ULUSLARARASI SİBER ÇATIŞMA ANALİZİ: RUSYA'NIN ABD SEÇİMLERİNE MÜDAHALESİ

Çağrı Gülerer[♣]

Özet

Amerika Birleşik Devletleri, 2016 yılında yapılan başkanlık seçiminden sonra çok derin bir siber güvenlik açığıyla sarsılmıştır. Seçimlerin öncesinde Demokrat Parti'nin adayı Hillary Clinton'ın e-postalarının sızdırılması, yalnızca Clinton'ı ilgilendiren bir güvenlik açığı gibi görünürken; seçimlerden sonra Rusya Federasyonu adına çalışan hackerların seçimlere ciddi bir müdahalede bulunduğu iddiası ortaya atılmıştır. Cumhuriyetçi Parti adayı Donald Trump Jr.'ın kazandığı 2016 başkanlık seçimleri sonrası Amerika Birleşik Devletleri'nde bu konuyla ilgili ciddi bir soruşturma başlatılmış ve ortaya atılan iddialar ayyuka çıkmıştır. Trump, seçimlere müdahale edilmiş olabileceği söylerken, Rusya Federasyonu kendi hükümetlerine bağlı bir hacker timinin böyle bir eyleminin olmadığını öne sürmüştür. Çalışmada, Rus hackerların seçimlere nasıl müdahale ettiği incelenirken, iki ülke arasında yaşanan bu kriz siber çatışma analizi perspektifinden incelenmiştir.

Anahtar Kelimeler: siber güvenlik, siber çatışma analizi, Donald Trump Jr., Rus hackerlar

Abstract

After the 2016 presidental elections, United States of America has been shocked with a deep cyber security gap. It had seen that being leaked of Democrat Party's candidate Hillary Clinton's e-mails is a security gap interests only Clinton; after the election it was claimed which a hacker group works for Russian Federation interfered to the elections seriously. An investigation has started after the triumph of Donald Trump Jr. at 2016 elections in United States of America, and the alleged claims were louded. While Trumps says there might be an intervention to the elections, Russian Federation asserted that there was no action of any hacker team which works for themselves. While it's searched how Russian hackers interfered to the elections in this work, the crisis between those two countries studied from the perfpective of cyber conflict analysis.

Key words: cyber security, cyber conflict analysis, Donald Trump Jr., Russian hackers

♣ Ph.D. Student, Department of International Relations, Selçuk Univetsity-Konya-Turkey

Giriş

Çatışmalar, uluslararası ilişkiler disiplininde önemli bir yer teşkil etmektedirler. Bu konudaki çalışmalar, uzun yıllardır kinetik çatışmaları analiz etme amaçlı yapılmışlardır. Kinetik çatışma analizleri günümüzde halen yapılmaya devam etse de uluslararası ilişkilerin siber uzaya sıçramasıyla, siber çatışmalar popülerlik kazanmaya başlamışlardır. Bu durum, uluslararası ilişkilerin de birçok açıdan yeniden yorumlanmasına neden olmaktadır. Siber çatışmaların popülerleşmiş olması, kinetik çatışmaların önemini azaltmamış; aksine her iki çatışma çeşidi arasındaki bağ ve ilişki, araştırmaya değer bir konu olarak ortaya çıkmıştır.

Siber çatışmaları analiz etme safhası ise çok daha karmaşık ve belirsizdir. Bunun nedenlerinin başında, siber çatışma kavramının çok yeni olması ve özelliklerinin tam anlamıyla netleşmemiş olması gelmektedir. Kinetik çatışmaların analizinde kullanılan parametrelerin çoğu, siber çatışmalar için kullanılamamaktadır. Günümüzde siber çatışma analizi yapılabilmesi için, mevcut konuyla ilgili bazı kritik bilgilerin bilinmesi gerekmektedir. Aynı şekilde, siber çatışmaları ölçen parameterelerin kinetik çatışmalarınkilerle örtüşmemesi, araştırmacıları farklı parametre araçları bulmaya yönlendirmektedir. Kinetik çatışma analizlerinde elde edilen sonuçlardan ortaya çıkan bilgilerin kavramsal boyutu ise yine siber çatışmalarda farklılık göstermektedir.

