Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi

A. Burak DARICILI[*], Barış ÖZDAL[**]

Öz

Espiyonaj, kontr/espiyonaj, dezenformasyon, elektronik savaş kabiliyeti, psikolojik savaş ve propaganda, siber saldırı gibi faaliyet ve planlamaları kapsayan geniş bir siber savaş kabiliyetine sahip olan Rusya Federasyonu (RF) sahip olduğu siber etkinlik ve gücü, günümüzde dış politika hedeflerine ulaşmak amacı için baskı aracı olarak kullanabilmektedir. 24 Kasım 2015 tarihinde Türk F-16'larının hava sahasını ihlal eden bir Rus Su-24 uçağını düşürmesi sonrasında başlayan gerginlik bilindiği üzere 14 Aralık 2015 tarihinde Türkiye'ye yapılan *"DDoS"* saldırıları ile yeni bir aşamaya taşınmıştır. Zira bu saldırıların ardından kamuoyunda RF'nin, Türkiye ile olan ilişkilerinde enformasyon savaşı stratejisi izlediği tartışılmaya başlanmıştır. Bu bağlamda çalışmamızda bu iddialar irdelenecek ve RF'nin sosyal medya imkânlarından azami ölçüde faydalanan ve yerel enstrümanlardan da beslenen küresel bir enformasyon savaşı strateji ile birlikte Türkiye'ye yönelik ciddi ve etkili bir siber propaganda faaliyeti sürdürüp sürdürmediği analiz edilecektir.

Anahtar Kelimeler: Rusya Federasyonu, Türkiye, Siber Saldırı, Enformasyon Savaşı, Hibrid Savaş

Analysis of Russian Federation and Turkey within the Context of Information Warfare

Abstract

Russian Federation (RF) which has a wide range of cyber warfare which cover espionage, counter/espionage, disinformation, electronic warfare capability,

Özgün Araştırma Makalesi [Original Research Article)
Geliş Tarihi: 25.11.2016 Kabul Tarihi: 04.02.2017
DOI: http://dx.doi.org/10.17336/igusbd.305525
[*] Doktora Öğrencisi, Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Bursa, Türkiye, E-posta: daricili@yahoo.com
[**] Prof. Dr., Uludağ Üniversitesi, İ.İ.B.F. Uluslararası İlişkiler Bölümü, Bursa, Türkiye, E-posta: barisozdal@gmail.com

psychological war and propaganda, and cyber-attack activities and planning, is capable of employing the cyber effectiveness and power which it owns as a pressure tool towards achieving its political objectives. As it is well known, the tension which had started after Turkish F-16 aircraft had downed a Russian Su-24 aircraft on 24 November 2015 after the aircraft had violated Turkish airspace was transferred to a new stage after "*DDoS*" attacks to Turkey on 14 December 2015. The reason being that following these attacks it was believed in the public opinion that RF was applying information warfare strategy in his relations with Turkey. Within this context, we will explicate these allegations in our work and analyze whether RF is applying a serious and effective cyber propaganda activities towards Turkey, together with a global information war strategy that takes full advantage of social media opportunities and is nourished from local instruments.

Keywords: Russian Federation, Turkey, Cyber Attack, Information Warfare, Hybrid War

İGÜ Sos. Bil. Derg., 4 (1), 2017, ss. 19-40.

Giriş

"Enformasyon Savaşı" kavramının üzerinde uzlaşılmış tek bir tanımı bulunmamakla birlikte, en geniş haliyle *"birisinin hasmı üzerinde avantaj sağlamak amacıyla; bilgiyi indirgeme, dağıtma, inkâr etme, koruma, transfer etme ve toplama yöntemlerini ihtiva eden teknikler bütünü olarak kullanması"* şeklinde tanımlanabilir.[1] RF ise 2000'li yılların başından itibaren siber uzay olarak adlandırılan alanda, özellikle de enformasyon savaşı kabiliyetinde etkinlik sağlamak amacıyla planlama ve stratejiler ortaya koymaktadır. Diğer bir deyişle tarihsel olarak Sovyetler Birliği döneminden günümüze kadar ulaşan stratejik ve teknolojik aklın da etkisiyle RF'nin siber kapasitesini saldırı ve savunma yönünde genişletme eğiliminde olduğu ileri sürülebilir.

Tarihsel süreç içerisinde RF'nin mevcut siber kapasitesinin oluşmasında etkili olan ilk olay, 1979–1989 arasında devam eden Afganistan Savaşı'dır. Savaş esnasında, Sovyet Ordusu'nun psikolojik savaş tekniklerini uygulamada ve Afganistan'daki saha birlikleri ile Moskova Riyaseti arasında etkili bir iletişimi sağlama noktasında yeterince başarılı olamadığı görülmüştür.[2]

Benzer şekilde 1994–1996 yıllarındaki Çeçen Savaşı sırasında, internet haberleşmesi ve bu haberleşmenin ortaya koyduğu imkânlar, savaş esnasındaki olayların RF aleyhine yansıtılması kapsamında oldukça başarılı

[1] Megan Burns, Information Warfare: What and How?, http://www.cs.cmu.edu/~burnsm/InfoWarfare.html (Erişim Tarihi 11 Kasım 2016).
[2] Roland Heickerö, Emerging Cyber Threats and Russian Views on Information Warfare and Operation, *Swedish Defense Research Agency Press*, March 2010, http://www.foi.se/rapport?rNo=FOI-R--2970--SE, Erişim Tarihi: 23 Haziran 2016), s. 15.

IGU J. Soc. Sci., 4 (1), 2017, pp. 19-40.

olmuştur.[3] Diğer bir deyişle RF, uluslararası kamuoyu nezdinde Çeçen Savaşı'nda insanlık dışı yöntemlere başvuran, savaş suçu işleyen bir devlet olarak kabul edilmiştir.[4] Söz konusu iki olayın olumsuz etkisiyle Rus güvenlik ve askeri bürokrasisinin, askeri ağ teknolojileri ve enformasyon savaşı alanındaki planlamaları ve hazırlıkları hızla gelişmeye başlamıştır. 1999 yılında NATO'nun eski Yugoslavya'daki Sırp güçlerini bombalamaya başlamasının ardından, Sırp ve Rus hackerler tarafından bu planlamaların ilk sonucu olarak NATO'ya, üye devletlerin askeri haberleşme sistemlerine, ABD Savunma Bakanlığı'nın alt yapılarına siber saldırılar gerçekleştirmiştir.[5]

Bu kapsamda, 2007 yılında Estonya'ya, 2008 yılındaki Gürcistan'a ve Litvanya'ya, 2009 yılındaki Kırgızistan'a, 2014 yılında Ukrayna'ya ve 2015 yılında Türkiye'ye yönelik siber saldırılar, enformasyon savaşı bağlamında değerlendirilebilir. Zira RF'nin günümüzde siber espiyonaj, siber kontr/espiyonaj, dezenformasyon, elektronik savaş, psikolojik savaş ve propaganda, siber saldırı gibi faaliyet ve planlamaları kapsayan geniş bir enformasyon savaşı kapasitesine sahip olduğu bilinmektedir.[6] Bu bağlamda çalışmada, RF'nin sosyal medya imkânlarından azami ölçüde faydalanan ve yerel enstrümanlardan da beslenen küresel bir enformasyon savaşı stratejisi ile birlikte Türkiye'ye yönelik ciddi ve etkili bir siber propaganda faaliyeti sürdürüp sürdürmediği analiz edilecektir. Analiz kapsamında öncelikle RF'nin siber uzay ile ilgili olarak 2000'li yılların başı itibariyle ortaya koyduğu resmi ve gayri resmi doktrin ve belgeler, makalenin sınırlılıkları içinde incelenmiştir.

