Russian Hegemony in Black Sea as a Cyber Power; Data Of 2015-2016 Cyber War

Vahit Güntay, Karadeniz Technical University

Abstract

With the dimension of internationalized cyber threats, phlosophical and ideological perception is evaluated with international security problems. At this juncture, data of cyber security and researches are revealed a conceptional base about the development of cyber terrorism. The determination of many studies with the frame of cyber deterrence is evaluated with the comparison Cold War theories and deterrence concept. There is one way of cyber attacks and it is hard to defend, besides there is not certain data about determining the facts. At the dimension of cyber security in Black Sea, for many experts; Russia is more dangerous than China at cyber war capacity. In a developing and changing world, Russia's hegemonic cyber area in a region has changed a threat dimension and now Russia has a deterrence ability. Some of the data and cyber war area support that idea. Particularly Turkey, region states have some weakness and that fact has some discussions in this research subject. In this study, Russia's capacity in Black Sea and its managing facilities at cyber area has been discussed with 2015-2016 data and risks for the region states have been revealed in the meaning of critical infrastructures.

Keywords: International Relations, Cyber Security, Cyber Politics, Cyber War, Cyber Deterrence

Özet

Siber tehditlerin uluslararasılaştığı boyutta felsefi ve ideolojik yaklaşım uluslararası güvenlik sorunlarıyla birlikte ele alınmaktadır. Bu noktada siber güvenliğe ilişkin veriler ve çalışmalar siber terörizmin gelişimine ilişkin kavramsal bir durumu ortaya çıkarmaktadır. *Siber caydırıcılık* dediğimiz kavram üzerinden birçok çalışmaya dair tespitler, caydırıclık kavramının Soğuk Savaş teorileriyle kıyaslanması üzerinden ele alınmaktadır ve tartışılmaktadır. Siber saldırıların bir yönü vardır fakat savunması zordur ve tespitine ilişkin kesin veriler kimi zaman olmayabilmektedir. Siber güvenliğin Karadeniz boyutunda; birçok farklı uzmana göre Rusya siber savaş kapasitesi açısından, Çin'den daha tehlikeli görülmektedir. Gelişen ve değişen dünyada, Rusya'nın bölgesel olarak hegemonyasını hissettirdiği siber alan bir tehdit boyutuna dönüşmüştür ve caydırıcılık kabiliyeti kazanmıştır. Son yıllarda karşımıza çıkan veriler ve siber savaş ortamı bunu destekler niteliktedir. Saldırı boyutunda ciddi adımlar atan Rusya'ya karşı başta Türkiye olmak üzere bölge devletlerinin zafiyetleri olduğu da tartışılan hususlar arasındadır. Çalışma kapsamında Rusya'nın Karadeniz bölgesinde siber alanı nasıl yönettiği, adımlar attığına ilişkin tespitler 2015-2016 verileriyle tartışılacak ve bölge ülkelerine ilişkin riskler hem veriler, hem de kritik altyapılar anlamında ortaya konulacaktır.

Anahtar Kelimeler: Uluslararası Ilişkiler, Siber Güvenlik, Siber Politikalar, Siber Savaş, Siber Caydırıcılık

MARMARA ÜNİVERSİTESİ

Giriş[1]

11 Eylül 2001, hiç beklenmedik bir şekilde yeni tehditleri beraberinde getirmiştir. Zengin ve güçlü ülkelerin de her an tetikte olmaları gerektiğini göstermiştir. Bazı devletler için ise Soğuk Savaş'ın çift-kutuplu sistemi sona erdikten sonra güvenlik sorunları daha da işin içinden çıkılmaz bir hal almıştır. Devletler adına zincirler kopmuş ve devletlerin birçoğu kitle imha silahları arayışına girmiştir. Siber kapasiteye dayandırılan unsurlar için ise maddi arayışlar kendini hissettirmeye başlamıştır.

Güvenlik algısındaki böyle bir değişimin temelinde Soğuk Savaş'ın sona ermesi, büyük bir dönüşüm olarak yorumlanmıştır. Bu dönüşümün nasıl ve hangi yönde olduğuna ilişkin sayısız imge ve kuram üretilmiştir.[2] Bu imgelerin başdöndürücü bir şekilde algısal değişimi ABD'de İkiz Kuleler ve Pentagon'a çarpan uçaklardan sonra yaşanmıştır.[3] Devletler arasında süren mücadeleler illegal yapılanmalara sıçramış ve uluslararası aktörler arasındaki güvenlik algısı artık bir algısızlığa dönüşmüştür.

Algının değiştirdiği rüzgar farklı savaş ve güvenlik konseptlerinden bir yenisini siyaset bilimi çalışmalarına eklemlemiştir. Uluslararası ilişkiler disiplini içinde sıkça adından söz ettirmeye başlayan siber güvenlik ve onun özelindeki çatışma boyutu bölgeler arasında yeni bir mücadele çeşidini ortaya çıkarmıştır.

Karadeniz özelinde de kendine yer bulan siber mücadele özellikle Rusya'nın içerisinde bulunduğu bir çerçeveyi ön plana çıkarmıştır. Soğuk Savaş yılları esnasında özellikle uzay çalışmaları ve askeri alanlarda siber alanı kullanan Rusya, günümüzün yeni savaş konseptlerinde bu baskınlığını koruma arzusu içine girmiştir. Karadeniz özelinde siber alandaki baskınlığıyla dikkat çeken Rusya, hibrit savaş dahilinde siber müdahele kartını hep masada bulundurmaktadır. Dönemsel olarak farklı zamanlardaki bu kartı kullanmaktan çekinmeyen Rusya, Karadeniz bölgesinde siber caydırıcı bir güç olarak bilinmektedir ve konuya ilişkin veriler oldukça artış içerisindedir.

