz edilerek, RF'nin siber güvenlik kapasitesi tespit edilmeye çalışılmıştır.

Anahtar Kelimeler

Rusya Federasyonu, siber güvenlik, Siber Güvenlik Strateji Belgeleri, siber saldırı, siber kapasite

---

* Bu makale Prof. Dr. Barış Özdal'ın danışmanlığında Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Doktora Programı'nda A. Burak Darıcılı tarafından yazılan ve başarı ile savunulan *"Amerika Birleşik Devletleri ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi"* isimli doktora tez çalışmasından üretilmiştir.

** Dr., Uludağ Üniversitesi - Bursa / Türkiye
daricili@yahoo.com

*** Prof. Dr.,Uludağ Üniversitesi,İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü - Bursa / Türkiye
barisozdal@gmail.com

Giriş

RF'nin özellikle son yıllarda askerî kapasitesini geliştirmek için siber uzayın sağladığı imkânları kullanma yönünde büyük bir çaba gösterdiği ileri sürülebilir. Aslında RF'nin bu çabası Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) döneminden kalan teknoloji mirasının da etkisiyle 2000'li yıllar ile birlikte ortaya koyduğu planlamalarının olağan bir sonucudur.

Bu itibarla tarihsel olarak SSCB Dönemi'nden günümüze kadar ulaşan stratejik ve teknolojik aklın da etkisiyle RF, siber kapasitesini saldırı ve savunma yönünde genişletme eğilimindedir (bkz. Darıcılı 2017: 1-2). Örneğin, SSCB döneminde Komitet Gosudarst Bezopasbosti (KGB) operasyonlarının bir bölümünün, Batı bloğundaki bilimsel gelişmeleri yakından takip ederek teknolojik casusluk yoluyla bu buluşları SSCB'ye aktarmak için planlandığı bilinmektedir. Söz konusu istihbari planlama süreci, Soğuk Savaş Dönemi sonrasında Rus İstihbarat Servisleri (RİS)'nin dış operasyonlarında da zaman zaman belirleyici bir etken olabilmiştir (Wirtz 2015: 32).

Diğer yandan Sovyet teknoloji kültürünün, yeni teknolojik gelişmeleri sofistike askerî imkânları geliştirme adına kullanmaya yatkın ve becerikli olduğu da dikkate alınmalıdır. Bu itibarla SSCB Ordusu'na teknolojik gelişmeleri yeni nesil askerî doktrinlere adapte eden fikirlerin teşvik edildiği, söz konusu geleneğin günümüz Rus Silahlı Kuvvetleri (RSK)'nde de devam ettiği genel kabul görmektedir (Wirtz 2015: 33).

RF'nin güncel siber politikalarını etkileyen önemli bir diğer tarihsel ve kültürel faktör ise Rus siyaset kültürünün savaş olgusuna bakışı ile ilgilidir. Rus politik elitleri için savaş, tarih boyunca bir politik hareket tarzı ve şerefli bir imge olarak kabul edilmiştir (Wirtz 2015: 33). Bu yaklaşım ile birlikte Rus siyasi kültürü için, savaşın veya sıcak bir çatışmanın politik çıkarların uygulanması noktasında sıklıkla başvurulmaktan çekinilmeyen bir yöntem olarak geliştiği de ileri sürülebilir.

Bu bağlamda 1980'lerde SSCB Ordusu'nda görev yapan Mareşal Nikolai Ogarkov tarafından başlatılan *Revoluation in Military Affairs* programı, günümüz RF siber stratejisinin temeli olarak kabul edilebilir (bkz. Mowthorpe 2005: 137-144). Ogarkov, bu program ile birlikte kitlesel ve hantal bir yapıya sahip olan SSCB Silahlı Kuvvetleri'ni ağ teknolojileri ve teknik operasyonlar ile takviye edilen ve yönetilen daha etkin bir yapılanmaya kavuşturma-

yı hedeflemiştir. 1990-1991 Körfez Savaşı esnasında, Koalisyon güçlerinin kullandığı iletişim ve enformasyon tekniklerinin, Irak Silahlı Kuvvetleri'nin harekât kabiliyetine verdiği zararın yanı sıra Koalisyon güçlerine kazandırdığı hız, dönemin Rus askerî uzmanları tarafından da yakından izlenmiştir. I. Körfez Savaşı'ndaki sıcak çatışmaların dünya kamuoyuna adeta canlı olarak aktarılması da kitle iletişim araçlarının ortaya koyduğu imkân ve kabiliyetin anlaşılması noktasında Rus uzmanlarca dikkatle tecrübe edilmiştir. Fakat söz konusu dönemde Rus toplumun içinde bulunduğu ekonomik ve sosyal çöküntü nedeniyle Rus Ordusu'nun iletişim teknolojilerindeki gelişmeleri silahlı kuvvetlerinin mevcut yapısına adapte edebilmesi için 2000'li yılları beklemesi gerekmiştir (Heickerö 2015: 17).

1979-1989 arasında devam eden Afganistan Savaşı esnasında, SSCB Ordusu'nun psikolojik savaş tekniklerini uygulamada ve bölgedeki saha birlikleri ile Moskova riyaseti arasında etkili bir iletişim sağlama noktasında yeterince başarılı olamadığı görülmüştür (Heickerö 2015: 18). Benzer şekilde 1994-1996 yıllarındaki Çeçen Savaşı sırasında, internet haberleşmesi ve internet haberleşmesinin ortaya koyduğu imkânlar, savaş esnasındaki olayların RF aleyhine yansıtılması boyutunda çok etkili olmuştur (Bıçakçı 2013: 30). Bu kapsamda RF, uluslararası kamuoyu nezdinde Çeçen Savaşı'nda insanlık dışı yöntemlere başvuran, savaş suçu işleyen bir devlet olarak kabul edilmiştir (Heickerö 2015: 19). Söz konusu iki olayın olumsuz etkisiyle Rus güvenlik ve askerî bürokrasisinin *"askerî ağ teknolojileri"* ve "*enformasyon savaşı*" alanındaki planlamaları ve hazırlıkları hızla gelişmeye başlamıştır (Darıcılı vd. 2017: 21). Bu planlamaların ilk sonucu olarak NATO güçlerinin 1999'da eski Yugoslavya'daki Sırp güçlerini bombalamaya başlaması ile birlikte, Sırp ve Rus hackerlar tarafından NATO'ya, üye ülkelerin askerî haberleşme sistemlerine, ABD Savunma Bakanlığı'nın alt yapılarına siber saldırılar gerçekleştirmiştir (Bıçakçı 2013: 31).

RF günümüzde, siber espiyonaj, siber kontr/espiyonaj, dezenformasyon, elektronik savaş, psikolojik savaş ve propaganda, siber saldırı gibi faaliyet ve planlamaları kapsayan geniş bir enformasyon savaşı kabiliyetine sahip olma noktasında ciddi gayret içindedir (Wirtz 2015: 35). RF böyle etkin bir siber güce ulaşarak, siber uzaydaki yeniliklerin ortaya koyduğu imkân ve fırsatları, dış politika hedeflerine ulaşmak amacıyla kullanmayı planlamaktadır. Bu gücün sistematiğine ve planlamasına yönelik detaylar ise RF'nin

2000'li yılların başından itibaren yayımladığı resmi siber güvenlik doktrin ve savunma stratejileri belgelerinin analiz edilmesi ile ortaya konabilecektir.

Bu bağlamda makalemizde Siber Güvenlik Strateji Belgeleri ile RSK ile RİS'lerin siber yapısı analiz edilerek, RF'nin siber güvenlik kapasitesi tespit edilmeye çalışılmıştır.

RF'nin Siber Güvenlik Strateji Belgeleri

Siber uzay ve siber güvenlik ile ilgili analizlerin uluslararası literatürde yoğun olarak tartışılmaya başlandığı süreçte RF tarafından yayımlanan ve "*bilgi güvenliği*" kelimesinin kullanıldığı ilk resmî belge, 24.01.2000'de yürürlüğe giren "*National Security Concept of the Russian Federation*" (*Rusya Federasyonu Ulusal Güvenlik Konsepti*)'dir. Bu belgede genel ifadelerle, enformasyon güvenliğinin öneminin yanı sıra bu alanda RF'nin çıkarlarına yönelik iç ve dış tehditlerin varlığından ve bu tehditlere yönelik tedbirler alınmasından bahsetmektedir (http://www.mid.ru/en_GB/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/589768, 2000).

09.09.2000'de yayımlanan "*Information Security Doctrine of the Russian Federation*" (Rusya Enformasyon Güvenliği Doktrini) ise RF'nin siber güç olma hedefi yolundaki ilk temel doküman olarak kabul edilmektedir. Bu doktrin, RF'nin enformasyon güvenliği konusundaki yol haritasını, prensiplerini, amaçlarını ve konu kapsamındaki resmî görüşlerini genel hatlarıyla ortaya koymaktadır (Medvedev 2015: 55). Doktrin de ayrıca RF'nin enformasyon güvenliğinin sağlanması konusundaki ulusal çıkarlarının temelde ekonomik yapının, sivil toplumun ve politik sistemin korunması ile sağlanabildiğine işaret edilmektedir (https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf, 08.09.2017).