RF'nin Siber Güvenlik Kapsamındaki Strateji Belgeleri

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 belge, 24 Ocak 2000 tarihinde yürürlüğe giren "*National Security Concept of Russian Federation"* (RF Ulusal Güvenlik Konsepti) isimli dokümandır. Söz konusu belgede, bilgi güvenliği kavramı ile ilgili olarak[7] *"RF'nin enformasyon alanında vatandaşlarının güvenliği ve ekonomik çıkarlarının sağlanması noktasında telekomünikasyon*

[3] Salih Bıçakcı, *21. Yüzyılda Siber Güvenlik*, İstanbul, Bilgi Üniversitesi Yayınları, Ağustos 2013, s. 30.
[4] Heickerö, loc.cit.
[5] Bıçakcı, loc.cit.
[6] James J. Wirtz, Cyber Warand 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).
[7] *NATO Cooperative Cyber Defence Centre of Excellence*, National Security Concept of Russian Federation, https://ccdcoe.org/cyber-security-strategy-documents.html, (Erişim Tarihi 23 Mart 2016). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/99.html, (Erişim Tarihi 23 Haziran 2016).

güvenliğine önem vermesi ve bu alana yatırım yapması gerektiği, Rus ulusal güvenliğine yönelik olarak enformasyon teknolojileri kaynaklı artan bir tehdit yapılanmasının bulunduğu" belirtilmiştir.

09 Eylül 2000 tarihli "*Information Security Doctrine of the Russian Federation"* (RF Enformasyon Güvenliği Doktrini) ise RF'nin siber güç olma hedefi yolundaki ilk temel belgedir. Bu doktrin, RF'nin enformasyon güvenliği konusundaki yol haritasını, prensiplerini, amaçlarını ve konu kapsamındaki resmi görüşlerini genel hatlarıyla ortaya koymaktadır.[8] Doktrinde, RF'nin enformasyon güvenliğinin sağlanması konusundaki ulusal çıkarlarının temelde ekonomik yapının, sivil toplumun ve politik sistemin korunması ile sağlanabildiğine işaret edilmektedir.[9]

RF hükümeti tarafından Mayıs 2009'da yayımlanan *"Russia's National Security Strategy to 2020"* (2020'ye doğru Rus Ulusal Güvenlik Stratejisi) tüm açıklığı ile siber güvenlik meselesine odaklanması bakımından dikkat çekici bir doküman olarak karşımıza çıkmaktadır.[10] Anılan belgede, RF istihbarat ve güvenlik güçlerine Rus toplumun ve Rus devletinin kritik altyapıların korunması noktasında tedbirler alınması gerektiği işaret edilmek ile birlikte, bahse konu tedbirlerin detayı ve mahiyetine ilişkin bilgi verilmediği görülecektir.

2011 yılında açıklanan "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 doküman, siber güvenlik alanında ciddi analiz, makale ve kitapları ile dünya genelinde tanınırlığı olan Keir Giles tarafından: *"Rus Ordusu'nun Ön Siber Savaş Doktrini"* şeklinde tanımlanmaktadır.[11] Bu dokümanda, diğer resmi RF stratejilerinin aksine bilgiyi merkeze alan bir bakış açısıyla siber faaliyetleri operasyonel bir mantık ve çatışma konsepti ile değerlendirme söz

---

[8] Sergei A. Medvedev, *Offence-Defence Theory Analysis of Russian Cyber Capability*, Naval Post-Graduate School, Master Thesis, Monterey, California, https://www.google.com.tr/?gfe_rd=cr&ei=qzHZVrreN7Go8wfMuYegDw#q=this+thesis+represent+mikhail+tsypkin, (Erişim Tarihi 05 Mart 2016), s. 55.

[9] *Ministry of Foreign Affairs of the Russian Federation*, Information Security Doctrine of Russian Federation, http://archive.mid.ru//bdomp/nsosndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd 24bc32575d9002c442b!OpenDocument, (Erişim Tarihi 23 Mart 2016). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/99.html, (Erişim Tarihi 23 Mart 2016).

[10] *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).

[11] Keir Giles, Russia's Public Stance on Cyber space Issues, *4th International Conference on Cyber Conflict*, Tallinn, NATO Cooperative Cyber Defense Centre of Excellence, 2012, http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublics, (Erişim Tarihi 23 Mart 2016), s. 68.

konusudur.[12] Bu kapsamda belgede, enformasyon savaşı kavramı, *"bilgi sistemlerine ve kaynaklarına zarar veren, toplumun ve hedef hükümetleri psikolojik savaş yöntemleri ile devirmeyi amaçlayan, politik, ekonomik ve kültürel sistemin altını oyan faaliyetler"*[13] şeklinde tanımlanmıştır.

IGU J. Soc. Sci., 4 (1), 2017, pp. 19-40.

09 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, ise çok kısa bir süre içinde uluslararası ilişkiler alanında geniş yankı bulmuştur.[14] Bu makale hakkındaki tartışmaların günümüze kadar hararetli bir şekilde sürmesinin temel nedeni ise Gerasimov'un yaklaşımına uygun bir tarzda, Rus Silahlı Kuvvetleri (RSK)'nın 2014 yılındaki Ukrayna Müdahalesi esnasında gösterdiği çok yönlü sıcak çatışma performansıdır. Zira RF, Ukrayna'da yürüttüğü yeni dönem sıcak çatışma konseptinin mini bir provasını 2008 yılında Gürcistan'da ortaya koymuştur. 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. Bu itibarla RF tarafından Ukrayna Müdahalesi esnasında ortaya konulan savaş performansı, kimi analistler tarafından *"hibrid savaş, kirli savaş, "non-linear" war, yeni savaş, bulanık savaş konsepti"* şeklinde de tanımlanan yaklaşımlarla değerlendirilmiştir.

Bu çerçevede, Gerasimov Doktrini ile ortaya konan prensipler dâhilinde RF'nin, temel olarak askeri niteliğe sahip olmayan yöntemleri, askeri kapasitesini dâhil ederek, daha az konvansiyonel güç ile dolayısıyla da daha az insan kaybı ve maliyet ile sıcak çatışma süreçlerini yönlendirmeyi ve yönetmeyi amaçladığı görülmektedir. Bu bağlamda, askeri 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, Gerasimov Doktrini ile ortaya konmak istenen hedefler arasında yer almaktadır.

Gerasimov söz konusu askeri yaklaşımı ile temel olarak, askeri olmayan yöntemlerin 21. yy sıcak çatışmalarındaki artan önemine vurgu yaparak, RF

---

[12] *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).
[13] Ibid.
[14] Medvedev, op.cit., p.55.

güvenlik bürokrasine bu konuda tedbirler geliştirilmesini önermektedir.[15] Bu kapsamda Gerasimov Doktrini ile RF Silahlı Kuvvetleri'nin[16] "*askeri olmayan ve özellikle siber saldırı yöntemlerini kullanan kapasite, planlama ve stratejilere sahip olması, RF istihbarat servisleri ile koordineli bir şekilde planlanan ve hedef ülkedeki dost-akraba topluluklardan da istifade eden gizli operasyonlar geliştirmesi, gerilla taktiklerini kullanan özel kuvvet birimlerini söz konusu şekilde düzenlenmiş olan hareket planlamalarına dâhil etme yeteneğine ulaşması, asimetrik tehdit yaratan psikolojik savaş yöntemlerine ağırlık vermesi*" gerektiğine vurgu yapılmıştır.

2013 tarihli *"Concept of the Foreign Policy of the Russian Federation"* (RF Dış Politika Konsepti) ise 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 söz konusu belgede, enformasyon ve siber güvenlik alanında da bazı tespit ve değerlendirmeler mevcuttur.[17] Bu kapsamda, anılan belgede enformasyon alanında yaşanmakta olan yeni teknolojilerin ulusal güvenlik için tehdit olduğu vurgusu yapılarak, geleneksel yaklaşımlarının ötesinde yeni enformasyon teknikleri ve kültürel metotların modern dış politika enstrümanları arasında kabul edilmesi gerektiği ifade edilmektedir.[18]

2013 tarihli bir diğer bir stratejik doküman olan *"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)'de RF'nin siber güvenlik kapsamındaki uluslararası girişim ve planlamalarının devamı kapsamında görülebilir.[19] Zira söz konusu belgenin başlangıcında, bu belgenin RF'nin ulusal kanunları ve geçmiş dönemde yayımlanan diğer enformasyon güvenliğine ait belgeler ile uyumlu olduğu vurgusu yapılarak, hedeflenen temel amacın, *"RF'nin bilgi ve*

---

[15] *In Moscow's Shadows*, The Gerasimov Doctrine and Russian Non-Linear War, https: //inmoscowsshad ows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russiannon-linear-war/, (Erişim Tarihi 24 Mart 2016).