Çalışma kapsamında siber savaş konsepti, kendi bütünlüğü içerisinde Rusya'ya yakınlaştırılarak açıklanmaya çalışılmış ve son yıllarda yükselişe geçen siber alana ilişkin birtakım veriler ortaya konulmuştur. Rusya'nın bölgesel olarak dikkat çekici baskınlığı ve bir müdahele çeşidi olarak siber alandaki araçları kullanması çalışma dahilinde değerlendirilen hususlar arasında yer almıştır.

1. Yükselen Siber Savaşlar

"Siber Savaş" kavramını; "ulusal bir hedefi gerçekleştirmek ya da süregelen bir savaşı desteklemek amacıyla, bir ülke tarafından veya inisiyatifinde, diğer bir ülkenin askeri ve sivil her türlü bilişim sistem ve altyapısının işlevselliğini engellemek, imha etmek ve kendi çıkarları doğrultusunda kullanmak için siber savaş yöntemlerinin kullanılması ve buna karşı koyacak tedbirler veya süreçler" şeklinde tanımlamak mümkündür.[4] Masrafsız bir savaş vizyonuna sahip olan siber savaş, saldırının hangi tarafında bulunduğuna göre, algısal bir farklılık temelinde kavramsal bir bütünlüğe sahiptir.[5]

[1] Bu çalışmanın bütünlüğü ve teorik açıklamaları yazarın "Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi (Micro-CAT)" adlı doktora tezinden kurgulunmıştır.

[2] Soğuk Savaş'ın hemen sonrasında, kapitalizm ve demokrasinin nihai zaferi ile birlikte dünyanın barışçı bir döneme girdiğini iddia eden Francis Fukuyama, savaş ve çatışmanın dönüşümüne dair dönemin en popüler imgesini üretmiş ve tarihin sonunun geldiğini ilan etmiştir.

[3] Evren Balta Paker, *Küresel Güvenlik Kompleksi: Uluslararası Siyaset ve Güvenlik* (İstanbul: İletişim Yayıncılık, 2012), 17.

[4] Gökhan Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi* (İstanbul: Yeniyüzyıl Yayınları, 2015), 48.

[5] Thomas Rid ve Peter McBurney, "Cyber Weapons", *The RUSI Journal* 157/I (2012): 7.

Siber savaş konseptinin gelişiminin aksine, yakın zaman itibariyle uluslararası alandaki tüm ilişkiler çatışma ya da savaş bağlamında gelişmemiştir. Farklı, karmaşık ilişkilerin biçimine ya da gelişimine göre aktörler stratejiler geliştirebilmektedir. Siber güvenlik alanında sadece çatışmacı bir yaklaşımla çalışmaların yönlendirilmesi önemli bir yanılgıyı beraberinde getirebilir. Bunun en önemli sebebi, uluslararası ilişkiler yaklaşımlarından inşacı teorinin konuyu ele alışı ile oldukça iyi özetlenebilir. Gelişim tek taraflı olarak devletler temelinde değildir. Bireysel ve toplumsal beklentiler de siber güvenlik alanındaki strateji düzeyini farklı alanlara taşıyabilir.

Strateji düzeylerini belirleyen devletlerin siber uzayın aktörü haline gelmesiyle devletlerarası çıkarlar, var olan güç potansiyelini siber güvenlik alanına kaydırmıştır. Devletlerin siber uzayın bir aktörü haline gelmesi, siber suçların etki alanının genişlemesine ve yarattığı tehdit potansiyelinin artmasına neden olmaktadır. Bu durum uluslararası ilişkiler içerisinde devletlerin siber güvenlik kavramını daha ciddi bir şekilde ele almaları zorunluluğunu getirmiştir. Siber güvenlik, iki büyük dünya savaşında olduğu gibi askeri ve jeopolitik üstünlüğü ön plana çıkaran taarruzlar yerine, bilgi sistemleri üzerinden yapılan, siber uzayın sunduğu sınırsız özgürlük ortamı içinde, daha kolay ve kısa sürede gerçekleştirilebilen saldırıları mümkün kılmıştır.[6]

Uluslararası sistemde bir aktörün stratejisinden söz etmek, aynı zamanda o aktörün amaçlarının neler olabileceğinden ve gücünden söz etmek anlamına gelmektedir. Siber savaşlar da bu yönde yoğrulmaktadır. Gelişmiş ve güç kriterlerini büyük ölçüde karşılayan bir aktörün amaçları ile bu amaçlarını karşılama ve tehditleri bertaraf etme kapasitesi, doğal olarak kendisine benzemeyenden farklı olacaktır.[7] Bu noktada siber savaş ve aktörler arasındaki farklılığa ilişkin saldırı ve savunma unsurları klasik güç yaklaşımına benzememektedir. Ülkelerin gelişmişlikleri ya da siber uzaya olan bağımlılığı ciddi sorunlara neden olabilmektedir.[8]

Rusya ve Siber Güvenlik

Bir çok farklı uzmana göre Rusya, siber savaş kapasitesi açısından Çin'den daha tehlikeli görülmektedir. Rusya'nın Moskova'da, ABD'nin NSA yapılanmasına benzeyen FAGCI (Devlet İletişim ve Bilişim Federal Teşkilatı) isimli bir kuruluşu vardır. Rusya siber yapılanması içinde Federal Güvenlik Servisi ve Beşinci Boyut Siber Ordusu öne çıkan birimlerdir.

Bir dönem Vladimir Putin'in de başında olduğu FSB, Rusya Federasyonu'nun iç güvenliğinden sorumlu teşkilattır. Rusya Devlet Başkanı'na doğrudan bağlı olan kurum, istihbarata karşı koyma, iç güvenlik, sınır güvenliği ve terörle mücadeleden sorumludur. Sovyetler zamanındaki KGB'nin günümüzdeki halidir. FSB, siber uzayda iletişim ağları dahil kritik altyapıların korunmasından sorumludur. FSB Kanunu'na göre. Rusya'da hizmet vermekte olan tüm telekomünikasyon hizmeti veren birey ve kurumlar, FSB'nin ek yazılım ve donanımlarına müsaade etmek zorundadır.[9] Bir başka deyişle, ülkenin telekomünikasyonel anlamdaki istihbarat altyapısı FSB tarafından denetlenmektedir.[10]

---

[6] Bayraktar, a.g.e., 24.

