U.U. International Journal of Social Inquiry / U.Ü. Sosyal Bilimler Enstitüsü Dergisi Cilt / Volume 7 Sayı / Issue 2 2014 ss./pp. 1-16

RUSYA FEDERASYONU KAYNAKLI OLDUĞU İDDİA EDİLEN SİBER SALDIRILARIN ANALİZİ

A. Burak DARICILI*

(Makale Geliş Tarihi-Received: 27.07.2016 /
Makale Kabul Tarihi-Accepted: 07.11.2016)

ÖZ

Rusya Federasyonu (RF), siber uzay olarak adlandırılan alanda etkinliğini her geçen gün artırmaktadır. RF'nin siber uzaydaki etkinliğini artırmasının temel sebebi ise uluslararası sistemdeki en önemli siber güçlerden biri konumuna ulaşarak, sahip olduğu bu gücü dış politika sorunlarının çözülmesi noktasında bir baskı ve yaptırım aracı olarak kullanmak istemesidir.

Bu hedef kapsamında RF, mevcut siber saldırı kapasitesine ulaşmak amacıyla 2000'li yıllarda ciddi gayret göstermiştir. İzlediği stratejinin sonucunda kısa bir süre içinde sahip olduğu siber saldırı gücünü arttıran RF, günümüzde siber uzayı domine eden en önemli aktörlerden biri konumuna ulaşmıştır.

Bu bağlamda makalede RF'nin 2007 yılında Estonya'ya, 2008 yılında Gürcistan'a ve Litvanya'ya, 2009 yılında Kırgızistan'a ve 2014 yıllında Ukrayna'ya yönelik olarak gerçekleştirdiği iddia edilen siber saldırılar incelenerek, RF'nin dış politika sorunlarının çözümü kapsamında sahip

* *Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler ABD Doktora Öğrencisi, daricili@yahoo.com*

olduğu siber saldırı kapasitesini ne şekilde kullanmakta olduğu analiz edilecektir.

Anahtar Kelimeler: RF, Siber Uzay, Siber Güç, Siber Saldırı, Dış Politika.

ANALYSIS OF ALLEGED CYBER ATTACKS FROM RUSSIAN FEDERATION

ABSTRACT

Russian Federation (RF) increases its activity in the field, called cyber space, day by day. The main reason why RF improves its efficiency in cyberspace is that it demands to be one of the most important cyber powers in the international system and needs to have power to use it as a means of pressure and sanction at the point of solving its foreign policy problems. Within this target, RF has made considerable efforts in the 2000s in order to reach the existing cyber attack capacity. As a result of the strategy it pursues, RF, which has increased its cyber attack power in a short period of time, is now one of the most important actors that dominate cyber space.

In this context, our article examines how RF uses its cyber attack capacity at the point of solving its foreign policy problems by analyzing on the alleged RF attacks on Estonia in 2007, Georgia and Lithuania in 2008, Kyrgyzstan in 2009 and Ukraine in 2014.

Keywords: RF, Cyber Space, Cyber Force, Cyber Attack, Foreign Policy.

GİRİŞ

Siber uzay kavramının uluslararası kabul görmüş bir tanımı bulunmamaktadır. Çoğunlukla interneti ifade etmek için kullanılan bir kavram olarak analizlerde sıklıkla ele alınmaktadır. Gerçekte bu kavram tabiri bir bilim kurgu romanı ile insanların karşısına çıkmıştır. Dünyanın en çok okunan bilim kurgu romanlarından biri olan Neuromancer'in yazarı William Gibson gerçeklikle hiçbir ilgisi olmayan söz konusu kavramı, bir söyleşisinde ilk defa kullanmıştır. Gibson'a göre siber uzay, "*milyarlarca meşru kullanıcı tarafından her gün tecrübe edilen uzlaşılmış bir halüsinasyon ve tasavvur edilemez karmaşa*" şeklindedir (Gibson, 1984: 69).

Belirtildiği üzere siber uzayın üzerinde uzlaşılmış tek bir tanımı bulunmamak ile birlikte bu kavram; "*internet, iletişim ağları, dış dünyaya kapalı askeri ağlar, enerji hatları ağları, cep telefonları yazılım altyapılı telsizler, elektronik komuta sistemleri, cep teflonları, uydu sistemleri, insansız hava araçları sistemleri gibi birçok yazılım ve donanım elemanların toplamı*" şeklinde tanımlanabilir (Akyazı, 2013).

Diğer yandan bu etkileyici tanımın mahiyeti ne olursa olsun, siber uzay günümüzde günlük hayattan, askeri ve ekonomik konulara kadar, ciddi ve derin anlamlara sahip bir içerik olarak karşımıza çıkmaktadır. Siber uzay, kimilerine göre birbirleri ile haberleşen bilgisayar teknolojileri için kavramsal bir çerçeve, kimilerine göre askeri doktrinde yeni bir cephe, kimilerine göre bütün ekonomik eko-sistemin büyüyüp geliştiği bilgiye dayalı bir alt katman, kimilerine göre ise dünya politik arenasında gittikçe önem kazanan yeni bir içerik anlamını taşımaktadır (Bkz. Demircioğlu, 2014: 41-42).