[16] Valery Gerasimov, Tsennos' Nauki v Vredvidenii (Value of Applied Science), *Voyenno-Promyshlennyy Kuryer*, Şubat 27, 2013, https://inmoscowsshadows. wordpress.com/2014/07/06/the-gerasimov-doctrine-and- russian-non-linear-war/, (Erişim Tarihi 24 Mart 2016).

[17] *The Russian Ministry of Defense*, Concept of the Foreign Policy of the Russian Federation, http://archive.mid.ru//brp_4.nsf/0/76389FEC168189ED44257B2E0039 B16D, (Erişim Tarihi 24 Mart 2016). Ayrıntılı bilgi için bkz. http://archive.mid.ru//brp_4. nsf/0/6D84DDEDEDBF7DA644257B16005 1BF7F, (Erişim Tarihi 26 Haziran 2016).

[18] Ibid.

[19] *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/f iles/strategy/ RU_state-policy.pdf, (Erişim Tarihi 24 Mart 2016). Ayrıntılı bilgi için bkz. http://www.scrf.gov.ru/documents/6/114. html, (Erişim Tarihi 26 Haziran 2016).

IGU J. Soc. Sci., 4 (1), 2017, pp. 19-40.

telekomünikasyon teknolojileri alanında dünyanın diğer önemli güçleri ile eşitliği sağlayabileceği şartların oluşturulması" olduğu ifade edilmiştir.[20]

Genel ve soyut olarak aktardığımız bilgilerden de anlaşıldığı üzere, RF internetin ve ağ teknolojilerinin hızla yayılmaya başladığı 2000'li yıllar sonrasında siber uzaydaki gelişmelerin verdiği avantajları, uluslararası ilişkilerde bir baskı aracı olarak kullanmak amacıyla stratejiler geliştirmiştir. Diğer bir ifade ile RF, siber saldırı kapasitesine yönelik yaptığı yatırımların yanı sıra internet teknolojileri kaynaklı siber psikolojik savaş yöntemlerini de geliştirerek günümüzde önemli bir siber güç konumuna gelmiştir.

RF bu sebeple, siber savunma ve saldırı kapasitesinde söz konusu gelişmişliğin bir sonucu olarak, uluslararası ilişkilerde özellikle de komşularıyla yaşadığı sorunlarda siber gücünü sofistike yöntemlerle kullanmaktan çekinmemiştir. Bu itibarla RF'nin 2007'de Estonya'ya, 2008'de Gürcistan'a, 2014'de Ukrayna'ya ve 2015'te ise Türkiye'ye yönelik gerçekleştirdiği iddia edilen siber saldırıları oldukça dikkat çekicidir. Söz konusu siber saldırılardan Türkiye'ye yönelik olanının, beraberinde geniş çaplı bir enformasyon savaşı stratejisi ile birlikte icra edilmesinden dolayı, çok daha nitelikli bir şekilde planlandığı ileri sürülebilir.

RF Tarafından Türkiye'ye Yönelik Olarak Gerçekleştirildiği İddia Edilen Siber Saldırılar

24 Kasım 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 etkileri çok ciddi boyutlara ulaşan bir gerginliğin de başlangıcını oluşturmuştur. Bu siyasi gerginlik, 14 Aralık 2015 tarihinde saat 12.00 itibariyle Türkiye'ye yönelik olarak *"DDoS"* saldırıları ile yeni bir aşamaya taşınarak, iki ülke ilişkilerindeki krizin 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 hedeflenmiştir. Bilindiği üzere, *".tr"* uzantılı adların tutulduğu sistem, *".tr"* uzantılı alan adlarının yerini yönlendirmekte ve dolayısıyla sitelerin bulunmasını sağlamaktadır. Eğer bu sistem ulaşılamaz olursa, adların nerede olduğu bulunamadığından, sitelere erişim mümkün olamamaktadır. Ayrıca saldırıların *"DNS Amplification DDoS Attack"* şeklinde planlanmış olduğu da ifade edilmektedir.[21]

[20] Ibid.

[21] Ayrıntılı bilgi için bkz. "Altıncı Gününde Nic.tr Saldırısı Sürüyor ama Açıklama Yok-Onun Yerine Yorumlar Var", *Türk İnternet Sitesi*, http://www.turk-internet.com/portal/yazigoster.php?yaziid=51749, (Erişim Tarihi 24 Nisan 2016).

İGÜ Sos. Bil. Derg., 4 (1), 2017, ss. 19-40.

Bu süreç sırasında yaşanan ilginç ve önemli bir diğer gelişme ise Anonymous hacker grubu tarafından 23 Aralık 2016 tarihinde yayınlanan bir video ile saldırıların üstlenilmesidir. Yayınlanan videoda, "*saldırıların Anonymous tarafından gerçekleştirildiği, saldırının Türkiye'nin IŞID'a verdiği desteğe bir misilleme olduğu, Türkiye'nin IŞID'tan petrol aldığı, örgütü finansal olarak desteklediği, IŞID militanlarının Türkiye'de tedavi gördüğü ve saldırıların devam edeceği*" belirtilmiştir.[22] Bu açıklamanın Rus istihbarat servisleri (RİS) tarafından planlanan "*sahte bayrak (false flag)*" operasyonunun bir parçası olması ise kuvvetle muhtemeldir.[23]

Bu itibarla *"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, askeri 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 RF bağlantılı bir şekilde planlama ihtimalini kuvvetlendirmiştir.[24]

Daha teknik bir yaklaşımla belirtirsek, saldırıların basit bir formatta hazırlanmış olmasının, olayın arka planı gizlemek ve saldırıyı bireysel bir hacker grubu saldırısı şeklinde gösterme amacından kaynaklandığı da belirtilebilecektir. Bu kapsamda, saldırının günlerce sürmesi için bir motor sistemine ihtiyaç duyması, bu kapasitede sunucuların uzun süreli olarak amatörler tarafından çalıştırılmasının teknik olarak mümkün olmaması, DNS sorgulamasında açık sunucu listelerine sürekli *"aldatıcı (spoof)"* istek göndermek suretiyle *".tr"* DNS sunucularına yansıtma saldırısı yapılabilmesi için belirli bir güce gerek duyması, yapılan bu saldırılarda 30 Gbps saldırı trafiği üretebilmek için sürekli olarak 5-10 Gbps aralığında bir trafiğin varlığını gerektirmesi, saldırının 276.000 farklı adresten ve zaman zaman 30-

[22] "Anonymous. Turkey reeling under cyberattack as government and banks websites paralysed", *IB Times Internet News*, http://www.ibtimes.co.uk/anonymous-turkey-reeling-under-cyber-attack-government-banks-sites-paralysed-1534984, (Erişim Tarihi 24 Nisan 2016).

[23] Sahte Bayrak (False Flag) Operasyonu: Gizli örgütlerin ya da istihbarat servislerinin halkı kışkırtmak, yönlendirmek veya başka bir subversif (yıkıcı/bölücü) amaçlı olarak, kendi yaptıkları bazı faaliyet ve operasyonları hedefteki kişiler yürütüyor gibi göstererek kamuyu aldatmak için tasarladıkları gizli planlamalara verilen isimdir.

[24] Ayrıntılı bilgi için bkz. "Could Cyberattack on Turkey be a Russian retaliation?", *The Telegraph Online News*,http://www.telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack-on-Turkey-be-a-Russian-retaliation .html, (Erişim Tarihi 24 Nisan 2016).

40 GB boyuta erişen niteliği, bu teknik kapasitenin ise ancak bir devlet organizasyonu desteği ile sağlanabilecek düzeyde planlanabilecek olması hususları dikkate alındığında, saldırının RF desteği ile gerçekleştiği ciddi bir iddia olarak ileri sürülebilir.[25]

Türkiye cevap olarak, saldırıların ilk gününde yurtdışı internet trafiğini kesmiştir. Böylelikle yurtdışından *".tr"* uzantılı sitelere ulaşım engellenmiştir. Ayrıca, saldırılar esnasında Türkiye hizmet sağlayan operatörleri gezdirerek, saldırıya uğrayan operatörleri adeta saldırılardan kaçırarak kamu hizmetinin devamını sağlamaya çalışmıştır. Bu aşamada, *"Siber Olaylarla Mücadele Ekipleri" (SOME)* önemli rol oynamıştır.[26] Bir diğer tedbir ise saldırıya uğrayan DNS sunucularının geçici olarak Hollanda'ya kopyalanması şeklinde alınmıştır. Böylelikle de saldırıların boyutu hafifletilmeye çalışılmıştır.