12.05.2009 tarihli "*Russia's National Security Strategy to 2020*" (*2020'ye Doğru Rus Ulusal Güvenlik Stratejisi*) ise tüm açıklığı ile güvenlik odaklı olması bakımından dikkat çekicidir. Bu Strateji Belgesi kabul edildiği tarih itibarıyla Rus güvenlik ve istihbarat servisleri için temel rehber ve plan niteliğine haiz önemli bir resmî dokümandır (http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020, 23.03.2016). Enformasyon güvenliği meselesi ile ilgili olarak anılan Strateji Belgesi'nde "*uluslararası siber yeteneğe sahip teknolojik silahların Rus ulusal güvenliği için tehdit oluşturduğu,*

bilgi teknolojilerindeki yeni gelişmelerin, önemli toplumsal, ekonomik ve kültürel yansımalara neden olduğu" yer almaktadır (http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020, 23.03.2016). Genel ve soyut olarak aktardığımız bu hususlardan da anlaşıldığı üzere Güvenlik Stratejisi Belgesi'nde güven artırıcı ve işbirliğini hedefleyen bir üslubun hâkim olduğu ve tercih edilen bu yumuşak savunmacı tarzın RF'nin siber güvenlik stratejilerinin gerçek amacının ve yapısının gizlenmesi hedefinden kaynaklandığı ileri sürülebilir (Giles 2012: 67).

2011'de 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 ise "*Rus Ordusu'nun ön siber savaş doktrini*" şeklinde tanımlanabilmektedir (Giles 2012: 68). Bu kapsamda belgenin siber uzayda Rus askerî varlığını ve hareketliliğini kabul eden ilk açık metin olduğu da ileri sürülebilir (https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf, 2011). Belge daha önceki diğer Rus belgelerinin aksine bilgiyi merkeze alan bir bakış açısıyla yazılmıştır. Siber faaliyetleri operasyonel bir mantık ve çatışma konsepti ile ele alan Belgede enformasyon savaşı; "*bilgi sistemlerine ve kaynaklarına zarar veren, toplumu ve hedef hükümetleri psikolojik savaş yöntemleri ile devirmeyi amaçlayan, politik, ekonomik ve kültürel sistemin altını oyan faaliyetler*" şeklinde tanımlanmıştır. (https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf, 2011) Defansif bir bakış açısının hâkim olduğu tespit edilebilen belgede, siber uzay ile ilgili olarak RSK'nın kendi enformasyon güvenliğini sağlamak zorunda olduğu ve bu sebeple planlamalar geliştirmesi gerektiği şeklindeki sorumluluklarına da vurgu yapılmaktadır (Giles 2012: 68).

09.11.2012'de RF Genelkurmay Başkanlığı görevine atanan Valery Gerasimov'un Şubat 2013'de Military Industrial Kurier Dergisi'nde yayınlanan "*The Value of Science in Prediction*" adlı makalesinde ortaya koyduğu askerî yaklaşım ise uluslararası ilişkiler alanında geniş yankı bulmuş ve "*Gerasimov Doktrini*" olarak tanımlanarak, tartışılmaya başlanmıştır (Medvedev 2015: 56). Gerasimov Doktrini ile ortaya konan prensipler dâhilinde RF; askerî niteliğe sahip olmayan yöntemleri, askerî kapasitesine dâhil ederek, daha az konvansiyonel güç (dolayısıyla da daha az insan kaybı ve maliyet) ile sıcak çatışma süreçlerini yönlendirmeyi ve yönetmeyi amaçlamıştır. Bu bağlamda

askerî bir müdahale öncesinde; hedef bölge, ülke, topluluk ya da devlete yönelik olarak siber saldırılar ile avantaj sağlanması, hedefin yıpratılması, psikolojik savaş yöntemleri ile baskı altına alınması, moralinin bozulması, savunma direncinin kırılması, kritik altyapılarına zarar verilerek, ekonomisinin zarara uğratılması ortaya konmak istenen hedefler arasında yer almaktadır (https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/, 24.03.2016).

Söz konusu makale hakkındaki tartışmaların günümüze kadar hararetli bir şekilde sürmesinin temel nedeni ise RSK'nın Gerasimov'un yaklaşımına uygun bir tarzda 2014'teki Ukrayna müdahalesi esnasında gösterdiği çok yönlü sıcak çatışma performansıdır. Diğer bir deyişle Ukrayna müdahalesi sırasında RSK, organize bir şekilde yönlendirilen ekonomik tedbirleri; siber saldırı yöntemlerini; yerel Rus azınlıklar ile koordineli bir şekilde gerilla faaliyeti gerçekleştiren özel piyade kuvvetlerinin operasyonlarını ve psikolojik savaş yöntemlerini kullanmıştır. Bu sebeple de Ukrayna Müdahalesi esnasında RF'nin savaş performansı "*hibrit savaş*", "*kirli savaş*", "*non-linearwar*", "*yeni savaş*" veya "*bulanık savaş konsepti*" şeklinde değerlendirilmiştir.

"*Concept of the Foreign Policy of the Russian Federation*" (RF Dış Politika Konsepti) ise 12.02.2013'de RF Devlet Başkanı Vladimir Putin'in onayı ile kabul edilmiştir. Esas itibariyle RF'nin **d**ış politikasının gelecek dönem hedefleri ile ilgili temel yaklaşım ve prensipleri ele alan bu Belgede, enformasyon ve siber güvenlik alanına ilişkin bazı tespit ve değerlendirmeler mevcuttur (http://archive.mid.ru//brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D, 24.03.2016). Bu kapsamda belgede, enformasyon alanında yaşanmakta olan yeni teknolojilerin ulusal güvenlik için tehdit olduğu vurgusu yapılarak, geleneksel uluslararası ilişkiler disiplini yaklaşımlarının ötesinde yeni enformasyon tekniklerinin ve kültürel metotlarının modern dış politika enstrümanları arasında kabul edilmesi gerektiği ifade edilmiştir(http://archive.mid.ru//brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D, 24.03.2016).

2013'de yayımlanan "*Basic Principles for State Policy of the Russian Federation in the Field of International Information Security*" (Rusya Federasyonu Devlet Politikasının Uluslararası Enformasyon Güvenliği Alanındaki Temel Prensipleri) ile RF'nin uluslararası enformasyon güvenliği alanındaki temel unsurları tespit edilmiştir. Belgenin temel amacının ise "*RF'nin bilgi ve tele-*

komünikasyon teknolojileri alanında dünyanın diğer önemli güçleri ile eşitliği sağlayabileceği şartların oluşturulması" olduğu açıklanmıştır. Belge ile RF'nin siber güvenlik alanında uluslararası konsensüsün oluşmasını hedefleyen ve böylelikle de siber uzayı düzenleyen, internet ve bilgi güvenliği alanında kurallar ortaya koyan ve iş birliğinin geliştirilmesini isteyen bir dış politika sürdürme niyetinde olduğu ilan edilmektedir (https://ccdcoe.org/cyber-security-strategy-documents.html, 2013).

Yukarıda genel ve soyut olarak aktardığımız belge ve doktrinler dâhilinde RF'nin geliştirmeye devam ettiği Siber Güvenlik Stratejisi'nin tüm detayları ile analiz edilmesi için siber uzay alanı kapsamında faaliyetleri ile ilgili olarak Rus istihbarat ve güvenlik kuruluşları da bizce ele alınmalıdır. Zira ancak bu tarz bir analiz ile büyük resim daha kolay anlaşılabilir.

Rus Silahlı Kuvvetleri ile Rus İstihbarat Servisleri'nin Siber Kapasiteleri

Rus Federal Güvenlik Servisi (Federalnaya Slujba Bezopasnosti / FSB), Rus İstihbarat Servisi (SluzhbaVneshney Razvedki / SVR) ve Rus Askerî İstihbarat Direktörlüğü (Glavnoye Razvedyvatel'noye Upravleniye / GRU)'nün gerek tek başlarına sahip oldukları siber kapasiteleri gerekse de Rus kriminal örgütleri ile olan illegal bağlantıları, RF'nin siber savunma ve saldırı kapasitesini belirleyen temel faktörlerdendir. Bu servislerden FSB ve SVR, RF Devlet Başkanı'na doğrudan bağlı durumdayken, GRU Savunma Bakanlığı'nın bir parçası konumunda ve RF Silahlı Kuvvetleri emrinde görev yapmaktadır (Heickerö 2015: 27).

