RUSYA FEDERASYONU'NUN SİBER GÜVENLİK STRATEJİSİ: KIRIM ÖRNEĞİ*

Servet Habip TOPÇU**

Makale Geliş Tarihi/Received: 28/03/2022
Makale Kabul Tarihi/Accepted: 08/06/2022
Makale Yayın Tarihi/Published: 30/06/2022
Atıf için/To cite: Topçu, S. H. (2022). Rusya Federasyonu'nun Siber Güvenlik Stratejisi: Kırım Örneği. *Uluslararası İlişkiler Çalışmaları Dergisi, 2*(1), 19-35.

Özet: Uluslararası İlişkiler alanının, ilgi odağında olan sorunlardan biri de güvenlik sorunudur. Güvenlik algısı, tarihsel olarak birçok değişime uğramıştır. Teknolojik gelişmeler, yaşanan bu değişim için itici unsurlardan olmuştur. 21. yüzyıl itibariyle, siber güvenlik, devletler ve uluslararası toplum için önemli meselelerden biri haline gelmiştir. Rusya Federasyonu da siber alanın ve siber güvenliğin erken farkına varan ülkelerden birisidir. Rusya Federasyonu, yayınladığı belgelerle ve gerçekleştirdiği iddia edilen saldırılarla siber alanda dikkate alınması gereken ülkelerden biri olduğunu göstermiştir. Bu çalışmanın ana odağını, Rusya Federasyonu'nun siber güvenliğe dair yayınladığı belgelerde ortaya koyduğu strateji ile gerçekleştirdiği iddia edilen olaylar arasında bir uyum olup olmadığını anlamak oluşturmaktadır. Ayrıca, Rusya Federasyonu'nun siber güvenlik stratejisini bir örnek olay üzerinden anlamak bu makalenin diğer bir amacıdır. Rusya Federasyonu tarafından yayınlanan resmî belgelerdeki savunmacı üslup ile Kırım'da siber alana ilişkin sergilenen saldırgan tavır arasında bir uyum bulunmamaktadır. Ancak bilgi savaşının diğer bir boyutu olan medya kısmında ise resmî belgelerde ifade edilen hususların Kırım örneği üzerinde uygulandığı açıkça görülmektedir.

Anahtar Kelimeler: Siber Güvenlik, Bilgi Savaşı, Rusya Federasyonu, Kırım

CYBER SECURITY STRATEGY OF THE RUSSIAN FEDERATION: THE CASE OF CRIMEA

Abstract: The security problem is one of the problems in the focus of attention of the field of international relations. The perception of security has undergone many changes historically. Technological developments have been one of the driving factors for this change. By the 21st century, cyber security has become one of the important issues for states and the international community. The Russian Federation is one of the countries that became aware of cyberspace and cyber security early. The Russian Federation is one of the countries that should be taken into account in the cyber field, considering the documents it has published and the alleged attacks that were carried out by Russia. The main focus of this study is to understand whether there is a coherence between the documents published by the Russian Federation on cyber security and the events in which Russia is mentioned, and to understand the cyber security strategy of the Russian Federation. There is no coherence between the defensive wording in the official documents published by the Russian Federation and the aggressive attitude displayed in Crimea. However, in the media part, which is another dimension of the information war, it is clearly seen that the issues expressed in the official documents are applied to the example of Crimea.

Keywords: Cyber Security, Information War, Russian Federation, Crimea

* Bu çalışma, 21-22 Nisan 2022 tarihinde Atatürk Üniversitesi Uluslararası İlişkiler Bölümü tarafından düzenlenen I. Uluslararası İlişkiler Lisansüstü Öğrenci Kongresi'nde özet bildiri olarak sunulmuştur.

** Araştırma Görevlisi, Hatay Mustafa Kemal Üniversitesi, Uluslararası İlişkiler Bölümü, servethabip.topcu@mku.edu.tr

https://orcid.org/0000-0002-6046-7441

Giriş

Uluslararası ilişkilerin temel aktörlerinden olan devletlerin, egemenlikleri ve bununla bağlantılı olarak ulusal güvenlikleri önem taşıyan bir konudur. Ulusal güvenlik konusu küreselleşme süreciyle birlikte değişim yaşayan bir kavram olmuştur. Uluslararası gündemi oluşturan ihtilafların ve konu başlıklarının farklılaşması, güvenlik kavramının ele alınış biçimini etkileyen faktörlerin başında gelmektedir. Uluslararası politikada gündemin yanı sıra aktörlerin de değişmesi ve çeşitlenmesi ulusal güvenlik yaklaşımlarında birçok değişimi gerektirmiştir. Uluslararası örgütler, bireyler ve çokuluslu şirketler gibi yeni aktörler sisteme katılmıştır. Tüm bunlara ek olarak, yaşanan teknolojik gelişmeler, devletlerin ulusal güvenlik stratejilerine yeni bir başlığı eklemelerini bir zorunluluk haline getirmiştir. Yaşanan teknolojik gelişmeler, sosyal yaşantının yanı sıra ulusal politikaları ve birçok alanda kullanılan araçları da farklılaştırmıştır. Siyasi, ekonomik, sosyal, kültürel ve askerî alanlarda kullanılan birçok araç dijitalleşerek internet ağlarına bağlı hale gelmiştir. Teknolojik anlamda yaşanan ilerlemeler, hayatın birçok alanında kolaylık sağlamasına karşılık; siber alandan kaynaklı tehditler artmış ve siber güvenlik kavramı devletleri ilgilendiren bir konu haline gelmiştir.

Devletler, 2000'li yılların başından itibaren siber uzaydan kaynaklı tehditlerin arttığını ve bu alanı güvenlik politikaları içerisine dâhil etmeleri gerektiğini fark etmişlerdir. Bu çalışmanın konusu olan Rusya Federasyonu (bundan sonra Rusya diye bahsedilecektir) özelinde konuya yaklaşılırsa, Rusya 2000 yılı itibariyle siber güvenlik alanında harekete geçen öncü ülkelerden birisi konumundadır.

Bu çalışmada ilk olarak siber güvenlik kavramı tanımlanıp önemine değinilecektir. Akabinde siber güvenliğe ilişkin yayınlanan resmî belgeler ve doktrinler üzerinden, Rusya'nın siber güvenlik meselesine yaklaşımı sunulacaktır. Son olarak, Kırım'ın ilhakı sürecinde (2014) yaşanan olaylar siber uzay açısından değerlendirilip Rusya'nın siber güvenlik stratejisinin söylem ve eylem açısından tutarlılığı bilimsel ilkeler ışığında tartışılacaktır.

1. Siber Güvenlik

Siber uzay kavramının üzerinde uzlaşılmış bir tanımı yoktur. Bir tanıma göre, siber uzay "*internet, iletişim ağları, dış dünyaya kapalı askerî ağlar, enerji hatları ağları, cep telefonları yazılım altyapılı telsizler, elektronik komuta sistemleri, cep telefonları, uydu sistemleri, insansız hava araçları sistemleri gibi birçok yazılım ve donanım elemanlarının toplamı*" şeklinde ifade edilebilir (Akyazı, 2013: 216). Siber uzay kavramının tanımlanması farklı şekillerde ele alınıyor olsa da günlük hayattan, askerî ve ekonomik konulara kadar, geniş çapta önemli etkilere sahip bir kavram olduğu kesindir.

Siber uzay kaynaklı tehditler, bir taraftan devletler için güvenlik sorunu yaratan savaş ortamının oluşmasına neden olurken (Güntay, 2017: 84); diğer taraftan ise devletler için ulusal güvenlik problemi yaratacak boyutlara ulaşmıştır. Örneğin; devletlerin kritik altyapısı kabul edilen enerji, elektrik, ulaşım ve haberleşme gibi sistemlerine saldırılar düzenlenebilmekte, çeşitli araçlar/teknikler vasıtasıyla kamuoyu oluşturulup devletin siyasi ve sosyal istikrarı hedef alınabilmektedir. Bu noktadan hareketle siber güvenlik kavramı, güvenlik yaklaşımları içerisinde ele alınan bir kavram haline gelmiştir. Uluslararası Telekomünikasyon Birliği (ITU) siber güvenliği: "*…kurumları ve kullanıcı varlıklarını korumak adına kullanılabilecek araçların,*

politikaların, güvenlik konseptleri ve yönergelerinin, risk yönetim yaklaşımlarının, eylemlerin ve teknolojilerin toplamı" şeklinde tanımlamaktadır (ITU, t.y.). Dolayısıyla siber güvenlik, siber uzay kaynaklı her türlü tehdidin önlenip güvenliğin sağlanması olarak tanımlanabilir.