Söz konusu siber saldırıların etkisizleşmesi noktasındaki bir diğer husus ise Türkiye'nin internet altyapısının zayıflığı ile ilgilidir. Normalde, bu tür büyüklükteki bir saldırının misliyle bir cevap üretmesi beklenirken, bu durum Türkiye'de farklı gelişmiş ve saldırının etkisi daha düşük olmuştur. Zira günümüz itibarı ile Türkiye'nin fiber altyapısı 250.000 km'dir. Hâlbuki bu rakamın Portekiz ile kıyaslanacak olursa 4 milyon km, Afrika'nın bir ülkesi olan Gana ile kıyaslasak olursak ise 3 milyon km. olması gerekmektedir. Bunun yanı sıra Türkiye'de internet kullanımı oldukça pahalıdır. Bu nedenle de sunucu başı trafikler düşük düzeyde kalmaktadır. Avrupa'da sunucu başı 1 Gbps olan trafikler, Türkiye'de 10 Mbps gibi düşünülebilir.[27]

Uluslararası ilişkiler açısından ise Türkiye'ye yönelik siber saldırılar, RF'nin bugüne kadar Estonya, Gürcistan, Ukrayna, Kırgızistan ve Litvanya'ya yönelik olarak gerçekleştirdiği iddia edilen saldırlar ile benzer özellikler içermektedir. Tüm bu saldırılarda olduğu gibi söz konusu siber saldırı da *"DDoS"* atakları şeklinde ve Türkiye'nin kritik altyapısını olumsuz olarak etkilemeye yönelik olarak planlanmıştır. Daha öncede belirtildiği üzere saldırının başlangıcı 24 Kasım 2015 tarihli uçak düşürme olayının hemen sonrasına denk gelmektedir. Bu saldırı ile RF'nin siber kapasitesini kullanarak, Türkiye'yi diplomatik baskılar ve ekonomik tedbirlerle zorlamak istediği değerlendirilebilecektir. Saldırılar ile eş zamanlı bir biçimde, RF'nin Türkiye'ye yönelik olarak sosyal medya olanaklarından da istifade etmek suretiyle ağır bir psikolojik savaş süreci de başlattığı ileri sürülebilir. Bu

[25] "Altıncı Gününde Nic.tr…", *Türk İnternet Haber Sitesi*, loc. cit.
[26] "Türkiye'ye Siber Saldırının Arkasında Ruslar Var", *Haberler İnternet Haber Portalı,* http://www.haberler.com/turkiye-ye-siber-saldirinin-arkasinda-ruslar-var-8006069-haberi/, (Erişim Tarihi 25 Nisan 2016).
[27] "6. Gününde Nic.tr…", *Türk İnternet Haber Sitesi*, loc. cit.

durum, RF'nin enformasyon savaşı enstrümanlarını kullanma noktasında ulaştığı yeni aşamayı göstermesi bakımından da oldukça önemlidir.

İGÜ Sos. Bil. Derg., 4 (1), 2017, ss. 19-40.

Söz Konusu Siber Saldırıların Enformasyon Savaşı Boyutu

Uluslararası sistemdeki etkili devletlerin, 1990'lı yıllar ile birlikte siber uzayın sağladığı imkânlardan askeri kapasitelerini destekleme ve dış politikada bir baskı aracı olarak kullanma noktasında faydalandıkları, ayrıca bu devletlerin iletişim ve telekomünikasyon teknolojilerinde yaşanmakta olan gelişmeleri bir enformasyon savaşı tekniği şeklinde okuyarak, bu alanda da stratejiler geliştirdikleri bilinmektedir.

Bu kapsamda CNN'in 1991 yılındaki I. Körfez Savaşı esnasındaki yayın performansı ile başlayan, daha sonra RF'nin 1994–1996 yılları arasındaki Çeçenistan Müdahalesi ile internetin bir propaganda yöntemi olarak ilk kez kullanılması ile devam eden, 2010 yılında başlayan Arap Baharı olayları kapsamında El Cezire'nin yayın politikası ile birlikte daha da gelişen, 2013 Gezi Olayları sırasındaki uluslararası medya kuruluşları tarafından yapılan yayınlarla da çok boyutlu hale gelen yeni nesil enformasyon savaşı teknikleri, sosyal medya olanaklarının da muazzam katkısıyla son yıllarda ciddi bir uluslararası müdahale aracı olarak karşımıza çıkmıştır.

Tüm bu gelişmeleri de dikkate almak suretiyle RF'nin siber güvenlik stratejisinin bir parçası olarak kendi enformasyon savaşı stratejisini geliştirme kapsamındaki gayretleri 2010 yılı sonrasında ivme kazanmıştır. Bu çerçevede Rusya Bugün (Russia Today / Rossiaya Segodnya) Medya Topluluğu, 09 Aralık 2013 tarihinde Putin'in talimatıyla, RF'nin uluslararası enformasyon alanındaki faaliyetlerini yürütmek amacıyla kurulmuştur. Sputnik Multimedya Haber Grubu ise 10 Kasım 2014 tarihinde Rusya'nın Sesi ve RIA Novosti Haber Ajanslarının birleştirilmesi ile tesis edilmiştir. Gerçekte, bu iki medya topluluğunun kuruluş nedeni, RF'nin bir enformasyon savaşı hamlesi olarak, Batılı medya organlarının tek taraflı ve hegemonik yayınlarına karşı Moskova'nın yanıtı olarak değerlendirilebilecektir.

Diğer yandan, söz konusu medya kuruluşları arasında özellikle Sputnik'in Türkiye'ye yönelik faaliyetleri ve yayın politikası dikkat çekicidir. Bu itibarla hem haber ajansı hem de radyoyu kapsayan bir medya ağı şeklinde yapılandırılan Sputnik, Türkiye'de bir internet haber portalı, etkin bir şekilde kullanılan sosyal medya ağı ve İstanbul, Ankara, İzmir, Antalya ve Bursa merkezli olarak faaliyet gösteren radyo istasyonları şeklinde örgütlenmiştir. Sputnik evrensel düzeyde ise "Sputnik" markası altında faaliyet gösteren, İngilizce, İspanyolca, Çince ve Arapça haber merkezleri, multimedya içerikle desteklenecek olan ve Rusça, Türkçe, Abhazca, Afganca, Almanca, Arapça, Azerice, Ermenice, Gürcüce, Fransızca, Kazakça, Kırım Tatarca, Kırgızca, Çince,

IGU J. Soc. Sci., 4 (1), 2017, pp. 19-40.