Daha ayrıntılı bir biçimde incelemek gerekirse FSB, SSCB döneminde faaliyet gösteren ÇEKA, NVD ve KGB'nin yerini alan ve iç güvenlik alanında faaliyet gösteren bir gizli servistir. Bir iç güvenlik servisi olarak FSB'nin faaliyetleri iki boyutlu olarak düşünülmelidir. FSB'nin ilk görevi ülke genelinde devlet güvenliği aleyhine sürdürülen faaliyetler hakkında istihbarat toplamaktır (Gady vd. 2010: 5). Örneğin, RF'deki ayrılıkçı Çerkez / Çeçen gruplarının, cihat yanlısı selefi veya tekfiri terör örgütlerinin veya organize suç odaklarının faaliyetlerini izlemek, takip etmek ve haklarında istihbarat toplamak FSB'nin görevidir. FSB'nin bir diğer görevi ise RF'ye yönelik olarak sürdürülmekte olan espiyonaj faaliyetlerine karşı koymaktır. Bu karşı koyma faaliyeti kontr/espiyonaj çalışması olarak adlandırılır ve RF aleyhine dış istihbarat servisler aracılığıyla sürdürülen subversif (yıkıcı/bölücü)

operasyonların da engellenmesi amacını içerir. Bu kapsamda, RF'ye yönelik siber saldırılara karşı koymak ve temelde ülkenin siber güvenliğini sağlamak, FSB'nin görevidir (http://www.cicentre.com/?page=191, 27.03.2016).

FSB'nin siber güvenlik alanındaki diğer bir sorumluluğu ise ülke genelindeki Rus vatandaşlarının ve yabancıların telekomünikasyon iletişim bilgilerinin istihbar olunan bilgiler kapsamında takip edilmesidir. Bu görev kapsamında FSB, Rus GSM ve telefon şirketlerinin yasal bir zorunluluk olarak kurmak zorunda oldukları, RF'deki internet ve analog haberleşmesini takip eden ve bir nevi denetleme sistemi şeklinde tesis edilmiş olan "*Operatif Denetleme Faaliyetleri Sistemi*" (System for Operative Investigative Activities / SORM)'nin kontrolünü 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 (Carr 2011: 318). Ayrıca önemle belirtmek gerekir ki FSB, siber güvenlik alanındaki çalışmalarının yanı sıra diğer tüm faaliyetlerini SVR ile koordinasyon içinde sürdürmektedir (bkz. Staar 2010: 1-10).

SVR de KGB'nin devamı olarak RF'nin ülke dışındaki espiyonaj faaliyetlerini yürütmek amacıyla kurduğu dış istihbarat servisidir. SVR, RF'nin dış istihbarat ihtiyaçlarının karşılanmasında, GRU ile birlikte temel aktör konumundadır. SVR, hedef aldığı devlete yönelik askerî, siyasi, biyografik, ekonomik, sosyal, ulaştırma, iletişim, bilim ve teknoloji konularında istihbarat toplamaktadır. Siber güvenlik stratejisi açısından ise RF'nin bir ülkenin bilim ve teknoloji kapasitesini hedef alan siber casusluk operasyonlarını planlamak 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 (bkz. Heickerö 2015: 30-32).

GRU, Rus Genelkurmayı'na bağlı olarak faaliyet gösteren askerî istihbarat teşkilatıdır. SSCB zamanında Kızıl Ordu'ya bağlı olan GRU, RSK'nin büyüklüğü kapsamında RF'nin en geniş sayı ve kapasiteli istihbarat teşkilatıdır.

GRU, askerî ve dış istihbarat konularının yanı sıra ülke güvenliği ile ilgili her alanda istihbarat toplama yetkisine sahiptir. Siber güvenlik açısından GRU'nun temel görevleri Rus askerî kapasitesini hedef alan dış servis kaynaklı siber operasyonlara karşı kontr/espiyonaj faaliyeti yürütmek ve imkân bulunması hâlinde hedef ülkenin askerî kapasitesine yönelik siber casusluk operasyonları planlamaktır (http://www.cicentre.com/?page=191, 27.03.2016). Stratejik Füze Birlikleri'nin faaliyetlerinin sürdürülmesinin yanı sıra ülkeye yönelik siber saldırılara karşı koymak üzere kurulmuş olan "Computer Emergency Response Team"lerin kontrolü de GRU'nun diğer Rus istihbarat ve güvenlik kuruluşları ile koordineli olarak gerçekleştirdiği görevler arasındadır (Heickerö 2015: 27).

Bu noktada, GRU'nun RSK'nın 2014 yılındaki Ukrayna müdahalesi esnasında gösterdiği çok yönlü sıcak çatışma performansına yaptığı katkı ve bu katkının başarısı nispetinde RİS'ler arasında meydana gelen rekabet, RF'nin siber kapasitesinin net bir şekilde ortaya konulması amacı kapsamında ayrıca irdelenmelidir. GRU'nun 2008 yılındaki Gürcistan Müdahalesi esnasındaki başarısızlığı, bu istihbarat örgütünün diğer RİS'lere kıyasla itibarını ciddi biçimde sarsmıştır. Söz konusu kötüye gidiş 2011 yılında Igor Sergun'un GRU direktörü atanması ile sona ermiştir. Bu atama, GRU'nun yönetiminin ve sahip olduğu operasyonel kapasitenin kontrol edilmesi amacıyla FSB tarafından baskı altına alındığı bir tarihte meydana gelmesi bakımından V. Putin'in oldukça kritik bir kararı olarak okunmalıdır. I. Sergun, diğer RİS'lerde görev yapan rakipleri tarafından; *"iş yapmaktan ziyade, saray dengelerini gözeterek makam sahibi olmuş bir şahsiyet*" olarak ifade edilse de GRU anılanın direktörlüğü altında, özellikle Ukrayna Müdahalesi öncesi ve esnasında gerek siber operasyonların planlanmasında gerekse de özel kuvvet birlikleri ile Rus yanlısı ayrılıkçıların faaliyetlerinin koordinasyonunda son derece başarılı olmuştur. Sergun direktörlüğündeki GRU, Putin'in iktidarını sürdürme noktasında RF'deki istihbarat servisleri arasında dengeyi gözeten ve hiçbir servisin diğerine üstün olmaması kuralına bağlı olan siyasetini, Ukrayna Müdahalesi esnasında kendisine verilen imkân ve kabiliyetleri en üst seviyede kullanmak suretiyle elde ettiği popülerlik ve güç sayesinde ciddi biçimde sarsmıştır (bkz., Galeotti 2016: 6-13). Putin'in söz konusu siyasetinde meydana gelen bahse konu dengesizlik ise 2015 Ocak ayında Sergun'un Moskova'da kalp krizi sonucu ani bir şekilde ölmesi ile sona ermiştir (Meriç 2015). Diğer bir ifade ile vurgularsak, Sergun'un ölümü sonrasında

GRU'nun diğer istihbarat servislerine kıyasla Ukrayna Müdahalesi sonrasında elde ettiği üstünlük ortadan kaybolmuş ve Putin'in istihbarat servisleri arasında gözettiği denge yeniden tesis edilmiştir. Bu gelişmeyi destekleyen bir diğer olay ise Ukrayna İstihbarat Servisi ile irtibatlı bir kaynağın, FSB'nin 2015 Ocak ayı sonrasında Ukrayna'nın doğusunda yer alan RF yanlısı ayrılıkçı gruplar ile tekrar operasyonel planlamalara giriştiğini bildirmesidir (Meriç 2015). Bu tek örnekten de anlaşıldığı üzere, Sergun'un sahneden çekilmesi ve akabinde Putin'in yaptığı yeni atamalar ile birlikte RİS'ler arasındaki güç dengesi yeniden tesis edilmiştir (Galeotti 2016: 12-19).

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 itibarıyla 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 "*Federal İletişim ve Enformasyon Ajansı*" (Federal Agency of Government Communications and Information / FABSİ)'nı 2003'de lağvederek, bu kuruluşun yetki ve sorumluluklarını FSB, SVR, RF Savunma Bakanlığı ve "*Federal Koruma Servisi*" (Federalnaya Sluzhba Okhrany / FSO) arasında dağıtmıştır. FABSİ'nin kapatılmasının en önemli nedeni ise kurum içerisindeki yolsuzluk ve organize suç örgütleri ile bağlantılı yapılanmalardır. FSO'nun siber güvenlik alanındaki temel görevi, RF'nin ilgili kurumları ve yöneticileri arasındaki üst düzey ve gizlilik içeren iletişimin güvenli bir şekilde sürdürülmesini denetlemek ve yönetmektir. Doğrudan RF devlet başkanına bağlı olarak faaliyet yürütür. FSO'nun ayrıca, 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 (bkz. Heickerö 2015: 28-29).

Ayrıca, RF 2010'da enformasyon ve bilgi teknolojileri alanında çalışma yürütmek amacıyla Savunma Bakanlığı bünyesinde bir "*bakan yardımcılığı*" pozisyonunu da tesis etmiştir (bkz. Fayutkin 2012: 1-4). 2013'de alınan bir karar ile de RSK bünyesinde bağımsız bir siber savaş birimi kurulmasını planlama kapsamına almıştır (Vasudevan 2013).