Kavramsal anlamda bir uzlaşı olmamakla birlikte, Soğuk Savaş'tan sonra devletler ordularını, teknolojilerini, istihbarat ağlarını vb. bu alana yönelik yeniden bir uyarlama girişimi içerisine girmişlerdir. Siber güvenlik meselesi, hem ulusal güvenlik hem de uluslararası güvenlik açısından giderek daha büyük bir rol oynamaktadır (Thomas, 2014: 104). Bununla birlikte, devletler siber uzaydan gelebilecek tehditlere karşı yeni ulusal güvenlik stratejileri geliştirme çabası içinde olmuşlardır. Bu açıdan bakıldığında, siber güvenliğe dair ilerleme kaydeden devletler bir yandan güvenliklerini sağlarken diğer taraftan yeni bir rekabet alanı yaratmışlardır (Darıcılı, 2017: 33). Çünkü bir devletin bu alanda somut kaynaklara sahip olması diğer bir devletlere karşı üstünlük kurması anlamına gelebilecektir.

Devletler, geleneksel güvenlik anlayışına göre şekillenmiş kurumlarını, işlevsel siber güvenlik ve savunma kapasitesine sahip olmak için yeniden şekillendirme yoluna gitmişlerdir. Daha önce hava, deniz, kara ve uzayda gerçekleştirilen silahlı mücadele alanına bilgi alanı veya siber alan olarak ifade edilebilecek yeni bir alan daha katılmıştır (Tchekinov ve Bogdanov, 2013: 13). Bu doğrultuda, konvansiyonel savaş ve savunma stratejilerine ek olarak devletler, siber uzayın ruhuna uygun bir şekilde yeni stratejiler geliştirmişlerdir. Siber güce ve silahlara sahip olan devletler, bu unsurları uluslararası anlaşmazlıklarda konvansiyonel silahlar ile birlikte kullanıp çeşitli kazanımlar elde etmişlerdir. Böylece konvansiyonel ve siber saldırı silahlarının bir arada kullanıldığı, hibrit savaş olarak tanımlanabilecek yeni bir savaş modeli ortaya çıkmıştır.

Hibrit kavramı basitçe, melez yani bir tür karışım şeklinde ifade edilebilir. Erol ve Oğuz (2015: 263), bu noktadan hareketle hibrit savaşın en az iki farklı savaş türünü içermesi gerektiği üzerinde durmuşlardır. Hibrit savaş, genel bir ifadeyle politik, askerî ve siber tüm imkânların bir çatışma sırasında koordineli bir şekilde kullanımını ifade etmektedir (Karabulut, 2017: 126). Bu kapsamda belirtilmesi gereken hususlardan bir diğeri de hibrit savaş modelinin konvansiyonel araçları ve yöntemleri dışlamayışıdır. Bu yeni savaş anlayışı konvansiyonel ve modern araçların birlikte kullanımını içermektedir.

Hoffman (2007: 8), "*hibrit savaşın, geleneksel yetenekler, düzensiz oluşumlar, ayrım gözetmeyen terörist eylemler ve cezai düzensizlik dâhil olmak üzere çok çeşitli savaş tarzlarını içerdiğini*" ileri sürmektedir. Kofman ve Rojansky ikilisi (2015: 2), hibrit terimi, geleneksel, düzensiz, politik veya bilgi savaşlarının bir kombinasyonu şeklinde ifade etmektedir. Karabulut ise hibrit savaşın temel özelliklerini, (2017: 126), "*Düzenli ordulardan ve yarı otonom hareket eden hücrelerden oluşan karma askerî bir yapılanma; esnek ve her şarta uyum sağlayabilen pragmatik strateji; aşırıcı şiddet kullanma temayülü oldukça yüksek sansasyonel terör eylemleri; sosyal medyayı aktif ve saldırgan bir şekilde kullanan propaganda ağı ve bilgi savaşı tekniklerinin devreye sokulduğu bir iletişim stratejisi; finansal kaynak sağlamak için bütün illegal yolları kullanan yasa dışı bir suç ağı ve son olarak, savaş hukukunun temel prensiplerini göz ardı eden bir tür anarşik uluslararası hukuk yorumu*" şeklinde tanımlamıştır.

Rusya perspektifinden bu konuya bakıldığı zaman, 2012 yılında Rusya Genelkurmay Başkanı olarak atanan Valery Gerasimov'un "*The Value of Science in Prediction / Öngörüde Bilimin Değeri*" başlıklı makalesi ön plana çıkmaktadır. Gerasimov'un ortaya koyduğu yaklaşım *Gerasimov Doktrini* olarak da anılmıştır. Gerasimov Doktrini ile açıklanan prensipler çizgisinde

Rusya, askerî olmayan yöntemleri, askerî gücü ve stratejisi içerisine katarak, olası çatışma ve kriz durumlarını yürütme ve yönlendirme amacında olmuştur (Darıcılı, 2017: 152). Gerasimov, yeni savaş anlayışının, "*nüfusun protesto potansiyeliyle ortak gerçekleştirilen politik, ekonomik, siber, insani ve diğer askerî olmayan yöntemlerin kullanımı yönünde*" değiştiğini ileri sürmektedir. Rusya'nın 2013 yılında başlayan Ukrayna krizine yönelik yaklaşımı, Gerasimov'un ortaya koyduğu yaklaşımla uyuşmaktadır.

Bütün bu bilgilerden hareketle, siber uzay yapısından kaynaklı tehditler, devletleri yeni güvenlik anlayışlarına yöneltmiştir. Devletler, güvenlik stratejilerini küreselleşme ve dijitalleşme olgusuyla şekillenen 21. yüzyıla uyarlama mecburiyeti içerisine girmişlerdir. Siber alandan kaynaklı tehditlerin önlenmesi, devletler için göz ardı edilemeyecek bir olgu haline gelmiştir. Bu doğrultuda, geleneksel güvenlik stratejileri, bu yeni yaklaşımla uyum içerisinde çalışacak biçimde revize edilmiştir.

Ulusal güvenlik belgelerine, siber güvenliğin gerekliliklerini dâhil eden Rusya, bu alanda elde ettiği gücü konvansiyonel gücü ile birleştirmiştir. Bu konuda Ukrayna-Gürcistan örnekleri yeni savaş ya da hibrit savaş modeline uygun örnekler oluşturmaktadırlar. Ukrayna müdahalesi esnasında, Rusya birçok askerî ve siber unsuru bir arada kullanan bir yaklaşım sergilemiştir. Dolayısıyla bu savaş tarzı, hibrit savaş ya da yeni savaş şeklinde değerlendirilebilir. Rusya'nın Ukrayna müdahalesi NATO gibi önemli kuruluşlar tarafından da hibrit savaş olarak tanımlanmıştır.

2. Rusya'nın Siber Stratejisini Oluşturan Temel Belgeler

Rusya, siber uzaya yönelik politikalarını ve stratejilerini erken dönemde oluşturan ülkelerden biridir. Öncelikle Rusya, Sovyetler Birliği'nden miras kalan teknolojik alt yapıyı çoğunlukla kendisine aktarabilmeyi başarmıştır (Acar ve Pekcandanoğlu, 2020: 170). Bu doğrultuda, Sovyetler Birliği'nden aktarılan tarihsel ve kültürel akıl, Rusya'yı siber stratejilere yönlendiren unsurlardan birisi olmuştur.

Bir diğer önemli etken, 1990-1991 Körfez Savaşı sırasında Koalisyon kuvvetlerinin kullandığı iletişim ve enformasyon yöntemleri, Rus yetkilileri tarafından yakından takip edilmiştir (Darıcılı ve Özdal, 2017: 123). Rusya'yı enformasyon güvenliği alanında stratejiler geliştirmeye iten bir diğer etken, 1994-1996 Rus-Çeçen Savaşı esnasında yaşanan olaylardır. Çeçenler tarafından kullanılan iletişim yöntemleri, Rusya'nın uluslararası alandaki imajını olumsuz etkilemiştir (Acar, 2020: 89). Bu olaylardan hareketle, enformasyon savaşı alanındaki gelişmeler Rus karar alıcılar tarafından daha yakından izlenmeye başlanmıştır. Uluslararası alanda yaşanan teknolojik gelişmeler, askeri yeteneklerin değişen niteliği ve çatışma ortamlarında kullanılan enformasyon tekniklerinin etkinliği Rusya tarafından birçok olay aracılığıyla tecrübe edilmiştir. Rusya'nın siber alana ciddi anlamda ilgisinin başladığı yıl olan 2000 yılı ile birlikte Rusya siber alana dair doktrinler ve strateji belgeleri yayınlamaya başlamıştır. Söz konusu belgeler Rusya'nın siber stratejisinin temellerini oluşturmaktadır.