Kürtçe, Letonya dili, Moldova dili, Tacikçe, Lehçe, Farsça, Portekizce, Sırpça, Özbekçe, Ukraynaca, Fransızca, Hintçe, Estonya dili ve Japonca haber yayın akışları ile İstanbul, Londra, Washington, Yeni Delhi, Kahire, Montevideo, Pekin, Berlin, Rio de Janeiro, Paris, Buenos Aires, Belgrad, Helsinki, Minsk, Kiev, Taşkent, Astana, Bişkek, Duşanbe, Sohum, Tshinvali, Tiflis, Erivan, Bakü ve Kişinev'de bulunan yerel haber ofisleri şeklinde organize olmuştur. Diğer yandan yerel unsurlarla entegre bir şekilde, küresel ölçekte de geniş bir örgütlenme ile dizayn edilmiş olan Sputnik'in faaliyetleri ile ilgili olarak, Rusya Bugün (Russia Today) Genel Müdürü Dmitri Kisyelev: "Bugün hem Batı'ya hem de Doğu'ya kendi isteklerini empoze etmeye çalışan birtakım devletlerin müdahil olduğu coğrafyalarda yıllarca sürecek iç savaşların tohumları atılarak oluk oluk kan akmasına sebep olunuyor. Renkli Devrimler ile devletler yıkılmakta; tıpkı Irak, Libya, Gürcistan, Ukrayna ve Suriye örneklerinde olduğu gibi… Artık pek çok insan bu olaylarda Amerikalılar gibi düşünmenin ve olayları onların penceresinden değerlendirmenin bir zorunluluk olmadığını anlamış durumda. Rusya söz konusu şartlarda insanlığın yararına olacak yeni bir model öneriyor; biz çok renkli bir dünya düzeninden yanayız ve bu hususta bizimle fikir birliği yapan birçok müttefikimiz de bulunmakta. Bu sebeple medya grubumuz, yeni bir dünya markası olan Sputnik'i yaratmıştır. Sputnik, her ülkenin kendi ulusal önceliklerinin, geleneklerinin, kültürünün ve tarihinin ön planda olduğu çok kutuplu bir dünya düzeninin aynası olacaktır. Bizim çok uluslu ve çok kutuplu medeniyet anlayışımızda Japonya'da Japon, Türkiye'de Türk, Çin'de Çinli ve Rusya'da Rus olarak yer almaktadır. Biz hiç kimseye Rusya'nın ulusal menfaatlerine uygun olan bir yaşamı empoze etmeye çalışmıyoruz. Bize göre her millet kendi değerleri doğrultusunda yaşam hakkına sahiptir ve böyle bir dünya düzeninin temel dinamiği de uluslararası hukuktur. Mevcut küresel düzende bugün devam etmekte olan yeniden şekillendirme süreci insanlığın yararına olacaktır. Faaliyet gösterdiğimiz hiçbir ülkede muhalif bir medya kuruluşu anlayışı ile çalışmıyoruz. Objektif yayın anlayışına uygun olarak toplumun tüm kesimleri ile eşit mesafede ve iyi ilişkiler kuruyoruz. Sputnik'in yayını tamamen yurtdışındaki izleyici kitlesine yönelik olarak hazırlandı" açıklamasında bulunmuştur. Bu beyanda da açıkça vurgulandığı üzere RF'nin Sputnik'in yayın sistematiği ile hedeflediği amaç, küresel ölçekte ABD başta olmak üzere Batı karşıtlığı temelinde, etkili, yerel unsurlarla uyumlu, iyi örgütlü bir propaganda mekanizmasını siber güvenlik stratejisin bir parçası olarak geliştirmektir.[28]

Sputnik adeta RF'nin bir enformasyon savaş aparatı olarak dizayn edilmiştir. Bu itibarla Sputnik'in geleneksel Sovyet propaganda tekniklerinin

[28] Ayrıntılı bilgi için bkz. "Rusya'dan Medya Atağı", *Milliyet Gazetesi,* http://www.milliyet.com.tr/rusya-dan-medya-atagi/dunya/detay/1968251/default. htm, (Erişim Tarihi 21 Nisan 2016).

dışında, Kremlin'in doğrudan sesi olmak yerine, hedef alınan her ülkeye özgü olarak, Rus çıkarları doğrultusunda kafa karıştırıcı, yanıltıcı ve yönlendirici ve manipüle edici bir yayın akışı benimsediği de ifade edilebilecektir.[29] Yani Sputnik, bahse konu yayın akışı ile Kremlin'in bir nevi "medya silahı" olarak görülebilir.

Bu kapsamda, Türkiye'nin 24 Kasım 2015 tarihinde sınır ihlali yapan RF'ye ait bir savaş uçağını düşürmesi sonrasında Sputnik'in yayın politikası özellikle, Türkiye'nin "Irak ve Şam Devleti (IŞID) (Devlet'ül Irak ve'ş Şam / DAEŞ)"ne yardım ettiği şeklindeki agresif bir yıpratma propagandasına dönüşmüştür. Hatta Sputnik, Adalet ve Kalkınma Partisi (AK Parti) ve Cumhurbaşkanı Recep Tayyip Erdoğan aleyhtarlığını merkeze koyarak, sosyal medyadaki imkânlardan da istifade etmek suretiyle Türkiye'ye yönelik olumsuz yayın politikasını 2016 Mart ve Nisan aylarında zirveye çıkarmıştır. Bu noktada, Sputnik'in 01 Nisan 2016 tarihli maksatlı ve yönlendirici *"BM'ye Türkiye-IŞİD Bağlantısını Gösteren Belgeler..."*[30] başlıklı haberinin, Türkiye'de bazı medya gruplarınca kullanılma şekli dikkat çekicidir. 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 yer verilmiştir. 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 V. Putin'in uçak düşürülmesi olayını fırsata çevirerek, iç politika da güç kazanmak amacıyla Rus toplumunda nezdinde bulunan tarihi Türk düşmanlığını körüklemek istemesidir.[31]

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 ise Türkiye, Sputnik'in

---

[29] Edward Lucas ve Ben Nimmo, Information Warfare: What Is It and How to Win It, *Center for European Policy Analysis (CEPA)*, http://cepa.org/sites/default/files/Infowar%20Report.pdf, (Erişim Tarihi 20 Nisan 2016), s. 1.

[30] "BM'ye Türkiye-IŞİD Bağlantısını Gösteren Belgeler...", *Sputniknews Haber Portalı*, http://tr.sputniknews.com/rusya/20160401/.../rusya-bm-turkiye-isid.html, (Erişim Tarihi 15 Nisan 2016).

[31] Ayrıntılı bilgi için bkz. Salih Yılmaz, *Rusya Neden Suriye'de?*, Ankara, Yazar Yayınları, 2016, s. 257-267.

IGU J. Soc. Sci., 4 (1), 2017, pp. 19-40.

internet sayfasının ve sosyal medya hesaplarının erişimi engellenmiş[32] ve Sputnik Türkiye Genel Müdürü Tural Kerimov'un da Türkiye'ye girişi 26 Nisan 2014 tarihinde yasaklanmıştır.[33] Sputnik'e yönelik bu tedbirler ise 15 Temmuz 2016 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 Ağustos 2016 tarihinde kaldırılmıştır.

Sputnik ve diğer RF medya kuruluşlarının Türkiye'ye yönelik olarak başlattığı enformasyon savaşının bir başka ayağı ise bahse konu medya kuruluşlarının yerel unsurlarla işbirliği yaparak, kendi yayın akışına uygun politikacıları, siyasi analizcileri, gazetecileri ve sosyal medyayı manipüle etmesi amacıyla da paralı trolleri[34] kullanması şeklinde planlanmıştır.[35] Bu kapsamda, özellikle AK Parti ve Cumhurbaşkanı Recep Tayip Erdoğan karşıtlığı temelinde birleşen Türkiye'deki muhalif bazı çevreler bilerek veya bilmeyerek, Rus medya kuruluşları tarafından sürdürülen bu yayın politikasının birer vasıtası haline gelmişlerdir. Bu itibarla bahse konu dönemde "Fuat Avni" takma adlı Twitter hesabından yapılan ve RF'nin söz konusu iddialarını[36] manipülatif bir tarzda ele alan kimi paylaşımlar[37] dikkat çekicidir. Yine benzer şekilde Halkın Demokrasi Partisi (HDP) tarafından AK Parti ile DAEŞ irtibatına yönelik olarak RF iddialarını temel alan ve Türkiye Büyük Millet Meclisi'ne (TBMM) taşınan kimi soru önergeleri[38] ile bu konuda

---

[32] "Sputnik ve DİHA'ya Erişim Engeli Talebi Onaylandı.", *Anadolu Ajansı,* http://aa.com.tr/tr/turkiye/sputnik-ve-dihaya-erisim-engeli-talebi-onaylandi-/555880, (Erişim Tarihi 20 Nisan 2014).

[33] "Kerimov'a Yasak", *HaberTürk İnternet Haber Portalı*, http://www.Haberturk.com/gundem/haber/1227586-sputnik-turkiye-genel-muduru-tural-kerimova-giris-yasagi, (Erişim Tarihi 20 Nisan 2014).

[34] Trol: İskandinavya folklorunda genellikle dev ya da cüce olarak resmedilen, mağaralarda yaşayan efsanevi, çirkin bir yaratıktır. *"İnternet trollüğü"*: insanları tahrik ederek ve kızgınlıkla yazılmış cevaplar vereceklerini umarak, e-posta veya çevrimiçi grup mesajları göndermek şeklinde tarif edilir. Trol olarak faaliyet gösteren şahıslar, internet ve sosyal medya ortamında kasıtlı olarak karşısındaki kişinin ya da toplumun insan doğasından kaynaklanan zayıf noktalarını istismar edip, keyfini kaçırmaya ve işlerini aksatmaya çalışabilirler.