Bu gelişme ile ilgili olarak, 2014 Kasımı'nda açıklama yapan RF Savunma Bakanı Sergei Shoigu; "*Rus Ordusu'nun siber tehditlere karşı koymak amacıyla bünyesinde faaliyet gösterecek olan bağımsız bir yapılanmaya gittiğini, bu planlama kapsamında Rus hükûmeti olarak 500 milyon $ tutarında bütçe ayırdıklarını, anılan oluşumun siber tehditler ile mücadelenin yanı sıra yurt dışı kaynaklı iletişimin gözetlenmesi, toplanması ve denetlenmesi görevini de sürdüreceğini, bu nedenle de yazılım uzmanları ile yabancı dil bilen personele ihtiyaç duyduklarını*" belirtmiştir (Gerden 2014). Diğer yandan, RF Silahlı Kuvvetleri bünyesindeki söz konusu siber biriminin 2017 yılı sonu itibariyle operasyonel faaliyetlerine başlayacağı tahmin edilmektedir (State Security Magazine 2014).

Yukarıda aktardığımız bilgilerden de anlaşıldığı üzere Rus sivil ve askerî istihbarat servisleri, haber toplama yöntemi olarak geleneksel HUMINT (Human Intelligence / İnsan Kaynaklı Dayalı 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 (bkz. Hagestad 2013: 18-22). 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 yapılan yatırımlar ile ise RF'nin bu amaca hizmet eden siber kapasitesinde ciddi bir artış söz konusu olmuştur (bkz. Hagestad 2013: 22-25).

RF'nin Siber Alanının Yapısal Özellikleri

Bir devletin siber alanın yapısal özellikleri, o devletin internet ve ağ teknolojilerini düzenleyen ulusal kanunlar, söz konusu kanunların yaptırım gücü ve etkisi ile bu sektörlerde faaliyet gösteren şirketlerin yapısı ve teknolojik kapasiteleri ile birlikte değerlendirilmelidir. Bu kapsamda, RF'nin ulusal alanının detaylı bir şekilde analiz edilmesi, RF'nin siber güvenlik stratejisinin ve kapasitesinin anlaşılması noktasında oldukça önemlidir.

V. Putin'in devlet başkanı olmasında sonra, RF'nin ekonomik ve ticari yapısının giderek bir nevi nepotik kapitalizme (*akraba-dost kapitalizmi*) doğru evirildiği, bu yapı içinde devlet ve özel sektör arasında sıkı bir birliktelik

söz konusu olduğu literatürde genel kabul gören bir yaklaşımdır. Bu özellik Rus siber coğrafyasının yapısını da etkilemiş ve devlet ile özel sektör sıkı bir işbirliği içine girmiştir (Medvedev 2015: 31). Örneğin RF'de, mobil telefon sektörünün % 92'si 4 şirket, telekomünikasyon sektörünün ise % 62'si 6 şirket tarafından kontrol edilmektedir ve bu şirketlerin faaliyetleri de belirtilen haliyle akraba-dost kapitalizminin özellikleri kapsamında değerlendirilebilir. RF'nin bu şirketler üzerinde ciddi bir hükümet baskısı ve denetimi söz konusu olmakla birlikte, Rus donanım ve yazılım teknolojileri, telekomünikasyon, data ve iletişim altyapısı önemli ölçüde dış kaynaklı dizayn ve yapıya sahiptir (Kelly 2014).

Dışa bağımlı yapının bir stratejik zafiyet yarattığının farkında olan Rus güvenlik ve istihbarat bürokrasisi, bu yapıyı millileştirmek adına bazı girişimler içindedir. Bu kapsamda, RF Devlet Başkanlığı, işletim sistemleri ve yazılım altyapısında Microsoft başta olmak üzere diğer ABD orijinli şirketlere olan bağımlılığın azaltılmasını amaçlayan planlamalarını tamamlamıştır (bkz. Fayutkin 2012: 1-4).

Rus bilgi güvenliği (anti-virüs) alanında faaliyet gösteren en önemli şirket ise bilindiği üzere Kaspersky'dir. Bu firma, McAfee, Norton ve Symantec şirketleri ile anti-virüs sektöründe küresel alanda ciddi bir rekabet içinde olup, dünya genelinde 400 milyona yakın müşterisi olduğu tahmin edilmektedir (Kaspersky Company 2016). Kaspersky'nin RİS ile yakın irtibatının olduğu, bu şirketin ilk kurucusu olan ve şirkete adını veren Eugene Kaspersky'nin de eğitimine KGB destekli bir bilim akademisinde başladığı iddia edilmektedir (Shachtman 2012).

RF'nin ulusal internet kullanımına yönelik tedbirleri bir süre göreli olarak daha liberal bir tarzda gelişmiştir. Bu liberal ortamın da yardımıyla milliyetçi Rus hackerlerin Estonya ve Gürcistan'a yönelik siber saldırlar esnasında oldukça etkin rol oynadıkları ileri sürülmektedir. Rus çıkarlarını hedef almadıkları sürece genelde bir denetime tabi tutulmayan ve adi suçlar ile ilgili olarak faaliyet gösteren kriminal grupların faaliyetleri, 2012'ye kadar aktif bir tarzda gerçekleşmiştir. 2012'de ise RF Devlet Başkanlığı seçimleri sırasında sosyal medyanın Putin karşıtı faaliyetler için uygun ve etkili bir zemin oluşturmasının etkisiyle internetin denetlenmesi noktasında bazı tedbirler alınmaya başlamıştır (Kelly 2014).

Bu kapsamda siber saldırıların ve siber kriminal operasyonların planlanması noktasında hayati öneme sahip "*anonim*" (tor) bilgisayarların ve "*proxy*" servislerinin kontrol edilmesi amacıyla Putin'in talimatıyla RF İçişleri Bakanlığı 2014 Haziranında 3.9 Milyon Ruble bütçe ayırmıştır (BBC News 2014). Bu bağlamda FSB yöneticisi Alexsandr Bortnikov yaptığı açıklamada: "*tor servislerinin siber suçlar ve çocuk porno dağıtıcıları tarafından sıklıkla kullanıldığını, devlet olarak bunu engelleyeceklerini ve bu servislerin tümünü kapatacaklarını*" beyan etmiştir (Türk-İnternet Haber Portalı, 26.08.2013). Ayrıca, akıllı cep telefonları üzerinden internete bağlanılmasının denetlenmesi amacıyla da cep telefonlarında kullanılan sim kartların ve kamuya açık alanlarda kablosuz ağ girişi (wi-fi) girişi yapan akıllı telefonların kayıt altına alınmasına yönelik bir yasa da 2014 Ağustosu'nda kabul edilmiştir (Medvedev 2015: 39). 2014 Mayısı'nda kabul edilen bir başka yasayla da internet üzerinden kolaylıkla açılabilecek bloglara, günlük olarak 3000 kişi tarafından giriş yapılabilecek bir kapasiteye ulaşmaları hâlinde, Federal Komünikasyon, İletişim, Teknoloji ve Medya Denetleme Kurumu (Roskomnadzor)'na kayıt olma zorunluluğu getirilmiştir (Birnbaum 2014). Söz konusu yasayla ayrıca blog yazarlarının takma ad kullanmaları yasaklanmış, yazdıkları tüm yazıların doğruluğunu delillendirmeleri zorunluluk haline getirilmiş ve bloglara ziyaretçi giriş (log) kayıtlarını 6 ay süreyle arşivlemeleri mecburiyeti getirilmiştir (Türk-İnternet Haber Portalı, 08.05.2014).

RF ayrıca, siber güvenliğini sağlamak amacıyla 01.09.2016'da "*Rusya Bilgi Yerelleştirmesi*" (Russia Data Localizitaion) kanunu kabul etmiştir. Bu kanuna göre yabancı internet sitelerinin ve yabancı şirket internet sitelerinin RF kanunlarına dâhil olması, RF merkezli faaliyetlerinin "*ru, .su, .moscow*" gibi domain adlarını kullanmaları ve internet sayfalarının Rusça versiyonlarını da hazırlamaları kural altına alınmıştır. Bu kapsamda, RF vatandaşlarına yönelik kişisel bilgileri verdiği hizmet gereği elinde tutma imkânına sahip olan tüm şirketlerin, bu verileri RF resmî kurumlarının denetimindeki bir fiziksel arşiv ortamına aktarmaları da sıkı bir denetim tabi tutulmuştur (Bloomberg Tecnology News Portal, 05.08.2016).

RF'nin siber güvenlik alanında uygulamaya koyduğu belki de en önemli tedbir ise SORM sistemidir. SORM sistemi RF'deki internet ve analog haberleşmesini takip eden ve bir nevi denetleme sistemi şeklinde tesis edilen bir uygulamadır. SORM'un ilk versiyonu 1990'lı yıllarda geliştirilmiştir.