Bu belgelerden 24 Ocak 2000 tarihinde yürürlüğe giren "*National Security Concept of the Russian Federation / Rusya Federasyonu Ulusal Güvenlik Konsepti*" başlıklı belge, "*bilgi güvenliği*" kavramının ilk defa kullanıldığı belge olması açısından önemlidir (Rusya Federasyonu Dışişleri Bakanlığı (MID), 2000). Belgenin içeriği Rusya'nın siber stratejisinin gelecekte nasıl

şekilleneceğine dair bir çerçeve sunmaktan ziyade sadece bu alanın öneminden bahseden bir içerik taşıdığı söylenebilir (Darıcılı, 2017, s. 145). Yayınlanan bu belgede özetle (MID, 2000):

- *Ekonomik, politik, teknolojik, çevresel ve enformasyon faktörlerinin uluslararası alanda giderek daha fazla rol oynadığı;*
- *Enformasyon güvenliği alanındaki gelişmelerin, Rusya'nın ulusal çıkarlarını oluşturan bir bütünün parçası olduğu;*
- *Rusya'nın enformasyon alanındaki çıkarlarının, modern iletişim teknolojilerinin gelişiminde ve devletin enformasyon kaynaklarına izinsiz erişimin engellenmesinde yattığını;*
- *Enformasyon alanında, bilgi ve telekomünikasyon araçlarının normal işleyişinin bozulması, veri güvenliğinin sağlanamaması ve bu verilere izinsiz erişim gibi, Rus ulusal güvenliğine yönelik artan bir tehdidin var olduğu vurgulanmaktadır.*

Söz konusu belge analiz edildiğinde; enformasyon güvenliği açısından bazı tehditlerin tanımlandığı ve ve bu tehditlere yönelik bir kısım tedbirlerden söz edildiği göze çarpmaktadır. Bu açıdan bakıldığı zaman, güçlü bir strateji ortaya konulmamasına karşılık, Rusya'nın siber alandan kaynaklı tehditlerin farkında olduğu anlaşılmaktadır.

Rusya'nın siber güç olma yolunda attığı en önemli adımlardan birisi olan ve bilgi güvenliği görüşünü yansıtan ilk temel belge "*Information Security Doctrine of the Russian Federation/Rusya Federasyonu Enformasyon Güvenliği Doktrini*" başlıklı belgedir (ITU, 2008). 9 Eylül 2000 tarihinde yürürlüğe giren belge, Rusya'nın siber güvenlik alanındaki ana yol haritasını oluşturan ve bilgi güvenliğine yönelik hükûmet politikasına temel teşkil eden belgelerden birisidir. Söz konusu belge, Rusya'nın bilgi güvenliğini sağlamaya yönelik amaçlar, hedefler, ilkeler ve temel yönergeler hakkındaki resmî görüşlerin toplamını temsil etmektedir.

2000 yılında yayınlanan bu doktrin, yayınlandığı dönem itibariyle Rusya'nın bilgi güvenliğine yaklaşımını ve bilgi güvenliğinin ayrılmaz bir parçası olan siber meseleleri düzenleyen temel belge görünümünü taşımaktadır (Giles, 2012: 70). Belgede enformasyon güvenliğinin önemine aşağıdaki ifadelerle dikkat çekilmiştir: "*Toplumsal yaşamın sistem oluşturan bir faktörü olarak enformasyon alanı, Rusya Federasyonu güvenliğinin siyasi, ekonomik, savunma ve diğer bileşenlerinin durumunu aktif olarak etkiler*" (ITU, 2008). Doktrinde enformasyon güvenliği alanında Rusya'ya yönelik sıralanan tehditlerden bazıları aşağıda listelenmiştir (ITU, 2008):

- *Rus haber ajanslarının ve medyasının ulusal enformasyon alanında etkinliğinin azalması ve yabancı medya kuruluşlarına bağımlılığın artması;*
- *Dezenformasyon;*
- *Yabancı siyasi, ekonomik, askerî, istihbarat ve enformasyon kuruluşlarının faaliyetleri;*
- *Önde gelen küresel güçlerin teknolojik üstünlüğünün artması;*
- *Devletlerin enformasyon alanlarına tehlikeli saldırılar için araçlar geliştiren, telekomünikasyon sistemlerinin normal işleyişini bozan, enformasyon kaynaklarının güvenliğini ihlal eden bir dizi enformasyon savaşı konseptinin geliştirilmesi.*

Doktrin, Rusya'nın ekonomisini, sivil toplumunu ve siyasal sistemini geliştirmeye ve yabancı devletlerden gelebilecek olan tehditleri tanımlamaya odaklanmıştır (Medvedev, 2015: 55-56). Ortaya konulan tehditlerden sonra, bu tehditlerin önüne geçmek ve Rusya'nın bu alanda ulusal güvenliğini temin etmek için birtakım önlemler sıralanmıştır. Söz konusu belgede dikkat

çekici bazı hususlar bulunmaktadır. Bunlardan ilki, Doktrinin medyaya karşı tutumudur. Medya, kamuoyunun, hükûmet lehinde şekillendirilmesi için kullanılması ve yönetilmesi gereken bir araç olarak görülmektedir (Giles, 2012: 70). Medya hakkında önemli ifadeler aşağıda listelenmiştir (ITU, 2008):

- *Rusya Federasyonu'nun devlet politikası ve resmî konumu hakkında güvenilir bilgilerin, Rus ve yabancı vatandaşlara iletilmesi için devlet kitle iletişim araçlarının desteklenmesinin gerekliliği;*
- *Devlet televizyon ve radyo yayın kuruluşlarının ve diğer devletler tarafından yönetilen kitle iletişim araçlarının, enformasyon politikasını şekillendirme hususunda devlet katılımının etkinliğinin artırılması*

Ayrıca bu doktrinde ulusal medyanın, Rus dış politikasını, uluslararası kamuoyuna aktarmasını engelleyen girişimler de Rusya'nın enformasyon güvenliğine yönelik tehditler arasında kabul edilmiştir. (Medvedev, 2015: 56).

Doktrinde, bilgi güvenliği alanında artan silahlanma yarışına dikkat çekilmekte ve yapılacak uluslararası iş birliğinin, uluslararası toplumun tüm üyelerinin enformasyon güvenliğini arttırmasına yardım edecek bir yapıda olması gerektiği belirtilmektedir. Söz konusu belgenin geneli üzerine bir yorum yapılacak olursa, saldırgan bir beyandan ziyade, savunma yönü ağır basan bir dil ile yazıldığı görülmektedir (Giles, 2011: 47). Bu doktrin, istihbarat ve elektronik muharebe için önlemlerin, bilgi, propaganda ve psikolojik operasyonlara karşı koyma yöntemlerinin ve araçlarının iyileştirilmesine yönelik görevleri öncelikli olarak belirlemiştir.