[35] Ayrıntılı bilgi için bkz. Lucas ve Nimmo, op.cit., s. 8-12.

[36] Ayrıntılı bilgi için bkz. "*Fuat Avni, Rus Uçağının Düşürüleceğini Nereden Biliyordu?",* *Sputniknews Haber Portalı*, https://tr.sputniknews.com/columnists/201607241024055041-Rus-ucagi-darbe-pilot/, (Erişim Tarihi 08 Kasım 2016).

[37] Ayrıntılı bilgi için bkz. "WikiLeaks, Fuat Avni'nin Rus Uçağı İddiasını Paylaştı", *Birgün Net,* http://www.birgun.net/haber-detay/wikileaks-fuat-avni-nin-rus-ucagi-iddiasini-paylasti-97073.html, (Erişim Tarihi 08 Kasım 2016).

[38] Ayrıntılı bilgi için bkz. "HDP'li Kürkçü Yanıt Alamadığı IŞID Petrolü Sorusunu Yeniden Sordu", *Sputniknews Haber Portalı,* https://tr.sputniknews.com/turkiye/201603301021838524-hdp-isid-turkiye-petrol-rt-belge/, (Erişim Tarihi 08 Kasım 2016).

HDP'li milletvekilleri tarafından verilen beyanatların da bu kapsamda önemli örnekleri oluşturduğu ileri sürülebilir.[39]

İGÜ Sos. Bil. Derg., 4 (1), 2017, ss. 19-40.

Bununla birlikte, RF'nin enformasyon savaşı stratejisinde, sosyal medyanın bir siber propaganda enstrümanı olarak kullanmaya yönelik kapasitesi de bizce ayrıca analiz edilmelidir. RF tarafından, sosyal medyanın "uçak düşürme" krizi esnasında ve sonrasında etkili bir enformasyon savaş yöntemi olarak seçilmesinde, sosyal medya olanaklarına ulaşmanın herkes için kolay, hızlı, anonim (kullanıcısı belli olmayan), önemli oranda propaganda materyalini aynı anda ve çok kısa sürede yönlendirme kabiliyetine sahip ve coğrafi sınır tanımayan yapısı etkili olmuştur.[40] RF'nin Türkiye ile ilişkileri kapsamında sosyal medya imkânlarının kullanılması, 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, Yaptriot.ru, Whowho.com.ua, Novorus.info, Novorossia.ru vb.) Türkiye'nin Suriye'de bulunan DAEŞ unsurlarıyla irtibatlı olduğunu gösteren dezenformasyon haberlerinin profesyonel imkânlarla hazırlandığı belli olan görsel dokümanlar ile birlikte Rus ve dünya kamuoyuna servis etmesi şeklinde planlanmış ve geliştirilmiştir. Örneğin, 24 Kasım 2015 tarihi sonrası dönemde RF'de gerçekleştirilen sosyal medya paylaşımlarında Putin'in konuyla ilgili ifade ettiği *"sırtımızdan bıçaklandık"* ifadesi uzun bir süre en çok konuşulan olaylar arasına yer almıştır. Bu dönemde Türkiye'ye gitmeme çağrıları, "*Terörist Türkiye*" mesajları ve Cumhurbaşkanı Recep Tayyip Erdoğan'ın DAEŞ'e yardım ederken gösterildiği çizimler sosyal medyada sıklıkla paylaşılmıştır.[41] Yine benzer şekilde bu dönemde Rus sosyal medyasında Türkiye, AK Parti ve Cumhurbaşkanı Recep Tayyip Erdoğan aleyhine hazırlanmış sosyal medya görsellerinin paylaşımında adeta bir patlama yaşanmıştır.[42]

Diğer yandan söz konusu sosyal medya paylaşımları ile uyumlu şekilde ulusal Rus medyası da konuyu provokatif bir yayın politikası ile ele alarak, adeta körüklemiştir. Bu itibarla konu Vedomosti Gazetesi tarafından; "*Türkiye*

---

[39] Ayrıntılı bilgi için bkz. "Demirtaş: AKP Terör Üreticisi, IŞİD'in Siyasi Uzantısı", *Sputniknews Haber Portalı*, https://tr.sputniknews.com/politika/201602201021016742-demirtas-akp-isid/, (Erişim Tarihi 08 Kasım 2016).

[40] *NATO Communications Centre of Excellence*, "Social Media as a Tool of Hybrid War", http://www.stratcomcoe.org/social-media-tool-hybrid-warfare, (Erişim Tarihi 19 Ekim 2016), s. 24

[41] "Rusya'nın Savaş Uçağının Düşürülmesi Üzerine Sosyal Medyada Tepki", *Birgün Net*, http://www. birgun.net/haber-detay/rusya-nin-savas-ucaginin-dusurulmesi-uzerine-sosyal-medyada-tepki-95978.html, (Erişim Tarihi 08 Kasım2016).

[42] "How Social Media Users Responded to Turkey's downing of Russian warplane", *WeirdRussia Haber Portalı*, http://weirdrussia.com/2015/11/26/how-social-media-users-responded-to-turkeys-downing-of-russian –warplane /, (Erişim Tarihi 08 Kasım 2016).

IGU J. Soc. Sci., 4 (1), 2017, pp. 19-40.

Rusya'yı sırtından vurdu. Rusya bu işi sonuçsuz bırakmayacak", Komsomolskaya Pravda tarafından "*Biz bir ay önce Cumhurbaşkanı Erdoğan'ın Rus uçağı vurmaya hazırlandığını yazmıştık*", İzvestiya Gazetesi tarafından; "*Bizim uçak Türkiye'yi tehdit etmiyordu. Sırtımızdan vurdular*", Moskovskiy Komsomolets Gazetesi tarafından; "*Ankara savunmaya geçti. Vurulan savaş uçağında kime ait olduğuna işaret eden tanıtıcı işaretler bulunmadığını söylüyor*" şeklindeki manşetlerle gündeme getirilmiştir.[43] Bu enformasyon savaşı stratejisinin agresifliği ise günümüzde Türkiye ile ilişkilerin seyrine bağlı olarak sürekli kontrol altında tutularak ayarlanmakta ve sürdürülmektedir.

Sonuç

Günümüzde devletlerin güvenliği ile ilgili konuların teknolojik gelişmelerle eşgüdümlü olduğu düşünüldüğünde, siber uzay alanındaki teknolojilere sahip olamama halinin devletler açısından ciddi bir güvenlik zafiyeti yaratacağı açıktır. Aynı şekilde devletlerin güvenliklerini sağlama noktasında, geleneksel güvenlik anlayışına göre şekillenmiş tüm kurum ve stratejilerini etkili bir siber saldırı ve siber savunma kapasitesi yaratmak adına yeniden organize etmesi de gerekmektedir.

Bu değerlendirme ile uyumlu şekilde, RF'nin Soğuk Savaş sonrası dönemde, özellikle de 2000'li yılların başı itibariyle gerek ordusunu ve istihbarat birimlerini gerekse de kurumsal yapılarını siber uzayın sağladığı yeni imkânlar kapsamında etkili bir siber saldırı kapasitesine sahip olmak amacıyla yeniden organize etmeye çalıştığı, bu organizasyonu kapsamında da yeni nesil enformasyon savaşı planlamalarına özel önem verdiği ortadadır. RF'nin yaklaşık on yıldır planlı bir şekilde geliştirdiği siber saldırı kapasitesinin en önemli ayağı olan yeni nesil siber propaganda imkanları, Soğuk Savaş döneminde enformasyon savaşı alanında SSCB tarafından ortaya konulan stratejinin çok ötesinde, artık oldukça sofistike niteliktedir.

Bu kapsamda, iddia edildiği üzere RF'nin 2007 yılında Estonya'nın bilişim sistemlerini çalışamaz hale getiren siber saldırılar ile konvansiyonel bir savaşın etkilerini propaganda ile desteklediği; 2008 yılındaki Gürcistan Savaşı esnasındaki siber faaliyetleri; akabinde meydana gelen 2008 yılındaki Litvanya'ya, 2009 yılındaki Kırgızistan'a yönelik siber saldırıları ile 2014 Ukrayna Müdahalesi esnasında ortaya koyduğu *"yeni nesil"* savaş konsepti ve uçak düşürülmesi krizi sonrasında 2015 Aralık ayında Türkiye'ye yönelik *"DDoS"* atakları ile birlikte uygulama koyduğu enformasyon savaşı stratejisi bu devletin siber uzaydaki kapasitesini göstermesi bakımından kayda değer örneklerdir.