[7] Beril Dedeoğlu, *Uluslarararası Güvenlik ve Strateji* (İstanbul: Derin Yayınları, 2003), 61.

[8] Richard J. Kilroy, "The U.S. Military Response to Cyber Warfare", *Cyber Warfare and Cyber Terrorism*, 1. bs., haz., Lech J. Janczewski ve Andrew M. Colarik (Hershey: Information Science Reference, 2008), 443.

[9] SORM adı verilen bir internet izleme sistemi vasıtasıyla takipler yapılmakta, internet eşirim noktaları ve internet servis sağlayıcılarına sensörler yerleştirilmektedir. *İnternet Elektronik Gözetleme Merkezi*, elektronik iletişimin dinlenmesi ve deşifre edilmesinden sorumludur.

[10] Atalay Keleştemur, *Siber İstihbarat* (İstanbul: Level Kitap, 2015), 188.

Rusya'da siber savaş; hizmet dışı bırakma, hacker saldırıları, internet üzerinden dezenfermasyon yayma, devlet destekli grupların siyasi bloglarındaki faaliyetleri, siber takip ve muhaliflere baskı şeklinde gerçekleşmektedir. Yönetimsel anlamda, muhaliflerle olan siber mücadele yoğun bir şekilde Rusya gündemini meşgul etmektedir. FSB'nin kontrolündeki çeşitli gruplar, Rus ve uluslararası politik bloglarında Putin ve Rusya yanlısı propagandayı teşvik etmek amacıyla hareket etmektedirler.

Propagandaların temellendirilmesiyle birlikte, 1999 yılında Putin'in göreve gelmesi ile ulusal güvenlik politikası yeniden ele alınmış ve bilgi harekatı üzerine odaklanılmıştır. Bu tarihte ilk defa Rusya Federasyonu Bilgi Güvenliği Doktrini, yetkili Güvenlik Konseyi'ne sunulmuştur.

Rusya'nın siber alana ilişkin konseptinde siber güvenlik olgusunun askeri teknolojide son nokta olduğuna, hava kuvvetleri ve nükleer savaşlar kadar önemli olduğu varsayılmaktadır. Günümüze dek birçok siber saldırı sadece hedefteki bilgisayar ağlarına aşırı yük bindirmiş, sistemlerinin yavaşlamalarına veya çökmelerine sebep olmuştur. Rusya, 2008'deki Gürcistan işgalini bilgisayar sistemlerini aşırı yükleyerek gerçekleştirmiştir. Uluslararası ilişkilerdeki güç baskınlığı mücadelesinde, savunma sistemlerine saldıracak daha gelişmiş yöntemler tartışılmaktadır.[11] Bu gelişmeler neticesinde, klasik olarak güç algısı yerine, farklı yöntemlerle gücün kapsamını artırma ve küresel boyutta etkin olma adına farklı teorik yaklaşımların çıkış noktaları oluşturulmuştur. Uluslararası ilişkilerin aktörleri arasındaki mücadelenin de teknolojik bir devrim sonrasında teorik tartışmalarla yeni bir boyutta tartışılması kaçınılmaz hale gelmiştir.

Yeni ve gelişen boyut içerisinde Rusya'nın 2007 Estonya ve 2015 yılı Ukrayna'ya karşı yürütmüş olduğu müdaheleler stratejik siber savaşa tipik örnekler olarak karşımıza çıkmaktadır. Stratejik siber savaşlar açısından devlet içi sistemin aksatılması ve toplumsal olarak psikolojik harekata örnek oluşturabilecek bu türden olaylarda kısa dönem ve uzun dönemde devlet altyapılarında hasarların onarılması, nükleer ve konvansiyonel unsurların bıraktığı yıkıcı etkilere göre daha kolaydır.

Operasyonel siber savaşlar açısından ise müstakil bir savaş kombinasyonu yoktur ve tekil bir amaç dahilinde karakteristik özellikler mevcut değildir. Bir konvansiyonel savaşta, müdahele ya da askeri bir amaç güdülecekse fonksiyonel olarak siber unsurlarla destek gözetilmelidir. 2008 yılında Güney Osetya Savaşı esnasında Rusya'nın Gürcistan'a yürütttüğü eş zamanlı siber müdaheleler operasyonel siber savaşlar açısından özgün örnekler arasındadır.

Rusya ve siber güvenlik olgusu içerisinde rakibi yıpratmaya yönelik tartışılan hibrit savaşta uzun süreli planlar yapılabilir ve zamana yayılabilir. Kısa sürede kesin sonuçlar beklemek hibrit savaşlar açısından gerçekçi durmamaktadır. Rusya'nın 2014 yılında Ukrayna'daki faaliyetleri, Doğu Avrupa açısından Rusya'nın her fırsatta hibrit savaşı bir harekat biçimine dönüştürebileceği gerçeğini ortaya koymuştur. Karar alıcılar açısından yeni bir konseptin önlerinde olduğunu ortaya çıkaran benzer müdaheleler NATO gibi örgütlenmelerin de ajandalarında ilk sıralara yükselmiştir.[12]

Farklı örgütler ve devletler açısından siber savunma disiplininin oluşmasında her devlet kendi önceliklerini analiz etme yeteneğine sahip olmalıdır. Şekil 1, Rusya bazında ele alınan Hibrit Savaş (Gerasimov) Konsepti'nde bu ayrımın ve önceliklerin temel unsurlarını göstermektedir. Gerasimov konsepti, siber savaş yanında ekonomik savaş, diplomasi, bilgi savaşı ve propaganda, düzenli askeri birlikler, özel kuvvetler, düzensiz kuvvetler ve hatta karşı

[11] Michael G. Roskin ve Nicholas O. Berry, *Uluslararası İlişkiler Uİ'nin Yeni Dünyası*, çev., Özlem Şimşek (Ankara: Adres Yayınları, 2014), 328.