Öte yandan, 12 Mayıs 2009 tarihinde yayınlanan "*Russia's National Security Strategy to 2020/ 2020'ye Doğru Rus Ulusal Güvenlik Stratejisi*" başlıklı belge, ekonomiden sağlığa birçok alanı derinlemesine ele alırken bilgi güvenliği konusuna dolaylı yollardan değinmektedir (ETH Zurich, 2009). Derinlemesine bir yaklaşım olmasa da siber alandan kaynaklı tehditlerin Rus ulusal çıkarlarını tehdit ettiği gerçeği kabul edilmektedir (Medvedev, 2015: 57). Söz konusu belgede, bilgi güvenliğine ilişkin maddeler şu şekildedir (ETH Zurich, 2009):

- *Sibernetik ve yüksek teknoloji alanında yasadışı faaliyetlerin gelişmesi, Rus ulusal güvenliği üzerinde olumsuz bir etkiye sahiptir;*
- *Küresel enformasyon mücadelesinin artması, ülkelerin istikrarına, ekonomilerine, sosyal şartlarına ve kurumlarına yönelik tehditleri artıracaktır;*
- *Bilişim ve telekomünikasyon alanlarında teknolojik geri kalmışlığın giderilmesi; hükûmet, askeri yönetim sistemleri ve kritik öneme sahip sistemlere yönelik bilgi güvenliği teknolojilerinin geliştirilmesi ve ulusal enformasyon alt yapısının küresel bilgi ağlarıyla uyumlu hale getirilmesi gerekmektedir;*
- *Kritik öneme sahip alt yapı ve yüksek riskli tesislerin bilgi ve telekomünikasyon güvenliği ile kurumsal ve bireysel enformasyon güvenliği düzeyini artırarak ve ulusal güvenlik sistemi için birleşik bilgi telekomünikasyon sistemi oluşturarak ulusal güvenliğe yönelik enformasyon tehditleri önlenir.*

Söz konusu belge incelendiğinde; daha çok Rus sivil toplumuna ve kritik alt yapı ve sistemlerine yönelik tehditler ve bu kapsamda alınması gereken tedbirler dar kapsamlı bir şekilde ele alındığı görülmektedir.

2011 yılında yayınlanan "*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*" başlıklı belge, "*Rus Ordusu'nun enformasyon alanındaki rolünün ilk resmî bildirimi ve bir Rus ön siber savaş doktrini olarak*" tanımlanmaktadır (Giles, 2012: 67). *Kavramsal Görüşler* belgesi, Rusya Silahlı Kuvvetleri'nin küresel enformasyon alanındaki faaliyetlerine yönelik temel ilkelerini, kurallarını ve güven artırıcı önlemlerini ele almaktadır. Söz konusu belge, Rusya Silahlı Kuvvetleri'ne enformasyon alanındaki faaliyetlerine ilişkin rehberlik edecek yönergeler sunmaktadır (Thomas, 2014: 109). *Kavramsal Görüşler* 'de, "*... kara, deniz, hava ve uzayın yanı sıra gelişmiş ülkelerin orduları tarafından enformasyon alanı çeşitli amaçlar için kullanılmaya başlanmıştır*" (Siber Savunma İşbirliği Mükemmeliyet Merkezi/Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2011) ifadesiyle siber alanın devletlerarası mücadele için beşinci bir boyut oluşturduğu kabul edilmektedir. Ayrıca, Rusya'nın ulusal güvenliğine yönelik yeni bir tehdidin varlığı, "*Dünyada hızla yayılmaya başlayan enformasyon silahlarının rolü nedeniyle, Rusya küresel enformasyon alanından kaynaklanan yeni bir tehditle karşı karşıyadır"* (CCDCOE, 2011), ifadesiyle kabul edilmektedir. Dikkat çeken diğer bir ifade ise, siber alanın Rus ulusal güvenliğinin bir parçası olarak görüldüğünün açıkça belirtilmesidir: "*Rusya Federasyonu bilgi güvenliği sistemi, bilgi güvenliği alanında devlet politikasını uygulamak için tasarlanmış, ülkenin ulusal güvenlik sisteminin bir parçasıdır*" (CCDCOE, 2011).

Belgede, enformasyon savaşı kavramı, "*Kritik sistemlere, kaynaklara ve yapılara zarar vermek; siyasi ekonomik ve sosyal yapıyı bozmak için nüfusun beynini yıkamak ve ayrıca devleti, diğer tarafların çıkarları doğrultusunda karar almaya zorlamak için kritik öneme sahip yapılara zarar verme durumu"* olarak tanımlanmıştır (CCDCOE, 2011). Enformasyon alanı hakkında tanımlamalar göz önüne alındığında, Rusya'nın ilgili tanımlamaları ABD'nin siber uzaya yaklaşımından daha geniş bir perspektif sunmaktadır (Medvedev, 2015: 60). Enformasyon alanından kaynaklı tehditler, sadece elektronik sistemlere ya da kritik alt yapılara yönelik saldırılar olarak görülmemiştir. Bunun yanı sıra yürütülen propaganda ve dezenformasyon faaliyetleri aracılığıyla sosyal yapı ve bilince yönelik tehditlerin de kaynağı olarak enformasyon alanı görülmüştür. Bu doğrultuda hem ulusun hem de askeri personelin söz konusu faaliyetlerden kaynaklı tehditlerden korunması kapsamında alınması gereken önlemler belirtilmiştir.

Kavramsal Görüşler, ilk olarak "yasallık" ilkesi hükümleriyle başlamaktadır. Bu bölümde, Rusya Silahlı Kuvvetleri'nin enformasyon alanındaki faaliyetlerinin, Rus ulusal hukukuna ve uluslararası hukuka uygun bir şekilde yürütüleceği belirtilmektedir. Dikkat çeken bir diğer husus ise "iş birliği" ilkesidir. Rusya, enformasyon alanında küresel iş birliğine dikkat çekerek, bu alandaki faaliyetleri düzenleyen bir uluslararası yapının oluşmasını amaçlamaktadır. Rusya Silahlı Kuvvetleri'nin meydana gelebilecek olası bir savaş durumunda uyması gereken talimatların belirtildiği bölümde de söz konusu çatışmaların önlenmesi ve çözülmesi noktasında uluslararası iş birliğine vurgu yapıldığı göze çarpmaktadır. Enformasyon güvenliği sürdürebilmek için uluslararası kurumların önemi ve merkeziliği, uluslararası iş birliği açısından vurgulanan bir diğer hususdur. Rusya'nın, enformasyon güvenliği alanında uluslararası iş birliğinin teşviki konusunda yaptığı bu vurgu, Rus hükûmetinin ve ordusunun kendi enformasyon güvenliğini

sağlamasına duyulan güven eksikliğinden kaynaklandığı iddia edilmektedir (Medvedev, 2015: 61).

Kavramsal Görüşler belgesi, enformasyon güvenliği üzerine yayınlanan diğer Rus belgelerinde olduğu gibi savunma temasını yansıtan bir belge konumundadır (Giles, 2012: 68). Özetle ifade etmek gerekirse, 2011 yılında yayınlanan bu belgede, uluslararası iş birliği ve savunmacı anlayışın ön planda olduğu bir metin olmasıyla birlikte Rus ordusuna karşı tehditleri ve bu kapsamda alınacak tedbirleri içermesi bakımından askerî yönü ağır basan bir belgedir. Kavramsal Görüşler, Rus Silahlı Kuvvetleri'nin enformasyon alanındaki askerî faaliyetlerine ilişkin birçok talimatı içermesine rağmen, saldırgan siber faaliyetlerden hiç bahsedilmemesi belgenin eksik yönü olarak ön plana çıkmaktadır (Giles, 2012: 69).

27 Şubat 2013 tarihinde yayınlanan, 2012 yılında Rusya Genelkurmay Başkanlığı'na atanan Valery Gerasimov'un "*The Value of Science in Prediction/Öngörüde Bilimin Değeri*" makalesi ise ortaya yeni bir askerî yaklaşım koymuştur. Bu belgede bahsedilen stratejiler geniş yankı uyandırmış olup "*Gerasimov Doktrini*" olarak adlandırılmıştır. Gerasimov, makalesinde aşağıdaki noktalara dikkat çekmektedir (Galeotti, 2014):

- 21. yüzyılda savaş ve barış arasındaki çizgi artık daha da belirsiz hale geldiğinden savaş alışılmadık çerçevelerde gerçekleşmektedir;

- Savaşın bu yeni şekli, ortaya çıkardığı etki ve yıkım açısından, geleneksel savaşlar ile karşılaştırılabilir hale gelmiştir;

- Askeri olmayan araçların çatışmalarda istenen hedeflere ulaşmada etkinliği kanıtlanmış ve bazı durumlarda askeri araçların gücünü aşmıştır;

- Yeni kullanılan çatışma yöntemleri siyasi, ekonomik, enformasyon, insani ve diğer askeri olmayan araçları içermektedir. Söz konusu araçlar, hedef ülkenin nüfusunun protesto potansiyeli ile koordine bir şekilde kullanılmaktadır;

- Bütün bu araçlar, enformasyon savaşı eylemleri ve özel kuvvet harekâtı ile desteklenir. Bu araçlar gizli bir yapı içerisinde kullanılır. Askeri araçların açık kullanımı barışı koruma ve krizi yatıştırma görevleri adı altında gerçekleştirilir;

- Hedef ülkede oluşturulan bir cephe yani iç muhalefetin kullanılması ve enformasyon araçlarının kullanımı, düşmanın avantajlarını geçersiz kılacaktır;

- Enformasyon alanı karşı tarafın potansiyelini zayıflatmak için birçok olanak sunar. Bu alanda, Rusya Federasyonu faaliyetlerini mükemmelleştirmelidir.