[43] "Uçak Krizi Dünya'da Manşet", *Hürriyet Gazetesi*, http://www.hurriyet.com.tr/ucak-krizi-dunyaya-manset-40018345, (Erişim Tarihi 08 Kasım 2016).

İGÜ Sos. Bil. Derg., 4 (1), 2017, ss. 19-40.

RF'nin enformasyon savaşı alanındaki güçlü ve agresif rolü, Türkiye ile yaşadığı "uçak düşürme" krizi esnasında net bir şekilde gözlemlenebilmiştir. Türkiye örneğinde de görüldüğü üzere, RF'nin enformasyon savaşını modern güvenlik stratejisinin merkezine koyduğu açıktır. Bu stratejik yaklaşımın bir sonucu olarak, RF merkezli medya kuruluşlarının, etkili ve yaygın bir sosyal medya ağıyla dünyanın her hangi bir bölgesinde ve o bölgedeki her bir ülkede farklı bir enformasyon savaşı yaklaşımı gösterebilme kapasitesine sahip oldukları da ortadadır. Bu kapsamda, RF'nin enformasyon savaşı stratejisinin sahip olduğu esnek yapısı ile birlikte, takip edilen politik amaçlara uygun bir şekilde Baltık ülkelerinde Rus azınlıkları destekleyebilmekte ve Sovyet dönemi nostaljisi ile eski parlak günlere göndermeler yapabilmektedir. Benzer şekilde söz konusu enformasyon savaşı kapasitesi ile RF, Türkiye'de AK Parti muhalifi çevrelerle uyumlu yayınlar izleyebilmekte ve böylelikle AK Parti iktidarının toplum içindeki etkinliği yıpratabilmekte; Azerbaycan'da Türkiye aleyhtarlığı yapılarak Azeri Türklerine 2008-2009 yılları arasında yaşanan Türkiye-Ermenistan yakınlaşmasını sürekli olarak hatırlatabilmekte; Slovakya ve Çek Cumhuriyeti'nde çevreci ve anti-militarist bir eğilimle yayın politikası belirleyebilmekte; Orta Asya'da Türkiye'nin Turancı politikalar sürdürdüğü ifade edilerek, sürekli olarak Türk ve Batı aleyhtarı haberlere yer verebilmektedir.[44]

Sonuç olarak, Türkiye ile uçak düşürme krizi sonrasında yaşadığı gerginlik boyunca RF'nin iyi planlanmış ve finanse edilmiş, hedefe odaklı, yerelleşmenin öneminin farkında olan bir enformasyon savaş stratejisi performansı sergilediği ortadadır. Bu stratejinin temelini ise AK Parti ve Recep Tayyip Erdoğan aleyhtarlığı maskesiyle manipüle ettiği yerel unsurlardan da destek almak suretiyle, uluslararası medya kuruluşları vasıtasıyla sürdürdüğü etkili, agresif yayın politikaları ve söz konusu yayın politikalarını profesyonel imkanlarla hazırlanmış görsel imgelerle desteklediği sosyal medya paylaşımları oluşturmuştur.

[44] Bu konuda ayrıntılı bilgi için bkz. Lucas ve Nimmo, op.cit., ss. 3-5.

IGU J. Soc. Sci., 4 (1), 2017, pp. 19-40.

KAYNAKÇA

"Altıncı Gününde Nic.tr Saldırısı Sürüyor ama Açıklama Yok-Onun Yerine Yorumlar Var", **Türk İnternet Sitesi**, http://www.turk-internet.com /portal/yazigoster.php?yaziid=51749, (Erişim Tarihi 24 Nisan 2016).

"Anonymous: Turkey reeling under cyberattack as government and banks websites paralysed", **IB Times Internet News**, http://www.ibtimes. co.uk/anonymous-turkey-reeling-under-cyber-attack-government-banks-sites-paralysed-1534984, (Erişim Tarihi 24 Nisan 2016).

"BM'ye Türkiye-IŞİD Bağlantısını Gösteren Belgeler...", **Sputniknews Haber Portalı**, http://tr.sputniknews.com/rusya/20160401/.../rusya-bm-turkiye-isid.html, (Erişim Tarihi 15 Nisan 2016).

"Could cyber attack on Turkey be a Russian retaliation?", **The Telegraph Online News**, http://www.telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack-on-Turkey-be-a-Russian-retaliation .html, (Erişim Tarihi 24 Nisan 2016).

"Demirtaş: AKP Terör Üreticisi, IŞİD'in Siyasi Uzantısı**", Sputniknews Haber Portalı**, https://tr.sputniknews.com/politika/201602201021016742-demirtas-akp-isid/, (Erişim Tarihi 08 Kasım 2016).

"Fuat Avni, Rus Uçağının Düşürüleceğini Nereden Biliyordu?", **Sputniknews Haber Portalı**, https://tr.sputniknews.com/columnists/ 201607241024055041-Rus-ucagi-darbe-pilot/, (Erişim Tarihi 08 Kasım 2016).

"HDP'li Kürkçü Yanıt Alamadığı IŞID Petrolü Sorusunu Yeniden Sordu", **Sputniknews Haber Portalı**, https://tr. sputniknews.com/turkiye/ 201603301021838524-hdp-isid-turkiye-petrol-rt-belge/, (Erişim Tarihi 08 Kasım 2016).

"How Social Media Users Responded to Turkey's downing of Russian warplane", **WeirdRussia Haber Portalı**, http://weirdrussia.com/2015/11 /26/how-social-media-users-responded-to-turkeys-downing-of-russian–warplane /, (Erişim Tarihi 08 Kasım 2016).

"Kerimov'a Yasak", **Haber Türk İnternet Haber Portalı**, http://www.haberturk.com/gundem/haber/1227586-sputnik-turkiye-genel-muduru-tural-kerimova-giris-yasagi, (Erişim Tarihi 20 Nisan 2014).

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

"Rusya'dan Medya Atağı", **Milliyet Gazetesi**, http://www.milliyet.com.tr /rusya-dan-medya-atagi/dunya/detay/1968251 /default.htm, (Erişim Tarihi 21 Nisan 2016).

"Rusya'nın Savaş Uçağının Düşürülmesi Üzerine Sosyal Medyada Tepki", **Birgün Net**, http://www.birgun.net/haber-detay/rusya-nin-savas-ucaginin-dusurulmesi-uzerine-sosyal-medyada-tepki-95978.html, (Erişim Tarihi 08 Kasım2016).

"Sputnik ve DİHA'ya Erişim Engeli Talebi Onaylandı", **Anadolu Ajansı,** http://aa.com.tr/tr/turkiye/sputnik-ve-dihaya-erisim-engeli-talebi-onaylandi-/555880, (Erişim Tarihi 20 Nisan 2014).

"Türkiye'ye Siber Saldırının Arkasında Ruslar Var", **Haberler İnternet Haber Portalı**, http://www.haberler.com/turkiye-ye-siber-saldirinin-arkasinda-ruslar-var-8006069-haberi/, (Erişim Tarihi 25 Nisan 2016).

"Uçak Krizi Dünya'da Manşet", **Hürriyet Gazetesi**, http://www.hurriyet.com.tr/ucak-krizi-dunyaya-manset-40018345, (Erişim Tarihi 08 Kasım 2016).

"WikiLeaks, Fuat Avni'nin Rus Uçağı İddiasını Paylaştı", **Birgün Net**, http://www.birgun.net/haber-detay/wikileaks-fuat-avni-nin-rus-ucagi-iddiasini-paylasti-97073.html, (Erişim Tarihi 08 Kasım 2016).

BIÇAKCI, Salih, **21. Yüzyılda Siber Güvenlik**, İstanbul, Bilgi Üniversitesi Yayınları, Ağustos 2013, s. 30.

BURNS, Megan, **Information Warfare: What and How?**, http://www.cs.cmu.edu/~burnsm/InfoWarfare.html (Erişim Tarihi 11 Kasım 2016).