Siber uzay şeklinde tanımlanan alanda meydan gelen gelişmeler ile birlikte güvenlik çalışmalarında siber saldırı başlığı altında yeni analizlerin daha sık gündeme geldiği de görülmektedir. Siber saldırı kavramının da çeşitli kaynaklar tarafından yapılan farklı tanımları bulunmaktadır. Belirtilen tanımlardan birinde siber saldırı; "*hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar*" şeklinde tanımlanmıştır (Alkan, 2012).

Soğuk Savaş sonrası dönemde siber uzay alanındaki gelişmelere bağlı olarak ortaya çıkan siber saldırı imkânları ise uluslararası sistemde

kimi devletler tarafından askeri kapasitelerini artırma noktasında yeni bir fırsat olarak değerlendirilmiş ve bu devletler siber güçlerini artırmak amacıyla stratejiler geliştirmeye başlamışlardır. Siber güç şeklinde belirtilen içerik ise Joseph S. Nye tarafından: "*insan kaynağı ve yeteneği, yazılım ve donanım teknolojileri, altyapılar ve ağ teknolojileri ile ilgili tüm kaynaklar vasıtasıyla yaratılan bir imkân"* şeklinde tanımlanmıştır (Bkz. Nye, 2011: 3-7) .

RF'nin ağ teknolojilerindeki ilerlemelere bağlı olarak gelişen siber uzay alanı ve bu gelişmelerin ortaya çıkardığı güvenlik temelli ilk tecrübeler ise 1979–1989 arasında yaşanan Afganistan Savaşı'na dayanmaktadır. 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 (Heickerö, 2010: 15). Benzer şekilde 1994–1996 yıllarındaki Çeçen Savaşı'nda, internet haberleşmesi ve bu haberleşmenin ortaya koyduğu imkânlar, savaş esnasındaki olayların RF aleyhine yansıtılması kapsamında oldukça başarılı olmuştur (Bıçakçı, 2013: 50). Diğer bir deyişle RF, uluslararası kamuoyu nezdinde Çeçen Savaşı'nda insanlık dışı yöntemlere başvuran, savaş suçu işleyen bir devlet olarak kabul edilmiştir (Heickerö, 2010: 15). Söz konusu iki olayın olumsuz etkisiyle Rus güvenlik ve askeri bürokrasisinin, askeri ağ teknolojileri ve enformasyon savaşı alanındaki planlamaları ve hazırlıkları hızla gelişmeye başlamıştır. Bu planlamaların ilk sonucu olarak 1999 yılında Kuzey Atlantik Paktı (North Atlantic Treaty Organization / NATO)'nın eski Yugoslavya'daki Sırp güçlerini bombalamaya başlamasının ardından, Sırp ve Rus hackerler tarafından Pakt üyesi devletlerin askeri haberleşme sistemlerine, ABD Savunma Bakanlığı'nın alt yapılarına siber saldırılar gerçekleştirilebilmiştir (Bıçakçı, 2013: 50).

Bu dönemden itibaren RF, siber saldırı kapasitesini artırmak amacıyla 2000'li yıllarda ciddi gayret göstermiştir. İzlediği stratejinin sonucunda uluslararası sistemdeki en önemli siber güçlerden biri konumuna ulaşan RF, sahip olduğu bu gücü dış politika sorunlarının çözülmesi noktasında bir baskı ve yaptırım aracı olarak kullanmak istemiştir.

Bu itibarla 2007'de Estonya'ya, 2008'de Gürcistan'a ve Litvanya'ya, 2009'da Kırgızistan'a ve son olarak 2014'de Ukrayna yönelik olarak yapıldığı iddia edilen siber saldırılar, RF'nin sahip olduğu siber saldırı

kapasitesini dış politika sorunlarının çözümü kapsamında ne şekilde kullanmakta olduğu bağlamında analiz edilecektir. Zira söz konusu bu saldırı iddialarının analizi, RF'nin siber uzayın ortaya koyduğu yeni imkanları dış politika sorunlarının çözümü kapsamında ne ölçüde kullanmakta olduğunu göstermesi bakımından bizce önem arz etmektedir.

Estonya'ya Yönelik Siber Saldırılar

Estonya'ya yönelik olarak 2007 yılında RF kaynaklı olarak gerçekleştirildiği iddia edilen siber saldırılar, siber güvenlik literatürünün yanı sıra uluslararası ilişkiler disiplininde de birçok yönüyle detaylı olarak analiz edilmiştir. Söz konusu siber saldırı Estonya Parlamentosu'nun Tallinn Meydanı'ndaki Bronz Asker anıtını kaldırma kararı almasıyla başlamış olmakla birlikte, saldırının arka planında Estonya RF ilişkilerindeki yıllardan beri süregelen gerginliğin yanı sıra RF'nin başta ABD olmak üzere, diğer NATO üyeleriyle yaşadığı küresel mücadelenin de etkisi bulunmaktadır (Bıçakçı, 2014: 121).