Gerasimov, makalesinde savaşın değişen yapısının bir portresini sunmaya çalışmıştır. Savaşın değişen yapısından, kullanılan araçların değişen nitelik ve etkinliklerine dair birçok vurgu vardır. Rusya'nın yayınladığı resmî doktrinlerin aksine siber operasyonların çatışmalarda oynadığı role dair önemi, *Gerasimov Doktrini*'nde daha belirgindir (Medvedev, 2015: 62). Gerasimov'un tanımlamaya çalıştığı yeni savaşın içerisinde birçok etken ve araç mevcuttur. Bazı durumlarda bu araçlar, askeri araçlardan daha etkili olabilmektedir. Özellikle savaşın ilk safhasında enformasyon ve gizli askeri faaliyetlerinin yürütülmesi ve daha sonra *barışı koruma* görevleri adı altında askeri araçların görünür olması gerektiği görüşleri ayrıca önemlidir. Gerasimov, gerilimi azaltabilmek için enformasyon silahlarının kullanımından ziyade yalnızca söz konusu araçların saldırgan yönünü öne çıkarmaktadır (Medvedev, 2015: 63). Bu doktrinde,

resmî Rus doktrinlerinin aksine, Rusya'nın siber alandaki faaliyetlerine ilişkin daha saldırgan bir tutum benimsemesi gerektiği belirtilmektedir.

Rus askeri uzmanlar Tchekinov ve Bogdanov tarafından, *Askeri Düşünce* (*Military Thought*) dergisinde "*The Nature and Content of a New-Generation War/Yeni Nesil Savaşın Doğası ve İçeriği*" başlığıyla yayınlanan makaledeki görüşleri, Rusya'nın yeni savaş stratejisine ışık tutmaktadır. Yeni nesil savaşın aşamalarına ilişkin görüşleri, enformasyon savaşının yeni savaş içerisindeki önemini ortaya koymaktadır. Tchekinov ve Bogdanov, yeni nesil savaşa ilişkin, "*Yeni nesil savaşa, tarafların nüfusunu ahlaki ve psikolojik etki altına alacak enformasyon ve psikolojik savaş hâkim olacak ve bu savaşın yeni türünü kazanan asıl zaferin temellerini oluşturacaktır*" (Tchekinov ve Bogdanov, 2013: 16) görüşünü paylaşmaktadırlar. Tchekinov ve Bogdanov, askeri olmayan yöntemlerin yani ekonomik, enformatik ve teknolojik kampanyaların, yeni nesil savaşta düşmanı dengelemek için kullanılacaklarının altını çizmektedirler. Enformasyon alanında sağlanacak üstünlüğün nihai zafer açısından önemini şu sözlerle ifade etmektedirler: "*Yeni nesil bir savaşta, taraflardan birisinin diğerine üstünlük sağlaması, rakibine karşı enformasyon üstünlüğü sağlamasına bağlıdır*" (Tchekinov ve Bogdanov, 2013: 18). Adı geçen ikili, medya aracılığıyla yürütülecek dezenformasyon faaliyetlerinin öneminin de altını çizmektedirler.

Tchekinov ve Bogdanov, savaşın bu yeni şeklinde silahlı mücadelenin başlamasından önce enformasyon araçlarının kullanımıyla dezenformasyon faaliyetleri, hedef ülkeyi karıştırma, kritik alt yapılara saldırı ve istikrarsızlaştırma gibi faaliyetler yürütmenin önemini vurgulamaktadırlar. Siber saldırı ve dezenformasyon faaliyetleri, savaşın ilk safhasında yani ateşli silahların kullanımından önce çatışma sahnesinde görünür olacaktırlar. Belirtilen görüşlerin resmî niteliği olmamasına rağmen, 2014 yılında Kırım'ın ilhakı sürecinde yaşanan olaylarla söz konusu görüşlerin tutarlı olduğu söylenebilir. Bu makale, konusu gereği Rusya tarafından Kırım'ın ilhakı sürecine kadar (2014) yayınlanan doktrinleri dikkate almıştır.

3. Kırım'ın İlhakı ve Rusya'nın Bilgi Operasyonları

Ukrayna'da ilk olarak 2013 yılının sonlarında başlayıp ve daha sonra 2014 yılının ilk aylarında şiddetlenen olaylar neticesinde Kırım, Rusya tarafından ilhak edilmiştir. Bu süreçte yaşanan enformasyon ve siber kampanyalara değinmeden önce bu sürecin başlangıcını oluşturan *Euromaidan* protestolarından bahsedilecektir. Daha sonra, Kırım'ın ilhakı sürecinde, Rusya'nın başvurduğu enformasyon ve siber operasyonlara değinilecektir.

2010 yılında Ukrayna'da gerçekleştirilen seçimler neticesinde Viktor Yanukoviç iktidarı devralmıştır. Yanukoviç, Ukrayna'nın yönünü Doğu'ya çevirmiş ve bu doğrultuda politikalar yürütmüştür. Ukrayna'daki var olan Rus nüfuzu, Sovyetler Birliği'nin dağılışından beri var olmuş, Ukrayna'da gerçekleşen 2013 yılındaki olaylar itibariyle geri döndürülemez bir noktaya ulaşmıştır (Cin ve Tekin, 2021: 227). Ukrayna'daki Batı yanlısı gruplar tarafından başlatılan protestoların ilk ayağı, 21 Kasım'da Yanukoviç'in AB Ortaklık Anlaşması'nı imzalamayacağını açıklamasıyla başlamıştır (Guardian, 2013). Yanukoviç'in bu kararının üzerine on binlerce Ukraynalı, Kiev'de Bağımsızlık Meydanı'nda toplanmış ve bu kararı protesto etmiştir (BBC, 2013). Bu şekilde başlayan protestolar, *Euromaidan* ya da *Maidan* olarak anılmış ve ilerleyen süreçte kontrolden çıkarak Ukrayna için birçok sonucu beraberinde getirmiştir.

Yanukoviç'in AB kararı sonrasında, Rusya harekete geçmiş ve Ukrayna'yı ekonomik anlamda rahatlatacak bazı adımlar atmıştır.[1] Ancak bu adımlar, sürmekte olan protestoların şiddetini iyice artırır nitelikte olmuştur. Bunun yanı sıra, Ukrayna Parlamentosu'nun çıkardığı protesto karşıtı yasalar, protestocuları iyice alevlendirmiştir. Bunun üzerine, Ukrayna hükûmet binaları, protestocuların hedefi haline gelmiştir (BBC, 2014). Şubat ayından itibaren, barışçıl olarak başlayan protestolar kanlı bir niteliğe bürünmüştür. Ukrayna Parlamentosu, Rusya'ya kaçtığı iddiasıyla Yanukoviç'i görevden almıştır (BBC, 2014). Yanukoviç'in görevden alınmasının ardından Rusya, Ukrayna'nın bir Amerikan uydusu haline gelmesine müsaade etmeyeceğini duyurmuştur (Treverton vd., 2018: 14).

Yaşanan süreçte önemli kırılmalardan birisi, Yanukoviç'in görevden alınmasını takiben, Ukrayna Parlamentosu'nun Rusçayı yasaklamayı oylaması olmuştur.[2] Bu adım Rusya için yeni bir müdahale zemini oluşturmuştur. 20 Şubat 2014 günü *Maidan* protestolarının bir çatışma halini almasından kısa bir süre sonra Kırım'daki Rus operasyonları da (22-23 Şubat) başlamıştır (Kofman vd., 2017: 6-7). Ukrayna hükûmetinin yaşanan bu süreçte Kırım'ın kontrolü konusunda zayıf ve yetersiz kaldığı açıktır. 16 Mart tarihinde Kırım'da yapılan sözde referandumda ezici bir çoğunluk Rusya'ya katılımı desteklemiştir. Seçmenlerin %83,1'inin oy kullandığı referandumda, halkın %96,77'si Rusya'ya katılım lehinde oy kullanmıştır (The Washington Post, 2014). Kırım Parlamentosu'nun talebi doğrultusunda, 18 Mart 2014'te Rusya, Kırım'ı resmen ilhak etmiştir (BBC, 2014; Dilek, 2015: 245-272).