GERASİMOV, Valery, Tsennos' Nauki v Vredvidenii (Value of Applied Science), **Voyenno-Promyshlennyy Kuryer**, Şubat 27, 2013, https://inmoscowsshadows.wordpress.com/2014/ 07/06/the-gerasimov-doctrine-and-russian-non-linear-war/, (Erişim Tarihi 24 Mart 2016).

GILES, Keir, "Russia's Public Stance on Cyber Space Issues"**, 4th International Conference on Cyber Conflict**, Tallinn, NATO Cooperative Cyber Defense Centre of Excellence, 2012, http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublics, (Erişim Tarihi 23 Mart 2016).

HEICKERÖ, Roland, "Emerging Cyber Threats and Russian Views on Information Warfare and Operation", **Swedish Defense Research Agency Press**, March 2010, http://www.foi.se/rapport?rNo=FOI-R--2970--SE, (Erişim Tarihi 23 Haziran 2016), ss. 1-70.

http://archive.mid.ru//brp_4.nsf/0/6D84DDEDEDBF7DA644257B16005 1BF7F, (Erişim Tarihi 26 Haziran 2016).

http://www.scrf.gov.ru /documents/99. html, (Erişim Tarihi 23 Mart 2016).

http://www.scrf.gov.ru/documents/6/114.html, (Erişim Tarihi 26 Haziran 2016).

http://www.scrf.gov.ru/documents/99.html, (Erişim Tarihi 23 Haziran 2016).

LUCAS, Edward, NIMMO, Ben, "Information Warfare: What Is It and How to Win It", **Center for European Policy Analysis (CEPA)**, http://cepa.org/sites/default /files/Infowar%20Report.pdf, (Erişim Tarihi 20 Nisan 2016), ss. 1-26.

MEDVEDEV, A. Sergei, *Offence-Defence Theory Analysis of Russian Cyber Capability*, Naval Post-Graduate School, Master Thesis, Monterey, Colifornia, https://www.google.com.tr/?gfe_rd=cr&ei=qzHZVrreN7Go8wf MuYegDw #q=this+thesis+represent+mikhail+tsypkin, (Erişim Tarihi 05 Mart 2016), ss. 1-100.

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

NATO Communications Centre of Excellence, Resmi İnternet Sayfası, "Social Media as a Tool of Hybrid War", http://www .stratcomcoe.org/social-media-tool-hybrid-warfare, (Erişim Tarihi 19 Ekim 2016).

NATO Cooperative Cyber Defence Centre of Excellence, Resmi İnternet Sayfası, National Security Concept of Russian Federation, https://ccdcoe.org/cyber-security-strategy-documents.html, (Erişim Tarihi 23 Mart 2016).

NATO Cooperative Cyber Defense Centre of Excellence, Resmi İnternet Sayfası, 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 2016).

The Gerasimov Doctrine and Russian Non-Linear War, **In Moscow's Shadows**, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russiannon-linear-war/., (Erişim Tarihi 24 Mart 2016).

The Russian Ministry of Defense, Resmi İnternet Sayfası, Concept of the Foreign Policy of the Russian Federation, http://archive.mid.ru//brp_4.nsf/0/76389FEC168189ED4 4257B2E0039B16D, (Erişim Tarihi 24 Mart 2016).

The Russian Ministry of Defense Resmi İnternet Sayfası, 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).

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).

YILMAZ, Salih, **Rusya Neden Suriye'de?**, Ankara, Yazar Yayınları, 2016.

IGU J. Soc. Sci., 4 (1), 2017, pp. 19-40.

İGÜ Sos. Bil. Derg., 4 (1), 2017, ss. 19-40.

Summary

As a cyber power at the present day, the Russian Federation (RF) is in the position of one of the most important players which dominate the cyber space. The foundation of the details related to the systematic and planning of this power can be analyzed on approximately qty. 10 official and non-official doctrines, together with strategic documents which RF put forth during the early 2000's related to the cyber space. RF which presently has a broad cyber warfare capability consisting of activities and planning consisting of espionage, counter / espionage, disinformation, electronic warfare, psychological warfare and propaganda, and cyber-attack, is capable of employing its cyber effectiveness and power, together with the new battle strategies revealed by following closely the developments in cyberspace as a tool to apply pressure in order to achieve its present foreign policies.

Within the context of the views which Chief Of Staff Valery Gerasimov had put forward in his article, "Military The Value of Science in Prediction", which he had published on February of 2013, RF's "cyber combat power" has transformed into "mixed military operation strategy" which is supported by "special force operations" and "information warfare" planning. Through time, this new military strategy has been conceptualized as "hybrid war, dirty war," "non-linear war," "new war," "blurred war" in international relations discipline.

Within the context of this doctrine, RF applied information warfare strategy in her relations with Estonia, Georgia, Kyrgyzstan and Ukraine. The tension which had started after Turkish F-16 aircraft had downed a Russian Su-24 aircraft on 24 November 2015 after the aircraft had violated Turkish airspace was transferred to a new stage after "DDoS" attacks to Turkey on 14 December 2015. The reason being that following these attacks it was believed in the public opinion that RF was applying information warfare strategy in his relations with Turkey.

When we consider that today subjects which are related to the security of states, are closely coordinated with developments in technology, it is very clear that state of not having technologies in the field of cyber space will create vulnerabilities in the field of security. In the same manner, all of the organizations and strategies which had been shaped in accordance with traditional security approach of the states must be reorganized and reshaped in order to create an effective cyber-attack and cyber defense capacity.

In compliance with this evaluation, it is very clear that during the post-Cold War period and especially at the beginning of the 2000s, RF has tried to reorganize both its army and intelligence units and corporate structures in

IGU J. Soc. Sci., 4 (1), 2017, pp. 19-40.

order to obtain an effective cyber-attack capability within the context of the new capabilities which are provided by the cyber space and that within the context of this organization, RF gives great importance to new generation of information warfare planning. The new generation cyber propaganda capabilities which is the most important component of cyber-attack capability which has been developed in a planned manner by RF for almost ten years, is much beyond the strategy which had been put forward by the Union of Soviet Socialist Republics (USSR) during the Cold War Period in the field of information warfare. It is now quite sophisticated.

Within this context, as it is claimed RF's support of the effects of a conventional war with propaganda by means of cyber-attacks which made Estonia's computing systems inoperable in 2007; RF's cyber activities during its war against Georgia in 2008; following that its cyber-attacks which took place against Lithuania in 2008 and against Kyrgyzstan in 2009 and the "new generation" combat concept which RF put forward during its intervention to Ukraine and following that "DDoS" attacks conducted against Turkey following the crises related to shooting down of an aircraft are noteworthy examples of this country's capacity in space.

RF's powerful and aggressive role in information warfare was able to be clearly observed during the crises when a Russian aircraft had been "shot down" by Turkish aircraft. As it can be seen in the Turkey example, it is very clear that RF has placed the information warfare at the center of the modern security strategy. As a result of this strategic approach, it is also apparent that RF centered media organizations are capable of displaying a different information warfare in any region of the world and in every country in that region by means of an effective and widespread social media network. Within this context, in compliance with the political objectives which are pursued, together with the flexible structure of RF's information warfare structure, RF is capable of supporting Russian minorities in the Baltic countries and make references to bright old days with Soviet-era nostalgia. In a similar manner, by means of the subject information warfare capability RF is able to observe compatible with AK Party's opposition circle and thus it is able to wear off AK Party's effectiveness among the people; it is able to continuously remind Azeri Turks about Turkey-Armenia rapprochement during the years 2008-2009 and thus create antagonism against Turkey in Azerbaijan; it is capable of determining publication policy with an environmentalist and anti-militarist tendency in Slovakia and Czech Republic; it is stated in Central Asia that Turkey is continuing to pursue Turanist policies, and hostile news about Turkey and the West are continuously given to the public.

As a result, it is apparent that throughout the tension experienced with Turkey following the crises caused by downing of an aircraft, RF has exhibited a well planned and financed and target oriented information warfare strategy performance aware of decentralization. Effective and aggressive publishing policies which were continued through international media organizations supported by local elements which were manipulated under the mask of opposition to AK Party and Recep Tayyip Erdogan and which was supported by social media sharing supported by visual imagery prepared by professional means comprised the foundation of this strategy.