Daha sonra ise teknolojik gelişmelere bağlı olarak iki yeni versiyonu daha tesis edilmiştir. SORM'un kontrolü görevi de FSB'ye verilmiştir (bkz. Giles 2012: 8-9). Mahiyeti ve yetkinliği tam olarak bilinmemekle birlikte, SORM sistemi ile FSB'nin sadece RF sınırları içinde değil, ülke dışında gerçekleşen her türlü internet, sabit telefon ve cep telefonu iletişimi üzerinde etkin bir denetim kurduğu tahmin edilmektedir (Saldatov vd. 2013).

Putin'in sosyal medya imkânları kullanılarak sürdürülmesi olası siber tehditlere karşı aldığı en önemli tedbir ise Rus orijinli sosyal medya şirketlerinin RF'de kullanılmasını teşvik etmek ve bu şirketlerin yönetiminde kendisine yakın şahısların yer almasına özel önem vermektir. Bu önemin bir sonucu olarak da e-posta hizmeti veren "mail.ru"; "google.com" ile benzer hizmetleri sağlayan "yandex.com"; "facebook.com" ile aynı işlevi gören "vkontakte.ru" ve "odnaklassniki.ru" isimli şirketlerin sadece RF'de değil eski SSCB ülkelerindeki pazar payları oldukça yaygınlaşmıştır. Bu durum ise Putin iktidarına, RF'de ve eski SSCB üyesi ülkelerde sosyal medya merkezli planlanabilecek olası muhalif toplumsal hareketlerin kontrolü ve RF lehine propaganda faaliyetleri sürdürülmesi noktasında önemli avantaj sağlamaktadır (bkz. Thoburn 2015: 80-89).

Aktardığımız bilgilerden de anlaşılacağı üzere, 2000'li yıllar ile birlikte başlayan planlamaların bir sonucu olarak, RF'nin günümüzde gerek istihbarat servisleri ve bu servisler ile bağlantılı illegal organizasyonların faaliyetleri gerekse de silahlı kuvvetlerinin sahip olduğu siber imkânlar kapsamında önemli bir siber güç olarak siber uzayı domine edebildiği ortadadır. RF'nin söz konusu siber gücüne özellikle 2010 yılından sonra, Moskova merkezli uluslararası haber ajansları ve sosyal medya olanaklarından da geniş bir biçimde istifade eden enformasyon savaş kabiliyetleri de eklenmiştir. Tüm bu siber imkânlar ile birlikte RF, sahip olduğu siber gücü uluslararası ilişkilerde sorun yaşadığı devletlere karşı bir baskı ve zorlama aracı olarak kullanmaktan çekinmemekte ayrıca da bu tarzda planlanmış olan siber saldırılarını etkili ve yıpratıcı bir enformasyon savaşı ile destekleyebilmektedir.

RF Kaynaklı Olduğu İddia Edilen ve Enformasyon Savaşı Enstrümanları Kullanılarak Yürütülen Siber Saldırılar

2007'de Estonya'ya ve 2008'de ise Gürcistan'a yönelik olarak RF tarafından yürütüldüğü iddia edilen siber saldırılar, 2010 yılı öncesinde RF'nin eriştiği

siber kapasiteyi göstermesi bakımından oldukça önemlidir (bkz. Darıcılı 2017: 5-8). Öte yandan, RF tarafından 2014'de Ukrayna ve Türkiye'ye yönelik olarak yürütüldüğü iddia edilen siber saldırıları ise Moskova merkezli uluslararası medya kuruluşları tarafından sürdürülen küresel propaganda amaçlı yayın politikaları ve faydalanılan sosyal medya imkânları ile birlikte geniş bir enformasyon savaşı mahiyetine de sahiptir.

Bu bağlamda, Ukrayna Devlet Başkanı Viktor Yanukovich'in 2014 Şubatı'nda görevden uzaklaştırılması, RF ile Ukrayna arasındaki hibrit savaş özelliği de içeren sıcak çatışma sürecinin başlangıcı olarak kabul edilebilecektir. Bilindiği üzere Ukrayna ve RF arasında Kırım nedeniyle bir süredir devam eden gerginlik neticesinde, RF Parlamentosu 01.03.2014'de Kırım'a yönelik askerî güç kullanımına izin veren bir yasayı onaylamıştır. Daha sonra, Ukrayna İç Güvenlik Birimi SBU'nun Başkanı Valenty Nalyvaichenko tarafından 2014 Şubat ayı sonundan itibaren, Ukrayna mobil telefon iletişim ve internet altyapılarının saldırıya uğradığı ve büyük oranda çöktüğü, özellikle Ukraynalı bürokratlarla milletvekillerine ait akıllı cep telefonlarının tamamının "hack"lendiği ifade edilmiştir (Medvedev 2015: 27). Rus yanlısı bir hacker grupları olan "*CyberBerkut*" tarafından, Ukrayna Silahlı Kuvvetleri'ne, Ukrayna resmî sitelerine, Ukrayna ile ilgili faaliyet gösteren NATO'nun internet erişimlerine ve Ukrayna medya kuruluşlarına yönelik olarak "*DDoS*" saldırıları da düzenlenmiştir (Lee 2015). Saldırılarda kullanılan "*snake/Uroburos*" yazılımı, özellikle Ukrayna'nın resmi kurumlarına yönelik siber ataklarda son derece etkili olmuştur (Weedon vd. 2014).

Bu siber saldırılar ile eş zamanlı olarak RİS tarafından sosyal medya imkânları kullanmak suretiyle kışkırtılan Rus yanlısı sivil protestocular, Sivastopol'da şiddet içermeyen sokak eylemleriyle RF'ye bağlanma taleplerini beyan eden mitingler düzenlemeye başlamışlardır. Bu süreçte özellikle 16-28.03.2014 tarihleri arasında yoğunlaşacak şekilde, Ukrayna'nın resmî mobil telefon şirketi olan Ukrtelecom'un altyapısını çökertilmiş, bu sayede de Kırım'daki mobil telefonların sıcak çatışmanın ilk günlerinde kullanılması engellenmiş, internette kısmi bir yavaşlama sağlanmış, kritik altyapıları felç eden siber saldırılar organize edilmiş, Sivastopol limanındaki Rus savaş gemilerinden Kırım'daki televizyon ve radyo yayınlarını kesecek elektronik karıştırmalar yapılmış ve "*kimliği belirsiz kişilerce*" Kırım'daki tüm fiberoptik kablo altyapısı zarara uğratılmıştır (Gürcan, 2014). Akabinde, Rus kitlesel

medya organlarının yayınlarının yanı sıra RİS'lerin özellikle sosyal medya manipülasyonları ile provoke ettiği Rus yanlısı milis güçler, 2014 Nisan ayı sonuna kadar Lugansk ve Donetsk Bölgeleri'nin büyük bölümünü ele geçirmişlerdir 23.12.2015'de Ukrayna'nın Prykarpattyaoblenergo Bölgesi'nde bulunan bir enerji santraline yönelik olarak siber saldırı düzenlenmiş ve bu nedenle ilgili bölgede bir süre elektrik kesintisi yaşanmıştır. SBU tarafından konuyla ilgili olarak yapılan açıklamada "*kesintilerin siber bir saldırı nedeniyle gerçekleştiğinin düşünüldüğü, saldırının arkasında RF'nun olabileceği ve konunun araştırıldığı*" kamuoyuna duyurulmuştur (Reuters, 31.12.2015). RF ise konuyla ilgili olarak bir açıklama yapmamıştır.

Ukrayna Krizi esnasında RF, Rus yanlısı milis güçleri provoke edilmesi noktasında etkili bir şekilde sosyal medya olanaklarını kullanmıştır. Sosyal medyanın etkili bir enformasyon savaş tekniği olarak kullanabilmesinde, sosyal medya olanaklarına ulaşmanın herkes için kolay, hızlı, coğrafi sınır tanımayan yapısının etkili olduğu açıktır (http://www.stratcomcoe.org/social-media-tool-hybrid-warfare, Mayıs 2016: 24). Kriz kapsamında sosyal medya imkânlarının kullanılması, ilk etapta RİS ile irtibatlı kuvvetli ve etkili bir troll ve blogger ağının çeşitli ulusal ve uluslararası sosyal medya platformlarında (*yandex.com, youtube.com, facebook.com, vkontakte.ru, odnaklassniki.ru, twitter.com, whowho.com.ua, novorus.info, novorossia.ru vb*.) Ukrayna'daki Rus azınlığın baskı gördüğü şeklindeki dezenformasyon haberlerini profesyonel imkânlarla hazırlandığı belli olan görsel dokümanlar ile birlikte Rus halkına servis etmesi ile başlamıştır. Böylelikle Rus ve uluslararası kamuoyunun söz konusu müdahale lehine pozisyon alması teşvik edilmiştir. Bahse konu görsel materyaller ise özellikle Ukrayna'da yaşayan Rus azınlık mensubu olan yaşlı, çocuk ve kadınların Ukrayna güvenlik güçlerinin taciz, dayak, tecavüz gibi kötü muamelesine uğradıklarını ispatlamaya yönelik öğelerle hazırlanmıştır. Daha sonra bu yayınlara, ABD ve Batı karşıtlığı propagandaları temelinde, Ukrayna Hükümeti'nin de söz konusu dış mihraklarla işbirliği yaptığı şeklindeki ifşalar eklenmiştir. Bu doğrultuda önceden RİS tarafından kayıt altına alındığı belli olan kimi Ukraynalı politikacıların (Ukrayna Eski Başbakanı Yulia Timoşenko ve Güvenlik Dairesi eski Müsteşarı Nestor Surfiç) RF, Rus halkı ve Rus siyasiler aleyhine yaptıkları telefon görüşmeleri / tapeleri kamuoyuna sızdırılmıştır (bkz. http://www.stratcomcoe.org/social-media-tool-hybrid-warfare, Mayıs 2016: 5-20).