[12] Özellikle Rusya, hibrit savaş uygulamalarıyla ile birlikte, Soğuk Savaş sonrasında son 15 yılda gücünden söz ettiremezken yeniden atağa geçmiştir. Rusya'nın özellikle Estonya ve Ukrayna gibi ülkelerde açığa çıkan saldırıları ve faaliyetleri bölge ülkelerini de tedirgin etmeye başlamıştır.

taraftaki yerel ayaklanmaların desteklenmesini de aynı kategoriye alarak bir kombinasyon oluşturmuştur. Oluşturulacak her mimari ve devletlerin ortak noktaları özellikle yakın ittifakların kurulmasında çıkarsal kesişmeler doğurabilir.

Şekil 1. Konvansiyonel ve Konvansiyonel Olmayan Savaş Unsurlarının Çoklu Kombinasyonu[13]



Ortak siber savunma disiplini oluşturmada devletlerin belli güç paydalarında buluşabilmeleri ve bunu orantılayabilmeleri önemlidir. Siber kontrollü sistemleri daha fazla kullanması ve ulusal siber savunma sistemi eksikliklerinden dolayı ABD, günümüzde Rusya ya da Çin'e kıyasla, hatta siber alanda gelişmekte olan bir devlete göre saldırılara daha açık konumdadır. Özellikle uluslararası alanda, güvenlik temelli mücadelelerde geliştirilen her yön rakip kuvvetlerin temel hedefi haline dönüşebilmektedir.[14] ABD siber savaş kapasitesi olmayan, ama yetenekli hacker ekipleri kiralayabilecek devletler veya devlet sayılamayacak unsurlar tarafından tehdit bile edilebilir.[15]

3. Rusya ve Siber Verilere İlişkin Güncel Tespitler

Rusya'nın 2007 Estonya ve 2015 yılı Ukrayna'ya karşı yürütmüş olduğu müdaheleler stratejik siber savaşa tipik örnekler olarak karşımıza çıkmaktadır. Stratejik siber savaşlar açısından devlet içi sistemin aksatılması ve toplumsal olarak psikolojik harekata örnek oluşturabilecek bu türden olaylarda kısa dönem ve uzun dönemde devlet altyapılarında hasarların onarılması, nükleer ve konvansiyonel unsurların bıraktığı yıkıcı etkilere göre daha kolaydır.

Şekil 2'de web tabanlı saldırılarda devletlerin küresel etkilenme oranları gösterilmiştir. Ortaya çıkan oranlara göre Rusya bu etkiden en fazla payını alan ülkeler arasındadır. Temel olarak saldırı disiplini oluşturmaya çalışan ülkelerin genel sorunsalı şeklinde karşımıza çıkan bu etkilenme önemli bir göstergedir. Ülkelerin saldırı motivasyonunun bir parçası haline gelen siber unsurlar kendi içindeki alanını genişlettikçe birtakım açıkları ve sorunları da beraberinde

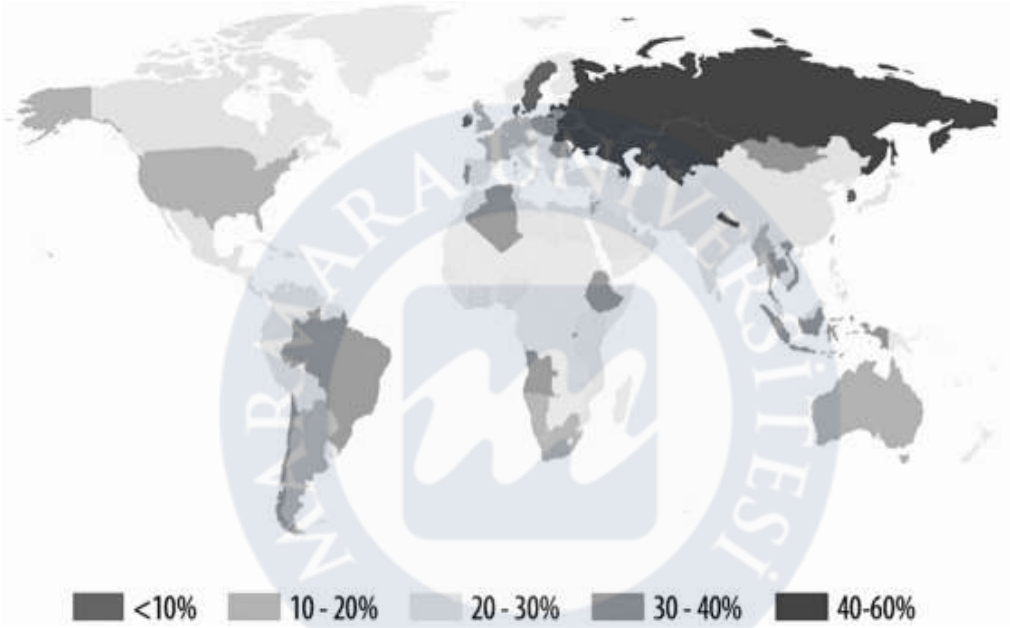
[13] Teo Jing Ting, Never Take Our Peace for Granted: Dr Ng, son güncelleme 6 Mart 2016, https://www.mindef.gov.sg/imindef/resourcelibrary/cyberpioneer/topics/articles/news/2015/mar/05mar15_news.html#.V6wveGXwyuV.

[14] ABD başka ülkelere göre daha gelişmiş siber saldırı olanaklarına sahip olabilir fakat Çin, ABD'nin büyük kentlerindeki elektrik şebekelerini haftalarca arızaya uğratır, verilerini bozarak finans pazarlarının kapanmasına neden olur ve demiryolu hatlarında yönlendirme sistemlerini bozarak gıda ve parça sıkıntılarına yol açarsa, siber saldırı olanaklarınızın üstünlüğü işe yaramayacaktır.