Siber savaş kavramı, Rus literatüründe, Batı literatürüne göre daha farklı ele alınmaktadır. Rusya siber kavramı yerine, elektronik savaş ve siber operasyonları da kapsayan *bilgi/enformasyon* kavramını kullanmaktadır (Giles, 2011: 46). Rus perspektifine göre siber savaş, daha kapsayıcı bir kavram olan bilgi çatışmasının bir bileşeni olarak görülmektedir (Hakala ve Melnychuk, 2021: 5). Rusya, Kırım'ın ilhakı sürecinde birçok aracı bir arada kullanarak hibrit bir savaş örneği ortaya koymuştur. Bu süreçte yaşanan siber ve bilgi operasyonları da bu savaşın önemli bileşenleri olarak ön plana çıkmıştır. Ukrayna'da gerçekleştirilen operasyonlar elektronik savaş, siber saldırı ve bilgi operasyonlarının karışımıyla desteklenmiştir (McCory, 2020: 35). Ukrayna çatışması esnasında kullanılan siber saldırılar, Gürcistan ve Estonya örneklerinden çıkarılan dersler üzerinden eyleme dökülmüştür. Söz konusu siber saldırılar, Ukrayna'nın meşruiyetini zedelediği gibi NATO açısından ise büyük hayal kırıklığı oluşturmuştur (Medvedev, 2015: 26).

2013 yılından başlayarak Ukrayna'ya yönelik yoğun siber saldırılar gerçekleştirilmiştir. Ukrayna internet sitelerine yönelik DDoS[3] saldırıları olaylar başladığı tarihten itibaren artarak devam etmiştir. Bilgisayar korsanları, kullanıcıların bilgilerini ele geçirip onlara propaganda içerikli mesajlar göndermişlerdir. Örnek verilecek olursa, protestolar sırasında, daha geniş katılımları önleyebilmek için Ukraynalılara tehdit içerikli mesajlar gönderilmiştir (Pakharenko, 2015: 61). Birçok siber güvenlik şirketi, Ukrayna ağlarında kötü amaçlı yazılımlar, siber casusluk

[1] Ayrıntılı bilgi için bkz. Al Jazeera, 2013, https://www.aljazeera.com/news/2013/12/18/russia-and-ukraine-strike-15bn-deal.
[2] Ayrıntılı bilgi için bkz. BBC, 2014, https://www.bbc.com/news/world-middle-east-26248275.
[3] DDoS: DDoS saldırısı, hedef alınan internet ağına çok sayıda istek göndererek saldırı altındaki sistemin işlem yapma kapasitesini aşmayı ve bu şekilde sistemin çalışmasını engellemeyi amaçlayan saldırılardır. Ayrıntılı bilgi için bkz. Kaspersky, https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks.

faaliyetleri ve askeri kuruluşlara ve personele yönelik saldırılar gerçekleştirildiğini bildirmiştir (Pernik, 2018: 61). Olayların yoğunlaştığı Şubat 2014'ten itibaren stratejik öneme sahip resmî kurumların ve ülkede faaliyet gösteren özel şirketlerin bilişim yapıları da, Rus istihbarat servisleri öncülüğü ve yönlendirmesiyle hacker saldırılarına maruz kalmıştır. (Costea, 2020: 51). Siber saldırılardan etkilenen kurumlardan bazıları, Ukraynalı telefon hizmetleri sağlayıcı firması UKRTelecom (Weedon, 2015: 76), parlamento mensupları, Ukrayna devlet siteleri, Ukrayna Ulusal Güvenlik Konseyi ve Ukrayna devlet haber ajansı Ukrinform'dur (Hakala ve Melnychuk, 2021: 24).

Rusya'nın gerçekleştirdiği iddia edilen, Kırım'ın ilhakı sürecinde yaşanan siber saldırılara bazı örnekler şu şekildedir:

- Mobil cihazlar üzerinden, ordu mensuplarına yönelik propaganda mesajları (McCory, 2020: 37);
- Kırım'da faaliyet gösteren Black Sea TV'ye yönelik DDoS saldırıları (Lange-Ionatamišvili, 2014: 14);
- 2014 Mayıs ayında gerçekleşen Ukrayna cumhurbaşkanlığı seçimlerine yönelik siber saldırılar (Hakala ve Melnychuk, 2021: 24);
- Ukraynalı yetkililerden çalınan e-posta ve dokümanların yayınlanması (Pakharenko, 2015: 63);
- Enerji altyapısına yönelik saldırılar (Pernik, 2018: 61);
- Ukrayna iletişim altyapısına yönelik saldırılar (Reuters, 2014).

Yapılan siber saldırılar hakkında belirtilmesi gereken önemli bir husus vardır. Söz konusu saldırıların, siber uzayın yapısı gereği bir kaynağa atfedilmesi oldukça zordur. Rusya yönetimi, söz konusu saldırıları, kendisi tarafından gerçekleştirdiğine yönelik yeterli kanıtın olmayışından da kuvvet bularak suçlamaları reddetmektedir. Ancak olaylar esnasında gerçekleştirilen siber saldırıların, Rusya'nın Kırım'da başarıya ulaşmasında katkıda bulunduğu açık bir durumdur (Medvedev, 2015: 27).

Rusya'nın Kırım'a müdahalesinin ikinci boyutunu bilgi operasyonları oluşturmaktadır. Kırım olayları sırasında Batı toplumuna, Batılı tarzda haber yayınları yapan Rus medyası, olayları Rus perspektifine ve çıkarlarına göre aktararak Kırım'ın ilhakını Rus hedefleri doğrultusunda desteklemiştir. Rus hükûmetinin, kitle iletişim araçları üzerindeki denetimi, Ukrayna'ya yönelik bilgi operasyonlarının etkin bir şekilde gerçekleştirilmesinde önemli bir faktör olmuştur. Rus hükûmetinin görüşlerinin yayılması amacıyla medya üzerinde kurulan denetim, Başkanlık İdaresi (*Presidential Administration*) tarafından gerçekleştirilmektedir (Lange-Ionatamišvili, 2014: 4).

Ukrayna'da Şubat 2014 tarihinde *Maidan* protestolarının kontrolden çıkmasını izleyen süreçte, Rus özel kuvvetleri mensupları Kırım'a yerleşerek kimliksiz bir şekilde operasyonlarını yürütmüşlerdir (Galeotti, 2015: 3). Daha önce de belirtildiği gibi siber saldırılar aracılığıyla ve fiziksel müdahaleler ile Kırım'da medyanın tek temsilcisi Rus medya temsilcileri olmuştur. Kırım'ın ilhakına giden süreçte yaşanan bilgi operasyonlarına dair bazı örnekler aşağıda listelenmiştir:

- "*Maidan protestoları sonucunda yeni kurulan hükûmeti, Washington'dan yönetilen bir oluşumdan ayırmak zor. Protestolar, ABD desteğiyle gerçekleşti*" (Russia Today (RT), 2014).
- "*Kırım'da silah zoruyla referandum efsanesi çökertildi*" (RT, 2014).

- "*Kırım 23 yıl önce işgal edildi*" (TASS, 2014).
- "*Ukrayna'da "darbe" ile gelen hükûmet, insan haklarını ihlal ediyor. Maidan'a katılan siyasi güçler, başta azınlık hakları olmak üzere insan hak ihlalleri çağrısında bulunuyor"* (RT, 2014).
- Aşırı sağcı grupların Yahudi ve Rus düşmanı oldukları vurgulanmıştır.[4] Rus medyası, bu şekilde Yahudi cemaati üzerinden güvensizlik ve kargaşa ortamı oluşturmayı amaçlamıştır (Cin ve Tekin, 2021: 237).
- "*Kırım'da Rusça konuşan halka yönelik provokasyonlar durdurulmalı"* (TASS, 2014).
- Duma Başkan Yardımcısı Sergey Zheleznyak: "*Ukrayna'da Rusça konuşan insanlar 'soykırım' riskiyle karşı karşıya*" (Euractiv, 2014).