Genel hatlarıyla aktardığımız tüm bu menfi propaganda faaliyetleri özellikle 2013'de kurulan Bugün Rusya (Russia Today / Rossiaya Segodnya) ile

2014'de kurulan Sputnik Multimedya Haber Grubu'nun yayınları ile şiddetli bir şekilde desteklenmiştir. Bu kapsamda, Sputnik'in, Ukrayna Krizi sırasında RF'nin ortaya koyduğu hibrit savaş yönteminin propaganda ayağını önemli ölçüde üstlendiği açıktır. Hatta Ukrayna Müdahalesi'nden çok önce Sputnik'in Ukrayna Hükümeti aleyhine ve bölgedeki Rus azınlığı da kışkırtacak şekildeki bir yayın akışı başlamıştır (bkz. http://www.stratcomcoe.org/social-media-tool-hybrid-warfare, Mayıs 2016: 20-24). Bu itibarla RF'nin 2013-2015 yılları arasında sürdürdüğü enformasyon savaşının maliyetinin yaklaşık 2 Milyar $ olduğu da iddia edilmiştir. (http://www.stratcomcoe.org/social-media-tool-hybrid-warfare, Mayıs 2016: 25). Benzer bir durum, Suriye İç Savaşı esnasında söz konusu Rus haber ajansları tarafından sürdürülen yayın politikası için de geçerlidir. Zira bilindiği üzere Suriye İç Savaşı'nın ilk yıllarından bu yana Rus haber ajansları Esad Rejimi'ne doğrudan destek vererek, adeta küresel ölçekteki sesi olmuştur.

Bu kapsamda irdelenebilecek bir diğer örnekte RF ve Türkiye arasında yaşanan krizdir. 24.11.2015 sabah saatlerinde Türk F-16'larının, hava sahasını ihlal eden bir Rus Su-24 uçağını düşürdüğü haberi tüm dünyada şok etkisi yaratmıştır. Bu olay kısa sürede derinleşerek, Türkiye ve RF arasında günümüzde çok ciddi boyutlara ulaşan siyasi gerginliğinde başlangıcını oluşturmuştur. Bu siyasi gerginlik, 14.11.2015'de saat 12.00 itibariyle Türkiye'ye yönelik olarak "*DDoS" saldırıları ile yeni bir aşamaya taşınarak, iki ülke ilişkilerindeki gerginliğin derinleşmesine neden olmuştur. Söz konusu siber saldırı ile ".tr" uzantılı adların tutulduğu sistemin kullandığı bant genişliği hedeflenerek, Türkiye'nin bankacılık ve finans, kamu kurumları, e-devlet sistemini teşkil eden kritik altyapılarının yıpratılması amaçlanmıştır. (*Türk-İnternet Haber Portalı, 20.12.2015). Bununla birlikte, "DDoS" saldırılarının gerçek planlayıcısının kimliği ile ilgili olarak hiçbir zaman net bir delillendirme yapılamayacak olmasına rağmen, Türkiye'ye yönelik saldırının en az 400.000 sitenin etkileyecek kapasitede olması, bu sitelerin ise e-devlet, üniversite, askerî ya da yerel şirket siteleri şeklinde hedeflenmesi, RF ile Türkiye arasında uçak düşürülmesi olayına bağlı olarak süregelen gerginlik, saldırılar ile Türkiye'deki tüm sistemin değil de sadece ".tr" uzantılı adların hedeflenmesi, saldırıların sadece mesai saatleri içinde gerçekleşmesi, RF'nin bu ve benzeri saldırılar kapsamındaki kabarık sicili, saldırının arka planının RF bağlantılı bir şekilde planlama ihtimalini kuvvetlendirmiştir (The Telegraph Online News, 18.11.2015).

Türkiye ve RF arasında uçak düşürülmesi ile başlayan gerginlik esnasında, başta Sputnik olmak üzere Rus haber ajansları tarafından Türkiye'ye yönelik yıpratıcı bir propaganda faaliyeti de sürdürülmüştür. Sputnik merkezli olan ve sosyal medya imkânlarından da geniş bir biçimde istifade eden bu propaganda faaliyetleri, süreç içinde Türkiye'nin cihat yanlısı Selefi gruplara yardım ettiği şeklindeki agresif bir yıpratma faaliyetine evrilmiştir. Hatta Sputnik, Adalet ve Kalkınma Partisi (AK Parti) ve Cumhurbaşkanı Recep Tayyip Erdoğan aleyhtarlığını merkeze koyarak, Türkiye'ye yönelik olumsuz yayın politikasını 2016 Mart ve Nisan aylarında zirveye çıkarmıştır. Bu noktada, Sputnik'in 01.05.2016'da maksatlı ve yönlendirici "*Rusya, BM'ye Türkiye-IŞİD Bağlantısını Gösteren Belgeleri Sundu" (Sputniknews Haber Portalı, 01.04.2016) başlıklı haberinin, Türkiye'de bazı medya gruplarınca da kullanılmasının dikkat çekici olduğu ortadadır.* Bu haberle eş zamanlı bir şekilde, Türkiye'yi DAEŞ ile irtibatlı göstermenin de ötesinde, RF yetkilileri tarafından bu örgütle kimi üst düzey Türk siyasetçilerin petrol ticareti yaptığını iddia eden bazı beyanlar da gündeme getirilmiştir. Benzer şekilde Rus halkını Türkiye aleyhine etkilemek amacıyla Rus ulusal medya organlarında Türkiye'yi DAEŞ ile irtibatlı gösteren ve uçak düşürülmesi olayında Türkiye'yi suçlayan haberlere de yer verilmiştir. (bkz. Yılmaz 2016: 257-258). Ulusal ve uluslararası Rus medyasında yer alan haberler, sosyal medyada yapılan olumsuz paylaşımlar ile birlikte, Türkiye kısa sürede yapılan tehdit değerlendirmesi anketlerinde Rus halkı gözünde "*1 numaralı düşman ülke" konumuna ulaşmıştır. Türkiye'ye yönelik bahse konu enformasyon savaşının arka planın da yer alan neden ise Putin'in uçak düşürülmesi olayını fırsata çevirerek, iç politika da güç kazanmak amacıyla Rus toplumunda ki tarihi Türk düşmanlığını körüklemek istemesidir (*bkz. Yılmaz 2016: 261-267).

Türkiye'nin RF tarafından kendisine yönelik olarak başlatılan söz konusu enformasyon savaşına cevabı ise genel olarak tansiyonun düşürülmesi amacına odaklanmış; gerginliği tırmandırıcı davranış ve beyanlarda mümkün olduğunca kaçınılmıştır. Bununla birlikte, Sputnik üzerinden yapılan olumsuz haberlerin dozunun giderek artması neticesinde Türkiye, Sputnik'in internet sayfasının ve sosyal medya hesaplarının erişimi engellenmiş ve Sputnik Türkiye Genel Müdürü Tural Kerimov'un Türkiye'ye girişi 26.04.2014'de yasaklanmıştır (HaberTürk İnternet Haber Portalı, 20.04.2016). Sputnik'e yönelik olarak getirilen söz konusu erişim engelleri 15.07.2016'da Türkiye'de yaşanan darbe girişimi sonrasındaki süreçte, Cumhurbaşkanı Recep

Tayyip Erdoğan'ın RF'ye yapacağı ziyaretin hemen öncesinde, iki ülke arasında gerginleşen ilişkilerin iyileştirilmesine yönelik Türkiye'nin arzusunu ifade eden bir jest olarak, 08.08.2016'da kaldırılmıştır. Ancak T. Kerimov'a yönelik belirtilen seyahat engelinin kaldırılması hakkında bir karar verilmemiştir (Sputniknews Haber Portalı, 08.08.2016).