[15] Richard A. Clarke ve Robert K. Knake, *Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit*, çev., Murat Erduran (İstanbul: İKÜ Yayınevi, 2011), 82.

getirmektedir. Rusya ve çevre ülkelerin artan biçimde web tabanlı saldırılardan etkilenmesi siber alana artan bağımlılık ve birtakım operasyonel unsurların bu alana entegre edilmesi ile ilgilidir. Askeri alandaki yenilikler ve atılım, Rusya gibi ülkeleri bu konuma daha da yakınlaştırmıştır ve siber alan hibrit savaşlarda Rusya'nın elini güçlendirirken karşılaştığı sorunsal bütünlüğü de genişletmiştir. Bu durum gelecek kurgusunda daha da fazla soruna yol açacaktır.

Şekil 2. Web Tabanlı Saldırılarda Devletlerin Küresel Etkilenme Oranları[16]

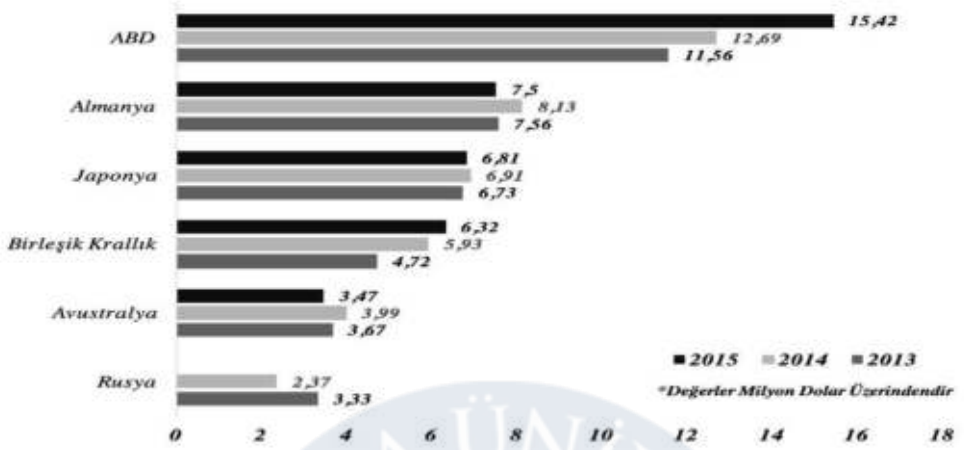


Özellikle Rusya gibi siber alanın farklı araçlarla kullanıldığı ülkelerde sahip olunan kaynaklara göre ise siber suçlar çoğu zaman çeşitlilik gösterememektedir. Grafik 1 bu durumun iyi bir örneğini sunmaktadır. Ülkelerin birçoğu gelişmişlik düzeyi ve sahip olduğu kaynaklara göre hedef haline gelmektedir. Siber alanda faaliyet gösteren ülke içinde ve dışındaki bireyler verilmek istenilen zararı maddi kaynağın niteliğine göre şekillenmektedir. Bu noktada başta ABD olmak üzere; Almanya, Japonya, Birleşik Krallık, Avustralya gibi ülkeler temel hedefler haline dönüşmektedir. Rusya'nın bu noktada oldukça geride olduğu dikkat çekicidir. Bu durumun oluşumunda ülke dışındaki saldırılar da belirleyici olmaktadır. Özellikle Rusya gibi ülkelerde hackerların yöneldiği merkezler doğal olarak kendi ülkeleri olmamaktadır. Bu temelde belirleyici olan husus ülkelerin hackerları ve siber suçları kanalize ettiği merkezlerdir. Rusya gibi ülkeler yine bu konuda rotayı farklı ülkelere çevirmeyi bilmektedir. Siber suçların sınır tanımayan özellikleri bu merkeziliği güçlendirmektedir.

Grafik 1. Siber Suçların Global Düzeyde Bazı Ülkelere Maliyetleri[17]

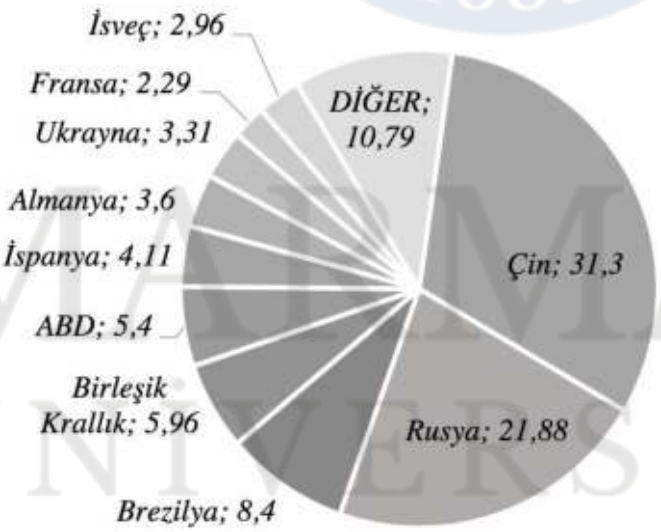
[16] Kaspersky Lab. "Kaspersky Security Bulletin", son güncelleme 13 Temmuz 2016, https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin2015_FINAL_EN.pdf, (Kaspersky Laboratuvarlarının ölçümlerine göre 2015 içinde her üç bilgisayardan (%29) biri, bir veya daha fazla web tabanlı saldırıya uğramıştır. Genel olarak yüksek oranlara sahip zararlı programlar rapor içerisinde ayrıca belirtilmiştir.)

[17] Ponemon Institute, "2015 Cost of Cyber Crime Study: Global", son güncelleme 6 Şubat 2016, http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states.