Genel ve soyut olarak RF ile Estonya arasındaki ilişkiler tarihsel olarak ele alındığında, iki ülke arasında Estonya'nın demografik ve sosyo-kültürel yapısı kapsamında ortaya çıkan bir gerginliğin mevcudiyeti görülecektir. II. Dünya Savaşı sonrasında, Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) tarafından maksatlı bir politik adım olarak Estonya'ya önemli oranda Rus kökenli nüfus yerleştirilmiştir. İlerleyen süreçte ise demografik denge Rus azınlık lehine değişmeye başlamıştır. Doğu Blok'unun yıkılması sonrasında ise diğer Baltık ülkelerinin aksine Estonya, ülkesinde % 40 oranında bulunan Rus azınlığa vatandaşlık hakkı verme noktasında isteksiz davranmış ve bu durum RF ile Estonya ilişkilerinde süregelen bir gerginliğe neden olmuştur (Yener, 2014).

Diğer yandan teknolojik mirasının ve eğitim seviyesi yüksek nüfusunun yanı sıra 2000'li yıllarda yapılan yatırımlarla birlikte Estonya; iletişim, telekomünikasyon, yazılım ve ağ teknolojileri alanlarında Avrupa'nın en gelişmiş "*e-devleti*" olarak kabul edilmiştir. Bu itibarla elektronik oy kullanma imkânını vatandaşlarına ilk defa sunan Estonya, halkının % 60'a yakının günlük ihtiyaçlarının önemli bir kısmını internet üzerinden karşıladığı, ülkedeki bankacılık

işlemlerinin yaklaşık % 96'sının internet üzerinden gerçekleştirildiği bir ülke konumuna ulaşmıştır (Ottis, 2008).

26 Nisan 2007 tarihinde yani Tallinn Meydanı'ndaki Bronz Asker heykelinin kaldırılması kararının alınmasından kısa bir süre önce; Estonya'nın kritik altyapılarına yönelik olarak geniş çaplı bir servis dışı bırakma (Distributed Denial of Service / DDoS) saldırısı başlatılmıştır (Bıçakçı, 2014: 122). Bu siber saldırılar ile Estonya'nın siyasi partilerinin, devlet kurumlarının, parlamentosunun web sayfalarına, akabinde; medya kuruluşlarının, bankacılık ve finans sistemine ataklar gerçekleştirilerek, ülkenin internet altyapısı çökertilmek istenmiştir (Tikk, 2010). Saldırılar, her ne kadar son derece organize ve yoğun bir şekilde gerçekleşse de Estonya hükümetinin ulusal internet ağını yurtdışından erişime kapatma kararı alması ile birlikte, saldırıların yoğunluğunun makul bir seviyede tutulması başarılmıştır. 19 Mayıs 2007 tarihine gelindiğinde ise saldırılar sona ermiştir (Ottis, 2008).

Siber uzayın anonim yapısından kaynaklanan isnat-ispat ilişkisi kurulması noktasındaki zorluk dikkate alınarak, bu saldırıların RF kaynaklı olduğu hiçbir zaman kesin olarak ispatlanamayacak olsa bile Estonya'ya yönelik siber saldırıların arka planında dönemin Rus hükümetinin olduğu aslında oldukça nettir. Estonya söz konusu siber saldırıları gerçekleştiren bazı IP'lerin Rusya kaynaklı olduğunu; saldırganların çoğunlukla Rusça dilini kullanarak blog ve forum sayfalarında organize olduklarını; büyük ölçüde bilgisayar korsanlığı tecrübesi olan kişilerden oluştuklarını iddia ederek, saldırı ile ilgili olarak RF'yi doğrudan suçlamıştır (Bkz., Yener, 2014).

Estonya saldırısı, iki komşu ülke arasında gerçekleşen bir yerel hadise olmanın ötesinde, siber saldırılar ve siber güvenlik kavramlarının uluslararası ilişkiler disiplini açısından da analiz edilmesine neden olması bakımından oldukça önemlidir. Ayrıca söz konusu siber saldırının bertaraf edilmesi noktasında başta Amerika Birleşik Devletleri (ABD) olmak üzere, NATO'nun oynadığı rol, ABD ile NATO ve RF ilişkileri açısından da siber uzayın yeni bir mücadele alanı olarak ele alınmasına yol açmıştır (Roth, 2009). Bu kapsamda, saldırıların ilk başladığı andan itibaren Estonyalı yetkililer NATO uzmanlarından büyük destek almış, Tallinn'e gelen NATO uzmanları, ülkenin saldırılara karşı geliştirdiği savunma mekanizmalarında önemli rol oynamışlardır. Tüm bu gelişmeler ile birlikte, Estonya aynı

zamanda siber güvenlik açısında sembolik bir önem kazanmıştır. Zira 2008 yılında Tallinn'de NATO tarafından bir siber güvenlik mükemmeliyet merkezinin kurulması kararlaştırılmıştır. Daha sonra bu merkez, 2008 Ağustos ayında Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defense Center of Excellence / CCD-COE) adıyla faaliyet göstermeye başlamıştır (Bkz., Bıçakçı, 2014: 123-125).