Sonuç

Günümüzde devletlerin güvenliği ile ilgili konuların teknolojik gelişmelerle ne denli bağlı olduğu düşünüldüğünde, siber uzay alanındaki teknolojilere sahip ol(a)mama hâlinin devletler açısından ciddi bir güvenlik zafiyeti yaratacağının farkında olan RF yönetimi, 1990 - 2000 yılları arasındaki toparlanma sürecinin ardından SSCB döneminden kalan geleneksel güvenlik anlayışına göre şekillenmiş tüm kurum ve stratejilerini, etkili bir siber saldırı ve siber savunma kapasitesi yaratmak adına yeniden organize etme hedefine büyük önem vermiştir. Bu kapsamda RF'nin, 2000'li yıllar sonrasında ortaya koyduğu strateji ve planlamalar ile birlikte, günümüzde siber uzayda güçlü ve agresif bir etkinliğe ulaşmış olduğu ileri sürülebilir.

Analiz ettiğimiz üzere RF'nin güncel savunma, dış politika ve Siber Güvenlik Strateji Belgeleri'nin temel amaçlarından biri, ülkenin enformasyon ve siber güvenliğinin sağlanmasıdır. RF, belirtilen amaç doğrultusunda devletin siber güvenliğini sağlamaya çalışırken, siber uzayın verdiği imkânlardan azami ölçüde faydalanan ve RF hükûmetlerinin istihbarat ihtiyaçlarının yanı sıra stratejik öneme sahip teknolojik yenilikleri elde etmeye yönelik bir siber espiyonaj sistemi de kurmayı hedeflemiştir. Bu çerçevede RF tarafından birbirleriyle eş güdüm halinde çalışan her biri ortak ve farklı amaçlara yönelmiş, siber uzayı kullanma noktasında önemli imkân ve kabiliyete sahip dört istihbarat (FSB, FSO, SVR, GRU) servisi kurulmuştur. RİS'lerin günümüzde ulaştığı ofansif, defansif, operasyonel, stratejik, elektronik harp kabiliyetine sahip, psikolojik istihbarat faaliyetlerine uygun, manipülasyona ve dezenformasyona elverişli yapısı, RF'nin siber uzayda faaliyet gösteren en önemli aktörlerden biri olmasını sağlamıştır.

Diğer yandan etkili bir siber saldırı ve savunma kapasitesinin tesisi noktasında, siber uzayın sağladığı imkânlardan askerî kapasitesini destekleme ve dış politikada bir baskı aracı olarak kullanma noktasında faydalanılabileceğinin farkında olan RF yönetimi, iletişim ve telekomünikasyon teknolojilerinde

yaşanmakta olan gelişmeleri bir enformasyon savaşı imkânı şeklinde okuyarak, bu alanda da stratejiler geliştirmeye de büyük önem vermiştir. Bu kapsamda, RF'nin siber güvenlik stratejisinin bir parçası olarak kendi enformasyon savaşı stratejisini tesis edilmesi kapsamındaki gayretleri de özellikle 2010 sonrasında ivme kazanmıştır. Sonuç olarak ise RF'nin, bu tarih sonrasında siber saldırı kapasitesini, millî yazılımlarla tasarlanan ulusal sosyal medya uygulamalarını, anti-virüs programlarını ve şirketlerini, yeni nesil tekniklerle yayın yapan küresel medya yapılanmalarını önemli ölçüde geliştirdiği gözlemlenebilmiştir.

RF'nin yukarda genel hatlarıyla özetlendiği şekilde yeni nesil enformasyon savaşı enstrümanları ve etkili bir uluslararası medya yapılanmaları ile desteklediği siber savunma ve saldırı kapasitesine sahip olmak adına ortaya koyduğu gayretin en önemli nedenlerinden biri ise RF çıkarları aleyhine Batı tarafından desteklenen ve 2000'lerin başında eski Doğu Blok'u ülkelerinde, Balkanlar'da yaşanan Renkli Devrim süreçleridir. Bu itibarla belirtilen süreçler sonrasında RF, siber uzay temelli yeni askerî imkânlar ile sosyal medya uygulamalarından istifade eden toplumsal hareketlerin önemini çok daha iyi anlamış ve kendi siber güvenlik sistematiğini bu gerçekliği görerek savunma ve saldırı yönünde geliştirmeye gayret etmiştir.

Sonuç olarak bir kez daha belirtmek isteriz ki günümüzde siber savunma ve siber saldırı kapasitesinin ulaştığı boyut, bu kapasitenin uygulanması noktasında istifade ettiği uluslararası medya kuruluşları ve sosyal medya imkânlarından yararlanarak geliştirdiği enformasyon savaşı strateji ile birlikte RF, küresel düzeyde çok önemli bir siber güç konumuna ulaşmıştır. Bu siber gücünün ulaştığı kapasiteyi de dış politika alanında çıkarları doğrultusunda kullanmaktan imtina etmeyen bir strateji izleyen RF, bu stratejisinin etkinliğini 2007'de Estonya'ya ve 2008'de Gürcistan'a, 2015'de ise Ukrayna ve Türkiye'ye yönelik olarak düzenlendiği iddia edilen siber saldırılar ve bu saldırılar ile birlikte başlattığı enformasyon savaşı uygulamaları ile ortaya koymuştur.

Kaynaklar

BBC News (28.06.2014). "Russia Offers $110,000 to Crack Tor Anonymous Network". http://www.bbc.com/news/technology-28526021. (09.09.2017).

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

Birnbaum, Michael (2014). "Russian Blogger Law Puts New Restrictions on Internet Freedoms". *Washington Post*. http://search.proquest.com/docview/1550033701. (15.04.2016).

Bloomberg Tecnology News Portal (05.08.2015). "Russia Clarifies Looming Data Localization Law". http://www.bna.com/russia-clarifies-looming-n17179934521/. (23.08.2016).

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

Darıcılı, Burak A. (2017). "Demokrat Parti Hack Skandalı Bağlamında Amerika Birleşik Devletleri ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Analizi". *Yıldırım Beyazıt* Üniversitesi Uluslararası Çalışmalar Dergisi (ULİSA) 1 (1): 1-24.

(2014). "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırılar". *Uludağ* Üniversitesi Sosyal Bilimler Dergisi 7 (2): 1-16.

Darıcılı, Burak A. & Barış Özdal (2017). "Enformasyon Savaşı Bağlamında Rusya Federasyonu ve Türkiye İlişkilerinin Analizi". İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi 4 (1): 19-40.

Fayutkin, Dan (2012). "The American and Russian Approaches to Cyber Challenges". *Defense Management* 2 (4): 1-4.

Gady, Franz-Stefan & Austin Greg (2010). "Russia, The United States, And Cyber Diplomacy Opening the Doors". *East-West Enstitute Report*. New York: 1-32. http://www.eastwest.ngo/sites/default /files/ ideas-files/ USRussiaCyber_WEB.pdf, (01.04.2016).

Galeotti, Mark (2016). "Putin's Hydra: Inside Russia's Intelligence Services". *European Council on Foreign Relations (ECFR)*: 1-19. http://www.ecfr.eu/publications/summary/putins _hydra_inside_russias_intelligence_services. (17.10.2016).

Gerden, Eugene (2014). "$500 Millionfor New Russian CyberArmy". *Security Magazine*. http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/. (26.03.2016).

Giles, Keir (2012). "Russia's Public Stance on Cyberspace Issues". *4th International Conference on Cyber Conflict*. Tallinn, NATO Cooperative Cyber Defense Centre of Excellence. 63-75. http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicS. (23.03.2016).

Gürcan, Metin (2014). "Rusya'nın Ukrayna'daki Bulanık Savaş Konsepti".http://www.academia.edu/11069073/RUSYANIN_BULANIK_SAVA%C5%9E_KONSEPT %C4%B0. (17.10.2016).

HaberTürk İnternet Haber Portalı (20.04.2016). "Kerimov'a Yasak". http://www.haberturk.com/gundem/haber/1227586-sputnik-turkiye-genel-muduru-tural-kerimova-giris-yasagi. (20.04.2014).

Hagestad, William II (2013). "Comparative Study: Iran, Russia and PRC Cyber War". *RSA Conference*. Europe. 18-25. http://www.rsaconference.com/writable/presentations file_upload/hta-w01-comparative-study-iran-russia-prc-cyber-war_copy1.pdf. (05.03.2016).

Heickerö, Roland (2010). "Emerging Cyber Threatsand Russian Views on Information Warfare and Operation". *Swedish Defense Research Agency Press*. 1-70. https://www.google.com.tr/?gfe_rd=cr&ei=iliWV8yUK8Sk8weF1bvIDQ&gwsrd=ssl#q=E merging+Cyber+Th reats+and+ Russian+Views+on+ Information+ Warfare+and+ Operation. (23.06.2016).

https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/. (24.03.2016).

http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020. (23.03.2016).

https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Russia_20 00.pdf. (08.09.2017).