Grafik 2'de ise zararlı yazılımların kaynaklandığı ülkeler ortaya konulmuştur. Özellikle Rusya'nın bu konudaki baskınlığı dikkat çekici bir diğer unsuru oluşturmaktadır. Siber politikada çıktılar oluşturma adına genelde G-8, özelde ise bu çatı altındaki İngiltere, Fransa, Almanya, İtalya ile Japonya, Kanada, Rusya ve ABD arasındaki siber suçlarla olan mücadelede güvenliğin bölgeselleşmesi açısından eldeki veriler kayda değerdir. Yapılan toplantılarda, 1995 yılından beri bölgesel gelişmelerle birlikte siber suçlarla mücadele konusu ele alınmaktadır. Bu toplantılar neticesinde çalışma grupları oluşturulmuş, siber suçlarla mücadelede eylem planları hazırlanmış ve faaliyete geçirilmiştir. Zararlı yazılımların oluşturduğu genel bütünlük tüm ülkeler adına ciddi bir sorunsalı oluşturmaktadır. Rusya bu konuda Çin ile birlikte ilk sıralarda yer almaktadır. Her ne kadar Rusya merkezli güvenlik şirketlerinin etkinliği baskın olsa da daha önce vurguladığımız gelişen siber alan içindeki faaliyet bütünü Rusya'nın elini zayıflatmaktadır.

Grafik 2. Zararlı Yazılımların Kaynaklandığı Ülkeler[18]

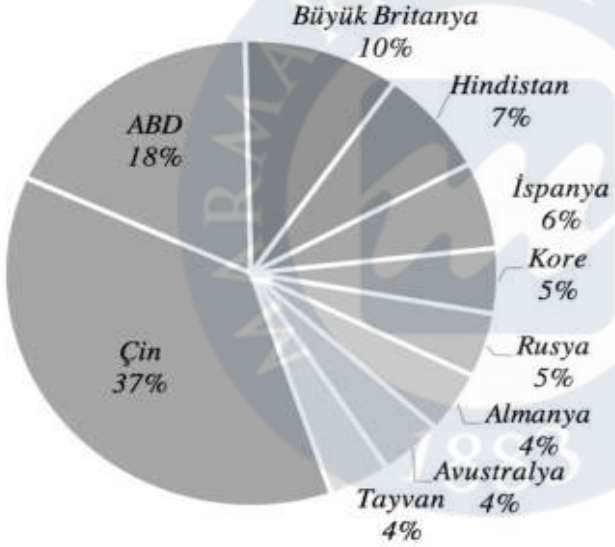


DDos saldırıları ve istihbarat amaçlı Botnetlerin kullanımında Rusya'nın saldırı kapasitesinin özellikle çevre ülkelerde etkin şekillerde kullanıldığı, bu saldırı türlerine maruz

[18] Bogda Botezatu, "H1 E-Threat Landscape Report: Malware, Spam and Phishing Trends", Bitdefender, son güncelleme 6 Temmuz 2016, http://www.bitdefender.com/media/materials/e-threats/en/H1_2011_E-Threats_Landscape_Report.pdf.

kalınması açısından Rusya'nın bazı temel noktalarda hazırlıklı olduğu görülmektedir.[19] Grafik 3'te DDoS saldırılarının kaynaklandığı ilk 10 ülke verilmiştir. Özellikle 2015 yılı içinde ABD, Çin ve İngiltere gibi ülkelere oranla geride kalan Rusya, tehdidin ortaya çıkışı açısından ve saldırı amaçlı kaynaklara göre, DDoS saldırılarında olduğu gibi düşük oranlara kaynaklık etse de farklı siber silahlarla etkinliğini sürdürmektedir. Rusya grafik 3 dahilindeki sıralama içinde oldukça iyi bir yere sahiptir. Özellikle uluslararası kimi sorunlarda, farklı siber saldırı türleriyle sahneye çıkan Rusya çoğu zaman yapmış olduğu müdahelelerde risk de almaktadır. Bunun temelinde uluslararası arenada çoğu dönemsel gelişme içerisindeki yalnızlığı belirleyici olmaktadır. Konvansiyonel birtakım unsurlar yerine siber saldırıları kullanması ve bu konuda ciddi bir araştırma içerisinde oluşu bu durum için iyi bir örnek oluşturmaktadır. Çevre ülkeler adına bu durum risk içermektedir. Türkiye ile yaşanan kimi dönemsel krizlerde siber saldırı seçeneği Rusya için iyi bir araç haline gelmiştir.

Grafik 3. 2015 Yılı DDoS Saldırılarının Kaynaklandığı İlk 10 Ülke[20]



Ters yönde etkinin yanında gelişmişliğin doğru orantılı bir şekilde ele alınabileceği husus siber savunma gücüne ilişkindir. Grafik 4'te yer alan bilgiler McAfee tarafından sunulan *Siber Güvenlik Raporu'*na aittir ve görüldüğü üzere tam kapasite güce sahip ülke mevcut değildir. Diğer taraftan Finlandiya, İsveç, İsrail gibi ülkelerin Rusya, Çin ve ABD gibi ülkelerin önünde siber savunma kabiliyetlerinin olduğu da dikkat çekicidir.[21] Ülkelerin siber savunma güçleri her ne kadar karşılaşılan saldırı türleri ve maddi kayıplara göre oranlanılsa da saldırıların yöneliş biçimi ve hedeflenilen unsurlar bu tür sınıflandırmalarda belirleyici olmaktadır. Savunma gücünün siber alanda gelişmekte olan ülkeler açısından ne ifade ettiği denetlenebilir bir husus değildir. Ülkelerin bir savunma kapasitesi varsa bu durum siber alana olan bağımlılık ve güvenlik faaliyetlerinin seyrine ilişkin olarak karşımıza çıkmaktadır. Rusya, Çin, Türkiye gibi ülkelerin aynı derecede yer almasında belirleyici olan unsur entegre edilen veri bütünlüğü