Rus medyasının, bilgi kampanyasının ana temaları şu başlıklar altında ifade edilebilir: "Ukrayna hükûmeti ABD uydusu", "*Maidan* protestocuları aşırı milliyetçi, Rus düşmanı ve anti-semitiktir", "Kırım aslında Rus toprağıdır", "Kırım'daki Rus nüfus tehdit altındadır" ve "Rusya, Kırım'daki olaylara müdahil olmamıştır". Sonuç olarak, Rus medyası, Ukrayna'daki kargaşa sırasında yürüttüğü yayın politikasıyla Kırım'da yaşananları Rus argümanları ve çıkarlarına uygun bir şekilde uluslararası topluma aktarmayı başarmıştır (Cin ve Tekin, 2021: 237). Bu süreçte Rus medyası, hem ülke içindeki nüfusun Rusya'nın güvenlik stratejisine destek vermesini; hem de ülke dışındaki Rusofon'un konsolide edilmesini hedeflemiştir.

Kremlin'in talimatıyla yürütüldüğü iddia edilen siber alandaki saldırganlıklar ile Rusya tarafından yayınlanmış olan siber güvenliğe dair resmî belgeler uyuşmamaktadır. Çünkü siber güvenliğe dair Rusya tarafından yayınlanan belgelerde, devletin saldırgan siber faaliyetlerini gerçekleştirebileceğine dair bir stratejiden bahsedilmemiştir. Bu belgelerde saldırgan tutumdan ziyade, savunma ve uluslararası iş birliğini vurgulayan bir dil kullanılmıştır. Meselenin medya boyutunda ise durum biraz daha farklıdır. Hemen hemen her belgede, Rus devletinin medya üzerindeki kontrolünün ve desteğinin arttırılması tavsiye edilmiştir. Medya kontrolü vasıtasıyla Rus halkı ve yabancılara yönelik uluslararası olaylar hakkında Rus argümanlarının doğru bir şekilde anlatılması amaçlanmıştır. Kırım örneği üzerinde bu hedefe ulaşıldığı görülmektedir. Son olarak, yaşanan bu olaylar Gerasimov Doktrini'nin ön gördüğü süreçler içerisinde yaşanmıştır. Bilgi harbi boyutunda yürütülen ilhak sürecinin, Rus askeri uzmanlar Tchekinov ve Bogdanov'un görüşleriyle de uyuştuğu ifade edilebilir. Adı geçen uzmanların yayınladığı makalelerin her ne kadar resmî niteliği olmasa da Rus görüşünü yansıttıkları Kırım örneğinde ortaya çıkmıştır.

Sonuç

Siber güvenlik, 2000'li yıllarla birlikte devletleri ve bununla doğrultulu olarak uluslararası ilişkileri ilgilendiren önemli meselelerden biri haline gelmiştir. Devletlerin en önemli amaçlarından birisi hukuki varlıklarını yani egemenliklerini devam ettirebilmektir. Bu yüzden devletler, tehdit algıladıkları durumlara karşı tedbir alma refleksi gösterirler. Siber alandan kaynaklı tehditler, devletler için siber güvenlik meselesini ortaya çıkarmıştır. Siber alanı fiziksel bir temelde kısıtlamak ya da tanımlamak mümkün olmasa bile siber alandan kaynaklı tehditlerin

[4] Konuyla ilgili bir haber için bkz. Russia Today, 2014, https://www.rt.com/news/ukraine-human-rights-violated-402/.

doğrudan fiziksel dünyayı etkileme potansiyeline sahip olduğu rahatlıkla ifade edilebilir. Bu nedenle siber güvenlik, devletleri ilgilendiren başlıca konulardan birisi haline gelmiştir.

Siber alanın dolayısıyla da siber tehditlerin ya da siber güvenliğin farkında olan devletler, ulusal güvenlik stratejilerini bu doğrultuda yenileme yoluna gitmişlerdir. Güvenliğe yaklaşımlar, sınırlarla ya da sadece fiziksel dünya ile kısıtlanabilir yapılarından çok farklılaşmıştır. Artık bir devleti devlet yapan en önemli unsurlardan olan ulusal sınırların korunması, bir devletin güvenliği için yeterli olmamaktadır. Bu durumun farkında olan devletlerden birisi de Rusya olmuştur. Rusya daha 2000 yılında, siber güvenliğe ilişkin bir belge yayınlayarak bu alandan kaynaklı tehditlerin ve fırsatların farkında olduğunu göstermiştir. Rus ulusal strateji belgelerindeki en önemli vurgulardan birisi de ulusal güvenlik stratejilerine, siber güvenlik tedbirlerinin dâhil edilmesi olmuştur. Rusya'nın yayınladığı resmî belgelerde dikkat çeken noktalardan birisi, belgelerin, savunma refleksini ön plana çıkaran ve yumuşak bir dil ile yazıldığıdır. Anılan belgelerdeki kullanılan bu dil, Rusya'nın asıl amacını gizlemek için bu dili tercih ettiği değerlendirmelerine neden olmuştur. Strateji belgelerinden farklı olarak anılan vakalara bakıldığı zaman, Rusya'nın siber alanı, bir saldırı sistemi içerisinde kullanmaktan çekinmediği görülmektedir. Rusya, yayınladığı belgelerde bilgi güvenliği stratejisinin iki ayağından birisi olan siber alana ilişkin yumuşak ve savunmacı bir dil kullanmış olsa da Kırım örneği üzerinden görüldüğü gibi aslında saldırgan bir tutum benimsemiştir. Siber uzayın sunduğu olanakları, ulusal güvenliğine sağlamaya yönelik girdiği çatışma veya operasyonlarda kullanmaktan geri durmamıştır. Rusya açısından bilgi güvenliğinin ikinci ayağını oluşturan bilgi-psikolojik boyutu daha çok medya üzerinden yürütülen bilgilendirme ve propaganda faaliyetlerine dayanmaktadır. Medya açısından, incelenen belgelerdeki liberal olmayan tutumun, Kırım örneğinde uygulanan strateji ile de tutarlı olduğu görülmektedir.

Sonuç olarak, Rusya attığı adımlarla siber alanda adından söz ettiren ülkelerden birisidir. Siber güvenliğe ilgisinin erken başlaması ve tarihsel olarak barındırdığı teknolojik miras, Rusya için önemli itici güçlerden olmuştur. Kremlin, ulusal güvenlik stratejisi içerisinde değerlendirdiği siber alanı, geleneksel saldırı yöntemleri içerisinde kullanmasıyla birlikte yeni bir savaş tekniğinin, birçok örneğini sunmuştur. Bunun en açık örneği *Maidan* protestoları sırasında gerçekleşen Kırım'ın ilhak edilmesi sürecinde görülmüştür. Bu gerçekler, Rusya'nın siber alanda önemli bir güç olma yolunda ilerlediğini ve diğer devletlerce dikkate alınması gereken bir aktör olduğu gerçeğini gözler önüne sermektedir.

Çıkar Çatışması: Yazar(lar) çıkar çatışması olmadığını beyan eder.
Disclosure Statement: No potential conflict of interest was reported by the author(s).

EXTENDED ABSTRACT

The sovereignty of states, which are among the main actors of international relations, and in connection with this, their national security is an important issue. Approaches to the issue of national security have been a concept that has changed with the globalization process. Many topics that are closely related to national security have been changed and new ones have been added: international organizations, individuals, climate change, technological developments, etc. Although internet-based systems provide many conveniences in all areas of life with digitalization, this convenience has brought many risks. Along with these risks, the issue of cyber security has become an issue that is handled by the states within the national security concepts.

The Russian Federation has been one of the first countries to realize the threats originating from cyberspace. In the early 2000s, Russia published a doctrine on cyber security and outlined its approach to cyberspace. Russia's approach to cyberspace differs from the Western literature. In Russian literature, the word "information", which corresponds to a broader meaning, is used instead of the word "cyber". In the documents published by Russia, it is seen that Russia uses a defensive and soft language regarding cyber security. On the other hand, Russia's attitude towards the media is considered as anti-liberal.

If the documents published by Russia are evaluated considering the events during the annexation process of Crimea, it is seen that Russia has taken a harsh stance despite the defensive language used in the documents. In the documents published by Russia, it is seen that it pays special attention to the control and supervision over the media. This attitude is in line with the information operations carried out by Russia through the media during the annexation of Crimea. As a result, Russia is one of the most important countries in cyberspace. Its early interest in cybersecurity and its historical technological legacy have been important driving forces for Russia. Russia has presented many examples of a new war technique by using cyber-space. The clearest example of this was seen during the annexation of Crimea, which took place during the Maidan protests. These facts reveal the fact that Russia is on the way to become an important power in the cyber space and is an actor that should be taken into account by other states.