Kaspersky Company (2016). "About Kaspersky Lab". www.kaspersky.com/about. (15.04.2016).

Kelly, Sanja (2014). "Freedom on the Net 2014: Russia". *Freedom House*. https:// freedom house.org/sites/default/files/resources/Russia.pdf. (15.04.2016).

Lee, David (2015). "Russia and Ukraine in Cyber 'Stand-Off". *BBC News*. http://www.bbc.com/news/technology-26447200. (23.04.2016).

Medvedev, Sergei A. (2015). "Offence-Defence Theory Analysis of Russian Cyber Capability". *Master Thesis for Naval Post-Graduate School*. Monterey, California. 1-110.http://calhoun.nps.edu/bitstream/handle/10945/45225/15Mar_Medvedev_Sergei.pdf?sequen ce=3. (05.03.2016).

Meriç, Enver (2015). "Rus İstihbarat Savaşları ve Putinizm". *Fikriyat.Net Portalı*. http://www.fikriyat.net/2016/11/28/rus-istihbarat-savaslari-putinizm/. (09.09.2017).

Mowthorpe, Matthew (2005). "The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views". The Journal of Social, Political, and Economic Studies 30 (2):137-153.

NATO Communications Centre of Excellence (Mayıs 2016). "Social Media as a Tool of Hybrid War". 1-49. http://www.stratcomcoe.org/social-media-tool-hybrid-warfare. (19.10.2016).

(2013). "Basic Principles for State Policy of the Russian Federation in the Field of International Information Security". https://ccdcoe.org/cyber-security-strategy- documents.html. (23.03.2016).

(2011). "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. (09.09.2017).

Reuters (31.11.2015). "Ukraine to probe suspected Russian cyberattack on grid". http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231, (12.11.016).

Shachtman, Noah (2012). "Russia's Top CyberSSonneleuthFoils US Spies, Helps Kremlin Pals". *Wired Magazine.* www.wired.com. (Erişim Tarihi:15.04.2016).

Saldatov, Andrei ve İrina Borogan (2013). "Russia's Surveillance State". *World Policy Institute*. http://www.worldpolicy.org/journal /fall2013 /Russia-surveillance. (03.05.2016).

Sputniknews Haber Portalı (01.04.2016). "Rusya, BM'ye Türkiye-IŞİD bağlantısını gösteren belgeleri sundu". https://tr.sputniknews.com/rusya/201604011021899203-rusya-bm-turkiye- isid/. (09.09.2017).

(08.08.2016). "AA: Sputnik'e Erişim Engeli Kaldırıldı". https://tr.sputniknews.com/turkiye/201608081024268110-sputnik-tib-erisim-engeli/. (03.01.2016).

Staar, R. Tocaso (2010). "Russia's Security Services". *Mediterranean Quarterly* 15 (1): 1-10.

State Security Magazine (2014). "Russia Announces Development of Cyber Military Unit". http://www.tripwire.com/state-of-security/latest-security-news/russia-announces-development-cyberwar-military-unit/. (26.03.2016).

The Centre for Counterintelligence and Security Studies (2016). "Russia's SVR, FSB, GRU Intelligence Services". http://www.cicentre.com/?page=191. (27.03.2016).

The Ministry of Foreign Affairs of The Russian Federation (2000). "National Security Concept of the Russian Federation. http://www.mid.ru/en_GB/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/589768. (09.09.2017).

The Russian Ministry of Defense (12.02.2013). "Concept of the Foreign Policy of the Russian Federation". http://archive.mid.ru//brp_4.nsf/0/76389FEC168189ED44257B2E0039B16D. (24.03.2016).

The Telegraph Online News (18.11.2015). "Could Cyber attack on Turkey be a Russian retaliation?". http://www.telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack -on-Turkey-be-a-Russian-retaliation.html. (24.04.2016).

Thoburn, Hoburn (2015). "Rusya Siyasetini Anlama Kılavuzu". *Siyaset, Ekonomi ve Toplum Araştırmalar Vakfı/SETA*: 1-91. http://file.setav.org/Files/Pdf/20151019183121_rusya-siyasetini-anlama-kilavuzu-pdf.pdf. (19.10.2016).

Türk-İnternet Haber Portalı (20.12.2015). "6. Gününde Nic.tr Saldırısı Sürüyor Ama Açıklama Yok-Onun Yerine Yorumlar Var". http://www.turk- internet.com/portal/yazigoster.php?yaziid =51749. (24.04.2016).

(08.05.2014). "Rusya'da Yürürlüğe Giren Yeni Yasayla Blog'lara Ağır Sorumluluklar Getiriliyor". http://www.turk-internet.com/portal/yazigoster.php?yaziid=46851. (27.04.2016).

(26.08.2013). "Rusya Tor Networkünü ve Anonimlik Araçlarını Erişime Kapatmaya Hazırlanıyor". http://www.turk-internet.com/portal/yazigoster.php?yaziid=43607. (09.09.2017).

Vasudevan, Sridharan (2013). "Russia Setting up Cyber Warfare Unit Under Military". *IB Times*. http://www.ibtimes.co.uk/russia-cyber-war-hack-moscow-military-snowden-500220. (26.03.2016).

Weedon, Jen ve Laura Galante (2014). "Intelligence Analysts Dissect the Headlines: Russia, Hackers, Cyberwar! Not SoFast". FireEye Executive Perspectives. https://www.fireeye.com/blog /executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html. (24.04.2016).

Wirtz, James J. (2015). "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy". *NATO CCDCOE Publications*. Tallinn. 31-36. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf. (05.03.2016).

Yılmaz, Salih (2016). "Rusya Neden Suriye'de?". Ankara: Yazar Yayınları.

The Analysis on The Instruments FormingtheCyber Security Capacity of Russian Federation*

Ali Burak Darıcılı**
Barış Özdal***

Abstract

Russian Federation (RF), besides United States of America, and People's Republic of factor distinguishing nature of RF's cyber capacity from the other two countries, is that RF uses cyber space as a means of pressure, and enforcement in resolution of problems relating to foreign politics, and particularly in relation with neighboring countries. Present cyber-attack capacity of RF, also as a result of technological China (CHN), is one of the world's leading cyber powers dominating cyber space. Main heritage of Soviet period, was developed within the scope of cyber security, and defense strategy documents which were formed by 2000s; and that capacity has been ever developing. In that context, it was tried to identify the cyber security capacity of RF by analyzing the strategic documents about the cyber security of RF, the cyber capacity of Russian Military Forces and Russian Intelligence Services and the structural features in Russian cyber area.

Keywords

Russian Federation, Cyber Security, Cyber Security Strategy Documents, Cyber Attack, Cyber Capacity.

---

* This article , under the consultation of Prof. Dr. Barış ÖZDAL, has been produced from the doctoral thesis study titled "Comparative Analysis of Cyber Security Strategies of United Statesand Russian Federation" , written and defence by A. Burak DARICILI in Uludağ University Social Sciences Institute of International Relations PhD program

** Dr., Uluda g University – Bursa / Turkey
daricili@yahoo.com

*** Prof. Dr., Uludağ University, Faculty of Economics and Administrative Sciences, Department of International Relations – Bursa / Turkey
barisozdal@gmail.com

Анализ инструментов, обеспечивающих кибербезопасность Российской Федерации*

Али Бурак Дарыджылы**
Барыш Оздал***

АННОТАЦИЯ

Российская Федерация (РФ), наряду с Соединенными Штатами Америки (США) и Китайской Народной Республикой (КНР), является одной из важнейших сил современного киберпространства. По характеру использования киберпотенциала Россия отличается от двух других упомянутых стран тем, что возможности, которые предоставляет киберпространство, служат РФ для решения внешнеполитических проблем и особенно для давления на соседей. Имеющийся у РФ потенциал кибератаки, являющийся отчасти технологическим наследием советского периода, сформировался вместе со стратегиями кибербезопасности и защиты 2000-х годов и продолжает развиваться в настоящее время. В данной работе с помощью анализа Документов стратегии кибербезопасности и киберструктуры Российских Вооруженных Сил и Федеральной Службы Безопасности делается попытка выявления потенциала кибербезопасности РФ.

Ключевые слова

Российская Федерация, кибербезопасность, стратегии безопасности киберпространства, кибератака, киберпотенциал.

---

* Настоящая статья написана на основе докторской диссертации «Сравнительный анализ стратегий кибербезопасности Соединённых Штатов Америки и Российской Федерации», успешно защищённой А. Бураком Дарыджылы (специальность «международные отношения», научный руководитель проф. Барыш Оздал) в Институте общественных наук Университета Улудаг.

** Д-р., Университет Улудаг- Бурса / Турция
daricili@yahoo.com

*** Проф., д-р., Университет Улудаг, факультет экономики и управления, отделение международных отношений – Бурса / Турция
barisozdal@gmail.com