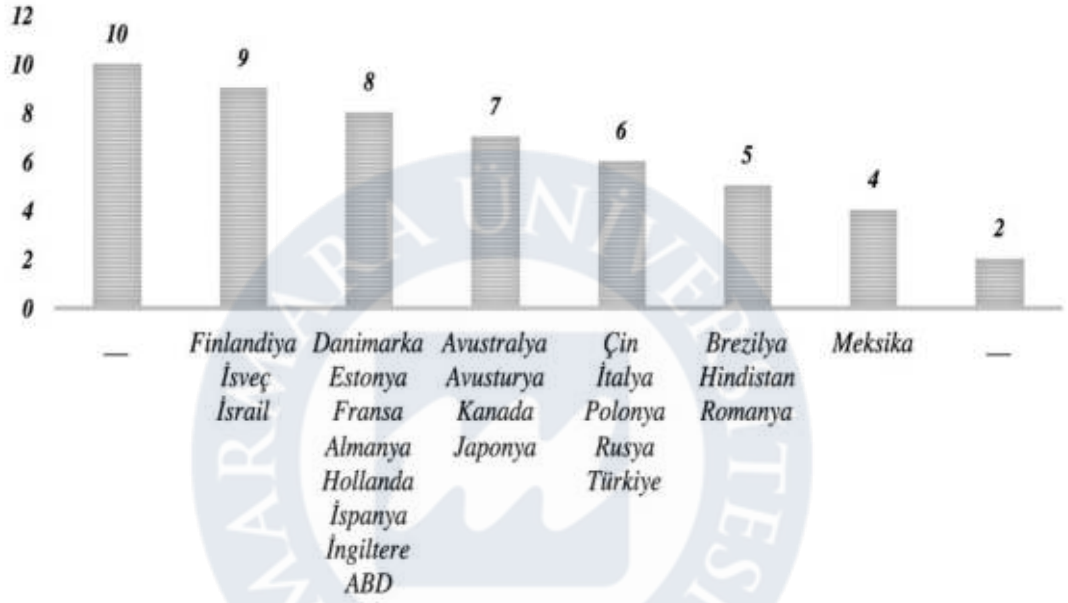
[19] DDoS saldırıları temel olarak 2 şekilde gerçekleştirilmektedir. Bunlardan birinde çok sayıda farklı kullanıcının; sosyal medya, forum, IRC gibi kanallar üzerinden organize olarak aynı anda bir sisteme erişmeye çalışması şeklinde olmaktadır. Diğerinde ise Botnet üyesi olan zombi makinelerin bilinçsizce sisteme erişimi şeklinde gerçekleşmektedir.

[20] Platform, "Internet Security Report Shows Spike in Cyber Threats", son güncelleme 9 Mayıs 2016, https://www.ncta.com/platform/broadband-internet/internet-security-report-shows-spike-in-cyber-threats/.

[21] Keleştemur, a.g.e., 171.

ile ilgilidir. Son yıllarda özellikle yönetenlere ait verilerin tehlike içinde oluşu ve genel bir tehdit aracı olarak görülmesi bu konuda önemli bir tespittir. Siber alanın oluşmuş bir bütünlüğü yoktur ve Rusya'nın saldırı yönündeki merkezi gelişimi savunma açısından birçok riski de beraberinde getirmektedir. Bu risklerin başında askeri alandaki verisel bütünlük ve bunun oluşturduğu tehdit gelmektedir.

Grafik 4. Ülkelerin Siber Savunma Güçleri[22]



Ülkelerin siber saldırı ve savunma güç kapasiteleri açısından, gelişmekte olan ülkeler adına belirleyici unsurlar daha çok sahip olunan özelliklerin dağılımıdır. Bu dağılım kendi içerisinde güç kapasitesini belirler ve ayrıştırır. Tablo 1'de görüldüğü üzere, belli özellikler dahilinde ülkeler farklı şekillerde gruplandırılabilmektedir. Birinci grup ülkelerin en ayırıcı özelliği siber güvenlik politikalarının oluşturulması ve bu konudaki yatırımların dağılımıdır. Türkiye'nin de içinde bulunduğu üçüncü grup ülkelerde farkındalık olmasına rağmen, öze ilişkin politikaların üretilemeyişi temel sorunlar arasındadır. Bunun altında yatan sebep, bu tarz ülkelerin siber saldırı ve savaş pozisyonları açısından denetime ihtiyaç duymalarıdır. Dikkat çekici diğer bir husus sınıflandırılan ülkelerin ekonomik gelişmişlik verileriyle siber kabiliyetleri arasında doğru orantılı bir ilişkinin olmadığıdır. Rusya her ne kadar savunma derecesi olarak düşük bir kategoride yer alsa da savaş kabiliyeti saldırı ve savunma ağırlığında üst kategoride yer alan bir ülkedir. Siber güvenlik politikaları oluşturma hususunda risk alabilen ülkeler arasında yer alan Rusya bu durumu gelecek vizyonu haline de dönüştürerek ciddi bir potansiyel haline gelmektedir. Bu potansiyelin oluşturulmasında gerekli kaynakların kullanılması öncelik haline gelmiştir. Özel bazı şirketlerle de iş biriliği halinde olan Rusya önemli adımlar atmaktadır.