CCD-COE, 2008 yılı sonrasında yaptığı çalışmalar ile birlikte, NATO'nun siber güvenlik stratejisinin belirlemesinde, NATO üyesi ülkeler arasında siber güvenlik alanında işbirliği ve koordinasyonun sağlanmasında, siber güvenlik konusunda strateji belgeleri, konferanslar ve akademik çalışmalar yapılmasında ve başta ABD olmak üzere pek çok üye ülkenin siber güvenlik stratejilerinin planlanmasında önemli rol oynamıştır (Bkz., Yener, 2014).

Gürcistan'a Yönelik Siber Saldırı

RF tarafından 2008 yılında Gürcistan'a yönelik olarak planlandığı iddia edilen siber saldırılar, Rus Silahlı Kuvvetleri'nin konvansiyonel saldırısını destekleyecek şekilde planlanması bakımında önemlidir. Diğer bir deyişle vurgularsak söz konusu siber saldırılar, Gürcistan ile RF arasındaki söz konusu sıcak çatışmayı dünyadaki ilk hibrit savaş örneği haline getirmesi bakımından da özeldir (Goble, 2009).

Genel ve soyut olarak tarihsel arka plana bakarsak bilindiği üzere Abhazya ve Güney Osetya, SSCB'nin dağılması sonrasında "*de facto*" bağımsız bölgeler olarak varlıklarını sürdürmüşlerdir. 2008 yaz ayları boyunca süregelen bir dizi milliyetçi provokasyon neticesinde, 7 Ağustos 2008 tarihinde Gürcistan Askeri Kuvvetleri'nin ülkenin toprak bütünlüğünü tesis etmek amacıyla Güney Osetya'ya yönelik operasyon başlatmasına cevaben, Rus güçleri de 8 Ağustos 2008 tarihinde Osetya'ya girmiş ve sonrasında da Gürcistan'ı işgal operasyonunu faaliyete geçirmiştir. Gürcistan'ın RF ile yaşadığı gerginliğin arka planında, bu ülkenin NATO'ya tam üyelik hedefi ve Batı Blok'u ile yakınlaşması bulunduğu pek çok kaynakta ileri sürülmektedir. Gürcistan'a yönelik siber saldırılar ise 7 Ağustos 2008 gecesinden itibaren Estonya saldırısına benzer şekilde ülkenin kritik altyapılarını hedef alan "DDoS" saldırıları şeklinde başlamıştır. Bu saldırılarda kullanılan siteler incelendiğinde, sitelerin ABD'den çalınan kredi kartlarıyla RF ve Türkiye'de açıldığı belirlenmiş, ayrıca

saldırı için gönderilen SPAM e-postaların hazırlandığı da tespit edilmiştir (Bıçakçı, 2012: 218).

Gürcistan'a yönelik siber saldırılar da Estonya saldırısına benzer şekilde, ülkenin hükümet, medya ve finans sektörlerini felç etmeyi amaçlamıştır. Ancak Gürcü nüfusunun sadece % 10'unun o dönemde internet erişimine sahip olduğu yani Estonya'nın tersine Gürcistan'ın ağlanma oranı ve e-devlet kapasitesi sınırlı olduğu için bu saldırılar Estonya örneğinin aksine kısmen etkili olmuştur (Tikk, 2010). Ayrıca saldırılar esnasında Gürcistan'nın NATO üyeliği henüz gerçekleşmediği için de İttifakın güvenlik şemsiyesinden doğrudan yararlanılamamış fakat NATO uzmanlarından saldırılara karşı koyma noktasında doğrudan destek alınmıştır (Bıçakçı, 2013: 38). Bu kapsamda, Gürcistan'ın siber kaynaklarını üçüncü ülkelere taşımasıyla, bahse konu siber saldırılar bir hafta içinde sona erdirilmiştir. Lakin siber saldırıların psikolojik savaş boyutunda RF, Gürcistan tezleri karşısında uluslararası kamuoyunda yeterli desteği bulamamıştır (Goble, 2008).

Gürcistan'a yönelik olarak düzenlenen siber saldırılardan çıkartılabilecek en önemli sonuç, literatürde genel kabul gördüğü üzere bu saldırıların gerçek bir hibrit savaş niteliği taşıyan ilk sıcak çatışma olduğudur. RF, silahlı kuvvetlerinin operasyonları öncesinde Gürcistan'ı siber saldırılar ile yıpratarak adeta işgale hazırlamak istemiştir. İlerleyen yıllar içerisinde de RF, Estonya ve Gürcistan saldırılarından da edindiği deneyimler ile birlikte, 9 Kasım 2012 tarihinde RF Genelkurmay Başkanlığı görevine atanan Valery Gerasimov tarafından hazırlanan yeni bir savaş stratejisini ortaya koymuştur. Hibrit savaş konsepti veya Gerasimov Doktrini şeklinde isimlendirilen bu strateji ise RF tarafından ilk olarak 2014 yılında Ukrayna'ya yönelik olarak başlatılan askeri müdahale esnasında tüm yönleriyle uygulanmıştır.