Kaynakça

Acar, H. & Pekcandanoğlu, M. (2020). Analysis of Russia's Cyber Security and Cyber Espionage Policies. *Türkiye Rusya Araştırmaları Dergisi, 3*, 167-189.

Acar, H. (2020). Rusya'nın Siber Güvenlik Politikası. İçinde Fulya Köksoy (Ed.). *Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları* (87-107). Nobel Yayıncılık.

Akyazı, U. (2013). "Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler". VI. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ISC Turkey, Ankara, 216-220.

"Brokering power: US role in Ukraine coup hard to overlook", Russia Today, 17 Şubat 2015, https://www.rt.com/news/233439-us-meddling-ukraine-crisis/

Cin, G. ve Tekin, H. H. (2021). Rusya'nın Hibrit Savaş Kapasitesinin Kırım ve Donbas Vakaları Üzerinden Analizi. *Güvenlik Stratejileri Dergisi, 17*(37), 203-246.

Costea, C. A. (2020). *Rusya'nın Ukrayna'daki Hibrid Savaşı*. SETA Yayınları.

"Crimea annexed by Ukraine 23 years ago — Naryshkin", TASS, 11 Haziran 2014, https://tass.com/russia/735705, (Erişim Tarihi: 10.03.2022).

"Crimea's parliament votes to join Russia", The Washington Post, 17 Mart 2014, https://www.washingtonpost.com/world/crimeas-parliament-votes-to-join-russia/2014/03/17/5c3b96ca-adba-11e3-9627-c65021d6d572_story.html, (Erişim Tarihi: 02.03.2022).

"Crimean 'referendum at gunpoint' is a myth – intl observers", Russia Today, 16 Mart 2014, https://www.rt.com/news/international-observers-crimea-referendum-190/, (Erişim Tarihi: 21.03.2022).

Darıcılı, A. B. (2017). *Siber Uzay ve Siber Güvenlik Nedir? ABD ve Rusya'nın Siber Güvenlik Stratejilerinin Karşılaştırılmalı Analizi.* Dora Yayıncılık.

Darıcılı, A. Burak ve Özdal, Barış (2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi. *Bilig*, Avrasya'nın Siyasal İktisadı Özel Sayısı, 121-146.

Dilek, M. S. (2015). Rusya Federasyonu'nun Kırım Hamlesine Analitik Bakış. *Turkish Studies, International Periodical for the Languages, Literature and History of Turkish or Turkic,* 10/14, 245-272.

"Duma Vice-Chair: Russian-speaking people in Ukraine risk 'genocide'", Euractiv, 13 Mart 2014, https://www.euractiv.com/section/europe-s-east/interview/duma-vice-chair-russian-speaking-people-in-ukraine-risk-genocide/, (Erişim Tarihi: 21.03.2022).

Erol, M. S. ve Oğuz, Ş. (2015). Hibrit Savaş Çalışmaları ve Kırım'daki Rusya Örneği. *Gazi Akademik Bakış, 9*(17), 261-277.

ETH Zurich, (2009). Russia: National Security Strategy to 2020. https://css.ethz.ch/en/services/digital-library/publications/publication.html/154915.

Galeotti, M. (2014). "The 'Gerasimov Doctrine' and Russian Non-Linear War". In Moscow's Shadows. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Galeotti, M. (2015). "Hybrid war and "little green men": How it works, and how it doesn't". İçinde Agnieszka Pikulicka-Wilczewska ve Richard Sakwa (Eds.), *Ukraine and Russia: People, politics, propaganda and perspectives* (156-165). Bristol, UK: E-International Relations.

Giles, K. (2011). ""Information Troops"- A Russian Cyber Command?". 3rd International Conference on Cyber Conflict. IEEE. 45–60. https://ieeexplore.ieee.org/abstract/document/5954699.

Giles, K. (2012). "Russia's Public Stance on Cyberspace Issues". 4th International Conference on Cyber Conflict. Tallinn, The NATO Cooperative Cyber Defense Centre of Excellence. 63-75. https://ccdcoe.org/uploads/2015/04/CyCon_2012_book_web_sisu.indd_.pdf.

Güntay, V. (2017). Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği. *Güvenlik Bilimleri Dergisi, 6*(2), 81-108.

Hakala J., Melnychuk J., (2021). Russia's Strategy in Cyberspace. Riga: NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210.

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars [Elektronik Versiyon]. Arlington: Potomac Institute for Policy Studies.

"Human rights violated by Ukraine's coup-appointed govt – European NGO", Russia Today, 12 Mart 2014, https://www.rt.com/news/ukraine-human-rights-violated-402/, (21.03.2022).

Karabulut, B. (2017). Uluslararası İlişkilerde Savaş Olgusunun Yaşadığı Dönüşüm: Hibrit Savaş ve Rusya Örneği. *KARAM Dergisi, 55*(14), 115-130.

Kofman, M. & Rojansky, M. (2015). "A Closer look at Russia's "Hybrid War", Wilson Center Kennan Institute, Report, No: 7. https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war.

Kofman, M., Migacheva, K., Nichiporuk B., Radin, A., Tkacheva, O. & Oberholtzer, J. (2017). Lessons from Russia's Operations in Crimea and Eastern Ukraine [Elektronik Sürüm]. Santa Monica, CA: RAND Corporation.

Lange-Ionatamišvili, E. (2014). Analysis of Russia's information campaign against Ukraine. Riga: NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf.

"Lavrov: ultranationalists provocations against Russian-speakers in Crimea should be curbed", TASS, 18 Mart 2014, https://tass.com/russia/724259, (Erişim Tarihi: 15.03.2022).

McCrory, D. (2020). Russian Electronic Warfare, Cyber and Information Operations in Ukraine. *The RUSI Journal, 165*(7), 34-44.

Medvedev, S. A. (2015). Offense-Defense Theory Analysis Of Russian Cyber Capability. Master Thesis for Naval Post-Graduate School. Monterey, California.

Pakharenko, G. (2015). "Cyber Operations at Maidan: A First-Hand Account". İçinde Kenneth Geers (Ed), *Cyber War in Perspective: Russian Aggression against Ukraine* (59-67). Tallinn: NATO CCD COE Publications.

Pernik, P. (2018). The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine. İçinde N. Popescu ve S. Secrieru (Eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies* (53–64). European Union Institute for Security Studies (EUISS).

Tchekinov, S.G. ve Bogdanov, S.A. (2013). "The Nature and Content of a New-Generation War". Military Thought: A RussiancJournal of Military Theory and Strategy, Sayı 4, s.12-23.

The Ministry of Foreign Affairs of the Russian Federation (2000). National Seurity Concept of The Russian Federation. https://www.mid.ru/en/foreign_policy/fundamental_documents/1737121/.

The NATO Cooperative Cyber Defence Centre of Excellence (2011). Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space. https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf.

The International Telecommunication Union (ITU). "Definition of Cybersecurity", https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

The International Telecummunication Union (ITU). (2008). Information Security Doctrine of The Russian Federation. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf.

Thomas, T. (2014). Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?. *The Journal of Slavic Military Studies, 27*(1), 101-130.

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., ve McCue, M. (2018). Addressing Hybrid Threats [Elektronik Sürüm]. Bromma: Arkitektkopia AB.

"Ukrainian MPs vote to oust President Yanukovych", BBC, 22 Şubat 2014, https://www.bbc.com/news/world-europe-26304842

"Ukraine protests after Yanukovych EU deal rejection", BBC, 30 Kasım 2013, https://www.bbc.com/news/world-europe-25162563

"Ukraine: Putin signs Crimea annexation", BBC, 21 Mart 2014, https://www.bbc.com/news/world-europe-26686949

"Ukraine says communications hit, MPs phones blocked", 4 Mart 2014, https://www.reuters.com/article/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304

"Ukraine suspends talks on EU trade pact as Putin wins tug of war", The Guardian, 21 Kasım 2013, https://www.theguardian.com/world/2013/nov/21/ukraine-suspends-preparations-eu-trade-pact

"Ukraine unrest: Protesters storm regional offices", BBC, 24 Ocak 2014, https://www.bbc.com/news/world-europe-25876807

Weedon, J. (2015). "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine". İçinde Kenneth Geers (Ed), *Cyber War in Perspective: Russian Aggression against Ukraine* (67-79). Tallinn: NATO CCD COE Publications.