Tablo 1. Ülkelerin Siber Savaş Kabiliyetlerinin Sınıflandırılması[23]

Grup	***Ülkeler***	***Özellikleri***
Birinci Grup	*ABD* *Çin* *Rusya*	*Siber güvenlik ve savunma geliştirme çabaları üzerine uluslararası politika üretme kabiliyetine sahip ülkelerdir. Bu ülkeler siber savunma konularına en büyük desteği vermekte,*

[22] Keleştemur, a.g.e., 171.
[23] Hasan Çifçi, Her Yönüyle Siber Savaş, (Ankara: TÜBİTAK Bilim Kitapları, 2012), 26.

		siber güvenlik politikaları oluşturma çabalarına en fazla kaynak ve insan desteği sağlamaktadır.
İkinci Grup	*İngiltere Fransa, İsrail*	*Birinci gruptaki ülkeleri yakından takip etmektedirler. Ancak daha az personel ve daha kısıtlı altyapıya sahiptirler.*
Üçüncü Grup	*Türkiye, Hindistan Güney Kore Tayvan, Almanya Kuzey Kore*	*Siber güvenlik politikası ve savunma kabiliyetleri geliştirilmesi için önemli ölçüde kaynak tahsis eden ülkelerdir. Bu alanda lider ülke değildirler. Birçok durumda, birinci gruptaki ülkeleri taklit etmektedirler.*
Dördüncü Grup	*İsveç, Japonya, İran Avustralya, Hollanda Pakistan, Finlandiya*	*Siber güvenlik ve savunma kabiliyetlerine yönelik kısıtlı kaynak tahsis eden ülkelerdir.*

Siber güç kapasitesi açısından, siber alanda gelişmekte olan devletler belli düzeyde iyi tanımlanmış kurum ve kuruluşlara sahip olsalar da, kurumsallaşma açısından gelişime duydukları ihtiyaç ortadadır. Bu tür devletler kapsamlı ve devamlı savunma faaliyetlerini kısmen sürdürebilmektedirler fakat saldırılara yönelik güdülerde daha zayıf oldukları gözden kaçırılmamalıdır. Tablo 2'de farklı silah türlerinin geliştirme maliyetleri gösterilmiştir. Rusya gibi ülkelerin askeri alanda yapabilecekleri her türden girişim farklı sistemlerin gelişmesine olanak veren kapasiteye sahip görünmektedir. Uluslararası alanda müdaheleci olma ve bunu günün şartlarına entegre edebilme imkanları daha da çok geliştirmektedir. Siber silahların geliştirilmesi maliyet hususunda konvansiyonel unsurlara göre daha kolaydır. Bu durum sistemsel olarak uluslararası düzenin yapısına daha fazla yük ve karmaşıklık eklemektedir. Uluslararası alanda baskın olma mücadelesi devletleri daha az maliyetlerle etkili olabilme noktasında Rusya gibi ülkelerin iştahını kabartmaktadır. Bu durumun oluşturduğu kaos ortamı siber savaşların yönünü de belirler hale gelmektedir.

Tablo 2. Silah Geliştirme Maliyeti[24]

Silah Sistemi	***Maliyet (USD)***	***Kimler Geliştirebilir?***
Görünmez Savaş Uçağı	*397 Milyar (F-35)*	*ABD, Çin, Rusya*
Nükleer Denizaltı	*11 Milyar*	*ABD, Rusya, İngiltere, Fransa, Çin, Hindistan*
Askeri Hedefler İçin Siber Silah programı	*1 Milyar*	*Gelişmiş Ülkeler*
Sivil Hedefler İçin Siber Silah Programı	*100 Milyon*	*Gelişmiş ve gelişmekte olan tüm ülkeler*
Kritik Bir Altyapıya Yönelik Siber Saldırı	*5 Milyon*	*Herkes (devlet, teröristler, organize suç örgütleri…)*
Ulusal Siber Güvenlik Programı (sivil)	*>1 Milyar*	*Politika, Strateji, İcra (5-10 sene)*

[24] Firuze Taytaş, "Türkiye Cumhuriyeti Siber Silah Geliştirmeli mi?", son güncelleme 25 Nisan 2016, https://www.linkedin.com/pulse/türkiye-cumhuriyeti-siber-silah-geliştirmeli-mi-firuze-taytaş.

Sonuç Olarak;

Siber savaşların teorik bir düzlemde ele alındığı günümüzde ışık hızından daha hızlı bir şekilde gerçekleşen siber saldırılar uzun vadede devletlerin tercih edeceği ve bir o kadar da sorun yaşayacağı unsur haline gelmiştir. Özellikle Karadeniz gibi bölgelerde güven bağının oldukça zayıf olduğu toplumlar ve genelindeki devletler bu konuda gerekli politikaları üretmeye mahkumdur.

Rusya'nın sahip olduğu kapasite ve alana ilişkin müdaheleleri oldukça gerçekçi ve saldırgan bir zeminde kısa vadede çıkarsal bir bütünlük oluşturmaktadır. Bunun örneklerini yapılan saldırılarda ve dönemsel olarak yaşanan sorunlarda bir tercih mekanizması gelen boyutuyla daha iyi gözlemlemekteyiz. Siber alanın kendi içindeki karmaşıklığı Rusya açısından bu saldırıları daha tercih edilir bir hale getirmektedir.

Siber alandaki mücadele son zamanlardaki verilerle de kurgulandığında, kendisini siber alanın karmaşıklığı içinde tanımlayan ülkeleri aynı zamanda karşı saldırılardan nasibini her an alabilir konuma getirmektedir. Özellikle Rusya gibi ülkelerin Karadeniz'de baskın olduğu siber alan ve mücadele mantığı, bu ülkeyi potansiyel risklerle de karşı karşıya getirmektedir. Fırsatların siber alanda genişletilmek istenmesi ülkelerin prestijleri açısından da ciddi sorunlar içermektedir. Hatta son dönemlerde uluslararası hukukta da sıkça tartışılmaya başlanılan siber saldırılara karşı olası konvansiyonel müdaheleler devletleri ciddi problemlere sürükleyecektir.

Karadeniz özelinde Türkiye gibi ülkelerin siber alanın karmaşıklığı ve Rusya'nın müdahelelerine ilişkin adımlar atması zorunlu gözükmektedir. Dönemsel bazı sorunlarda Rusya'nın misilleme olarak ilk tercih ettiği müdahele araçları arasına siber silahlar yerleşmiştir ve bir alternatifi değil, ilk kullanılan unsur haline gelmiştir. Bunun temelinde yatan sebep kapalı kapılar ardında gerçekleşen siber saldırıların aynı zamanda kimi kullanım türlerine göre maliyetsiz oluşudur.

MARMARA ÜNİVERSİTESİ