Ukrayna Müdahalesi öncesinde de RF'nin siber saldırı yöntemleriyle komşularını baskı altına alarak, dış politika sorunları çözme stratejisi izlediği ileri sürülebilir. Bu bağlamda 2008 yılında Litvanya'ya, 2009 yılında ise Kırgızistan'a yönelik gerçekleştirilen siber saldırılar çalışmanın bundan sonraki aşamasında analiz edilecektir.

Litvanya'ya Yönelik Siber Saldırı

Litvanya, 2008 Haziran ayında üç gün süreyle RF kaynaklı olduğu iddia edilen siber saldırılara maruz kalmıştır. Söz konusu siber saldırılar, Estonya ve Gürcistan örneklerindeki gibi Litvanya'nın kritik altyapılarının "DDoS" saldırıları ile çökertilmesi ve ülkede faaliyet gösteren popüler web sayfalarının "*orak-çekiç*" amblemleriyle hacklenmesi şeklinde gerçekleşmiştir (Ashmore, 2014).

Bu saldırıların arka planında da RF ile Litvanya arasında yaşanan politik gerginlik bulunduğu iddia edilebilir. Zira saldırılar RF'nin SSCB döneminde çalışma kamplarında ölen Litvanyalı kurbanların yakınlarına tazminat ödemeyi reddetmesi, akabinde de RF'nin Litvanya'ya enerji akışını kısıtlaması, buna cevap olarak da Litvanya hükümetinin eski Sovyet sembollerini yasaklayan bir kanunu meclise sunması ve RF-Avrupa Birliği (AB) ortaklık sürecini bloke etmesi sonrasında başlamıştır (Mclaughlin, 2014).

Söz konusu siber saldırıları planlayan kaynakların, Rus İstihbarat Servisleri (RİS) ve RİS ile irtibatlı kriminal potansiyele sahip Rus suç örgütleri olduğu iddia edilmiştir. Litvanya saldırısının da özellikle Estonya saldırısında olduğu gibi Baltık hükümetlerinin Batı Blok'unun da desteğiyle RF'nin ülkelerine yönelik müdahale girişimlerine direnmesinin bir sonucu olarak meydana geldiği ileri sürülebilir. Çünkü bu saldırıda da RF, 2000'li yılların ikinci yarısı itibariyle komşularıyla yaşadığı sorunların çözümü noktasında siber kapasitesi kaynaklı gücünü kullanmaktan çekinmediğini bir kez daha uluslararası kamuoyuna göstermiştir (William, 2014).

Kırgızistan'a Yönelik Siber Saldırı

2000'li yılların ikinci yarısında yaşanan siyasi gerilim neticesinde RF kaynaklı siber saldırı ile karşı karşıya kaldığı iddia edilen bir başka devlet ise Kırgızistan'dır. Kırgızistan'ın iki temel internet servis sağlayıcısı 8 Ocak 2009 tarihinde "DDoS" saldırıları ile karşı karşıya kalmış ve ülkenin tüm web siteleri ve e-posta haberleşmesi kesilmiştir (Rhoads, 2009).

RF'nin bu siber saldırıyı gerçekleştirmesinin arkasında yatan nedenin, Rus hükümetinin Kırgızistan'ı Manas'ta bulunan ABD askeri üssünü

kapatması noktasında baskı altına almak istemesi olduğu ileri sürülmüştür (Rhoads, 2009). Bilindiği üzere Manas askeri üssü ABD'nin Orta Asya'daki etkinliği için önemli bir merkez olmasının yanı sıra Afganistan operasyonlarının idamesi için de hayati öneme sahip bir askeri tesistir. Görüldüğü üzere RF kendi politik girişimlerine muhalefet eden komşu devletlerin hükümetlerini, bu ülkelerin kritik altyapılarını felç etmeyi amaçlayan siber saldırılar planlamak suretiyle baskı altına almaktan çekinmemektedir. Diğer yandan, Litvanya ve Kırgızistan'a yönelik siber saldırıların aşağıda belirtilen üç ortak özelliği vardır (William, 2014):

1. Tüm saldırılar, "DDoS" atakları şeklinde planlanmıştır ve RİS veya RİS ile bağlantılı Rus suç örgütleri kaynaklıdır.

2. Saldırılar hedef ülkelerin kritik altyapılarını çökertmeyi amaçlamıştır ve siber uzayın anonim yapısının avantajlarından da istifade edilmek suretiyle RF'yi doğrudan suçlayacak herhangi kanıtı geride bırakmayacak şekilde planlanmıştır.

3. Saldırılar, Rus hükümetinin dış politika önceliklerini benimsemeyen, bunlara muhalefet eden ve RF'ye karşı ABD başta Batılı ülkelerin desteği ile dengeleme politikası gütmeyi amaçlayan hükümetlerle yaşanan gerginliklerin hemen sonrasında, söz konusu hükümetleri baskı altına almak ve kendi kamuoyu nezdinde zorlamak amacıyla gerçekleşmiştir.

Ukrayna'ya Yönelik Siber Saldırı

Ukrayna Devlet Başkanı Viktor Yanukovich'in 2014 Şubat ayında görevden uzaklaştırılması, RF ile Ukrayna arasındaki hibrit savaş özelliği de içeren sıcak çatışma sürecinin başlangıcı olarak kabul edilebilir (Medvedev, 2014).

Daha öncede belirttiğimiz üzere Rus hibrit savaş konsepti, Valery Gerasimov tarafından detayları şekillendirilen ancak ilk örneği RF'nin Gürcistan'a yönelik askeri operasyonu esnasında görülen gayri-resmi savaş doktrinidir. Bu stratejide temel olarak, siber saldırı teknikleri kullanılarak, hasım devletin askeri gücünün sıcak çatışma öncesinde minimize edilmesi, aynı zamanda yoğun bir şekilde küresel ve yerel ölçekte enformasyon savaşı teknikleri ile RF lehine bir propaganda

sürecinin işletilmesi, tüm bunlar ile birlikte hasım ülkedeki dost ve akraba topluluklar ile koordineli bir şekilde planlanan özel kuvvet operasyonlarıyla konvansiyonel bir çatışma süreci sonunda amaca ulaşılması hedeflenmektedir (Medvedev, 2014).

RF'nin Ukrayna müdahalesi ilk etapta 23 Şubat-01 Mart 2014 tarihleri arasında Kola Yarımadası ile Ukrayna sınırı arasında Rus Kuzey Komutanlığı'nın 150.000 askerinin katıldığı bir "şaşırtma" tatbikatı ile başlayan süreçtir. Tatbikat, düşük tempolu bir güç gösterisi şeklinde icra edilmiştir. Bu aşamada ayrıca RF Parlamentosu 01 Mart 2014 tarihinde Kırım'a yönelik askerî güç kullanımına izin veren bir yasayı da onaylamıştır (Gürcan, 2014).

Daha sonra, Ukrayna İç Güvenlik Birimi SBU'nun Başkanı Valenty Nalyvaichenko tarafından 2014 Şubat ayı sonundan itibaren, Ukrayna mobil telefon iletişim ve internet altyapılarının saldırıya uğradığı ve büyük oranda çöktüğü, özellikle Ukraynalı bürokratlarla milletvekillerine ait akıllı cep telefonlarının tamamının hacklendiği ifade edilmiştir. Ayrıca, Rus yanlısı bir hacker grubu olan CyberBerkut tarafından, Ukrayna Silahlı Kuvvetleri'ne, Ukrayna resmi sitelerine, Ukrayna ile ilgili faaliyet gösteren NATO'nun internet erişimlerine, Ukrayna medya kuruluşlarına yönelik olarak "DDoS" saldırıları da düzenlenmiştir (Lee, 2014). Bu siber saldırıların, Estonya ve Gürcistan'a yönelik siber saldırılara nazaran çok daha etkili ve sofistike yöntemlerle planladığı da görülmüştür. Saldırılarda kullanılan "Snake/Uroboros" yazılımı, özellikle Ukrayna'nın resmi kurumlarına yönelik siber ataklarda son derece etkili olmuştur (Weedon vd., 2014).

Ukrayna'ya yönelik siber saldırıların etkili bir şekilde gelişmesinin bir diğer nedeni ise Ukrayna'nın internet altyapısının özellikleriyle ilgilidir. Genel hatları ile belirtirsek; bazı Ukrayna hükümetlerinin kısıtlayıcı çabalarına rağmen, Ukrayna'nın liberal internet kullanımı politikası bulunmaktadır. Ayrıca Ukrayna'nın küresel internet sistemi ile bağlantısı hem karasal bir yapıyla hem de uydu üzerinden sağlanmaktadır. Bu nedenle de hem internet kullanım politikaları göreli olarak serbestlik ilkesi ile şekillenen hem de küresel internet sistemi ile çeşitli vasıtalarla erişim halinde olan Ukrayna'nın, RF kaynaklı siber saldırlar esnasında ülkesinin internet erişimini dış dünyaya kapatmaya yönelik girişimleri yetersiz kalmıştır. Bu

kapsamda da söz konusu siber saldırılar etkili bir şekilde gelişmiş ve yaygınlaşmıştır (Kelly, 2014).

Bu siber saldırılar ile eş zamanlı olarak, RİS'nin provokasyonları ile kışkırtılan Rus yanlısı sivil protestocular Sivastopol'da şiddet içermeyen sokak eylemleriyle RF'ye bağlanma taleplerini beyan eden mitingler düzenlemeye başlamışlardır. Öte yandan, Kırım'daki Rus yanlısı Russkoye Yedinstvo Partisi, Kırım Ruslarının güvenliğini sağlamak maksadı iddiasıyla bir hafta gibi çok kısa sürede 10 bin kişilik silahlı bir güç oluşturduğunu ilan etmiştir. Bu grupların bu kadar kısa sürede silahlanarak organize edilmeleri dikkate alındığında, söz konusu grupların Rus özel kuvvetleri ve RİS ile doğrudan irtibatlı oldukları da rahatlıkla iddia edilebilecektir.

Belirtildiği üzere, söz konusu siber saldırılar ile direnme gücü törpülenen Ukrayna'ya yönelik sıcak çatışma süreci başlamadan önce, Kırım'ın Ukrayna ve küresel sistemden izole edilmesine yönelik planlama devreye sokulmuştur. Bu kapsamda, 16-28 Mart 2014 tarihleri arasında yoğunlaşacak şekilde Ukrayna'nın resmî mobil telefon şirketi olan Ukrtelecom'un altyapısını çökertilmiş, bu sayede de Kırım'daki mobil telefonların sıcak çatışmanın ilk günlerinde kullanılması engellenmiş, internette kısmi bir yavaşlama sağlanmış, kritik altyapıları felç eden siber saldırılar organize edilmiş, Sivastopol limanındaki Rus savaş gemilerinden Kırım'daki televizyon ve radyo yayınlarını kesecek elektronik karıştırmalar yapılmış ve "*kimliği belirsiz kişilerce*" Kırım'daki tüm fiberoptik kablo altyapısı zarara uğratılmıştır (Gürcan, 2014).

Daha sonra 2014 Nisan ayı sonuna kadar Lugansk ve Donetsk Bölgeleri'nin büyük bölümü RİS ve Rus özel kuvvetleri üyelerince eğitilen, yönlendirilen ve silahlandırılan Rusya yanlısı isyancılar tarafından ele geçirilmiştir. Karakollar ve hükümet merkezlerine isyancıların bayrakları ve RF bayrağı çekilmiş, Ukrayna bayrakları indirilmiştir. Donetsk ve Lugansk gibi iki büyük şehir de isyancıların eline geçmiştir.

SONUÇ

Devletlerin güvenliği ile ilgili konular, günümüzde tecrübe edilen teknolojik gelişmelerle birlikte değerlendirildiğinde, siber uzay alanındaki gelişmeleri yakından takip etmeyen/edemeyen devletlerin ciddi bir güvenlik zafiyeti yaşayacağı 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 imkanlar kapsamında etkili bir siber saldırı kapasitesine sahip olmak amacıyla yeniden organize etmeye çalıştığı da görülmüştür. Günümüzde siber savunma ve siber saldırı kapasitesinin ulaştığı boyut ile birlikte RF, küresel düzeyde çok önemli bir siber güç konumuna ulaşmış ve bu gücünü dış politikada bir baskı aracı olarak kullanmaktan çekinmeyen bir siber güvenlik stratejisini de benimsemiştir.

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 2008 yılında Litvanya'ya, 2009 yılında Kırgızistan'a yönelik siber saldırıları ile 2014 Ukrayna müdahalesi esnasında ortaya koyduğu "yeni nesil" savaş konsepti, RF'nin siber uzaydaki kapasitesini komşularıyla yaşadığı sorunlarda nasıl bir baskı ve zorlama yöntemi olarak kullandığının örnekleri olarak gösterilebilecektir.

Öte yandan RF'nin siber uzay alanında gösterdiği söz konusu etkinlik, sadece bu ülkenin komşuları üzerinde değil bir bütün olarak uluslararası sistemde de etkiler yaratmaya başlamıştır. Bu kapsamda RF'nin siber uzayda ortaya koyduğu her yenilik, planlama ve kapasite artırımı girişimi, başta ABD olmak üzere NATO'ya üye ülkeler tarafından kendilerine yönelik bir müdahale ve tehdit girişimi şeklinde okunmakta, bu hamleye cevap vermek adına da bu devletler hem siber savunma hem de siber saldırı alanında ciddi yatırımlar gerçekleştirmektedir.

Bununla birlikte RF'nin siber teknolojilere sahip olmak amacıyla yaptığı yatırımlar ve komşu ülkelere yönelik gerçekleştirdiği iddia edilen bahse konu siber saldırılar sonrasında, uluslararası sistemde yer alan diğer devletler de siber imkanların çok net bir şekilde dış politikada bir baskı aracı olarak kullanılabileceğini görmüşlerdir. Bir başka ifadeyle RF'nin siber uzay alanında ortaya koyduğu yenilikler ile geliştirdiği saldırı kapasitesi, bu hamlelere yönelik başta ABD olmak üzere NATO müttefiklerinin ortaya koyduğu tedbirler ve karşı girişimler günümüzde uluslararası ilişkilerde etkisini süratle hissettirmiştir. Bu nedenle süreç içinde söz konusu devletler, karşılıklı etkileşim ve etki-tepki ilişkisi kapsamında siber savunma ve saldırı kapasitelerini yeniden organize etmekte ve ülkelerinin savunma sisteminde siber tehditlere de ağırlık veren bir sistematiğe sahip olmak amacıyla planlamalar geliştirmektedirler.

KAYNAKLAR

ALKAN Mustafa (2012), **Siber Güvenlik ve Siber Savaşlar**, TBMM İnternet Komisyonu, https://www.google.com.tr/?gfe_rd=cr&ei=J0hhWLqZL6Ps8wfGxLD4Cg#q=Siber+G%C3%BCvenlik+ve+ Siber+Sava%C5%9Flar+tbmm, (25.12.2014).

AKYAZI Uğur (2013), **Uluslararası Siber Güvenlik Stratejisi ve Doktrinler Arasında Alınabilecek Tedbirler**, 6.Uluslararası Siber Güvenlik ve Kriptoloji Konferansı, http://www.iscturkey.org/s/2226/i/2013-paper105.pdf, (14.01.2014).

BIÇAKÇI Salih (2012), "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler**, Cilt 9, Sayı 34, Yaz 2012, ss. 205-226.

BIÇAKÇI Salih (2013), **21. Yüzyılda Siber Güvenlik**, İstanbul, Bilgi Üniversitesi Yayınları, Ağustos 2013.

BIÇAKÇI Salih (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler**, Cilt 10, Sayı 40, Kış 2014, ss. 101-130.

DEMİRCİOĞLU Cemalettin (2014), "Siber Uzayda Güç ve Güvenlik", **İdareci'nin Sesi**, http://www.tid.web.tr/ortak_icerik/tid.web/160/8%20Cemalettin%20DEM%C4%B0RC%C4%B0O%C4%9ELU.pdf, (10.02.2014).

GIBSON William (1984), **Neuromancer**, New York, Ace Books.

GOBLE A. Paul (2009), **Defining Victory and Defeat: The Information War Between Russia and Georgia**, In the Guns of August 2008: Russia War in Georgia**"**, edited by Svantee E. Cornell and S. Frederick Starr (Armonk, N.Y.: M.E. Sharpe)

GÜRCAN Metin (2014), **Rusya'nın Ukrayna'daki Bulanık Savaş Konsepti,** http://www.analistdergisi.com/sayi/2014/05/rusya-nin-ukrayna-daki-bulanik-savas-stratejisi, (22.04.2014).

HEİCKERÖ Roland (2010), "Emerging Cyber Threats and Russian Views on Information Warfare and Operation", **Swedish Defense Research Agency Press**, http://www.foi.se/rapport?rNo=FOI-R--2970--SE, (23.06.2014).

KELLY Sanja (2014), **Freedom on the Net 2014, Freedom on the Net (Freedom House, 2014),**
https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf., (24.04.2014).

LEE David (2014), **Russia and Ukraine in Cyber Stand-Off,** BBC News, http://www.bbc.com/news/technology-26447200, (23.04.2014).

MCLAUGHLIN Daniel (2014), **Lithuaniaaccuses Russian Hackers of Cyber Assault After Collapse of Over 300 Websites**,
http://lumen.cgsccarl.com/login?url=http://proquest.umi.com/pqdweb?did=1503762091&sid=2&Fmt=3&cl ientld=5094&RQT=309&VName=PQD;, (19.02.2014).

MEDVEDEV A. Sergei (2014), **Offence-Defence Theory Analysis of Russian Cyber Capability**, Master Thesis, Naval Post-Graduate School, Monterey, California, 2014,
https://www.google.com.tr/?gfe_rd=cr&ei=qzHZVrreN7Go8wfMuYegDw#q=this+thesis+represent+mikhail+tsypkin, (05.03.2014).

NYE S. Joseph (2014), **Cyber Power**, Harvard Kennedy School, Belfer Center for Science and International Affairs,
http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf, (19.02.2014).

OTTIS Rain (2008), **Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,** In Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, Reading: Academic Publishing Limited, 2008, http://www.academic-bookshop.com/ourshop/prod_1355933-ECIW-2008-7th-European-Conference-on-Information-Warfare-and-Security-Plymouth-UK.html, (18.04.2014).

RHOADS Christopher (2009), **Kyrgyzstan Knocked Offline**, Wall Street Journal, http://www.wsj.com/articles/SB123310906904622741, (19.04.2016).

ROTH Mathias (2009), **Bilateral Disputes Between EU Member States and Russia**, CEPS Working Document (Centre for European Policy Studies), August 2009, http://www.ceps.eu/files/book/2009/09/1900.pdf., (18.04.2014).

TİKK Eneken (2010), **International CyberIncidents: Legal Considerations**, Tallinn, Cooperative Cyber Defense Centre of Excellence, 2010, https://ccdcoe.org/publications/books/legalconsiderations.pdf, (16.04.2014).

WEEDON Jenand ve GALANTE Laura (2014), **Intelligence Analysts Dissectthe Headlines: Russia, Hackers, Cyberwar! Not So Fast,** Fire Eye Executive Perspectives, https://www.fireeye.com/blog/executive-perspective/2014/03/intel-analysts-dissect-the-headlines-russia-hackers-cyberwar-not-so-fast.html, (24.04.2014).

WILLIAM C. Ashmore (2014), **Impact of Alleged Russian CyberAttacks**, School of Advanced Military Studies United States Army Commandand General Staff College Fort Leavenworth, Kansas, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf, (19.04.2016).

YENER Yavuz (2014), **8. yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış**, https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/, (18.04.2014).