Geleneksel çatışmaların siber uzaya sıçraması, aslında Soğuk Savaş'tan günümüze uzanan bir hikayeye sahiptir. 2. Düyna Savaşı sonrası geleneksel savaşların terkedildiği çift kutuplu uluslararası sistem, Amerika Birleşik Devletleri ve Sovyetler Birliği'ni uzayda bile karşı karşıya getirmeye başlamıştır. Kitle imha silahlarıyla büyük yıkımlar yapılabildiğini gören dünya kamuoyu, bu tarz silahları kullanmaya çekinse de devletlerin hızla silahlanma yarışı içerisinde olduklarının farkına varmıştır. Bu silahlanma yarışında ise bir önceki yüz yılnda ön plana çıkan "endüstrileşme" hamleleri yerine, teknolojik ilerleme popülerleşmiştir. Bilginin güç olduğu bir çağda yaşayan insanlık, bu bilgi aracılığıyla ürettiği interneti ve siber uzayı, yine bilgi için bir depolama ve transfer aracı olarak kullanmaya başlamıştır. Bu durum da siber uzayı uluslararası ilişkilerde yeni bir değişken olarak ortaya koymuş ve birçok tehdit tarafından tehlike altına sokmuştur. Topla, tüfekle, donanmayla ya da çitle korunamaz olan siber uzay, tam anlamıyla anarşinin hakim olduğu yeni bir mecra haline gelmiştir.

Soğuk Savaş döneminde birçok teknolojik ilerleme kaydeden Sovyetler Birliği, Rusya Federasyonu döneminde de teknolojik ilerlemeyi siyasi stratejisinin merkezine oturtmuştur. Bu bağlamda, Rusya'nın siber uzaya ve internete yaklaşımı biraz daha farklı olmuştur. Birçok ülke bu teknolojiyi kendini ve insanlığı geliştirme amaçlı kullanırken, Rusya daha çok başka sistemlere zarar verip müdahalede bulunarak kendini geliştirme yolunu tercih etmiştir. Birçok farklı hacker örgütü bulunan Rusya; batı ülkelerinin seçimlerine müdahaleden seçim kampanyalarını destekleyen kurumlara, eski doğu bloğu ülkelerini yeniden dizayn etme çabasından medya kuruluşlarına müdahale etmeye kadar birçok farklı aktivite içerisindedir. 2016 ABD başkanlık seçimi de bunlardan biridir.

Bu çalışmada, Rus hacker örgütleri Cozy Bear ve Fancy Bear'ın ABD'deki 2016 başkanlık seçimine müdahale ettiği iddiaları analiz edilmektedir. Çalışmanın ana hattını kinetik çatışmalardan siber çatışmalara geçiş ve Amerika Birleşik Devletleri ile Rusya Federasyonu arasındaki bu etkileşimin "siber çatışma" kavramına ne denli girdiği oluşturmaktadır. Çalışmanın ilk bölümünde; çatışma kavramı ve kavramın kinetik ile siber olarak ayrımının yapılışı açıklanmaktadır. İkinci bölüm, Rusya Federasyonu'nun siber güvenlik stratejilerine ve Cozy Bear ve Fancy Bear örgütlerinin misyon ve vizyonuna odaklanmıştır. Bu bölümde Cozy Bear ve Fancy Bear örgütlerinin Kremlin ile bağlarının olduğu iddiaları üzerinde de durulmuştur. Son bölümde ise Amerika Birleşik Devletleri'nde gerçekleşen 2016 başkanlık seçimleri öncesi, Demokrat Parti'nin yürütme organı olan Demokratik Ulusal Komite'ye yapılan siber saldırı ve sızdırılan 20.000'i aşkın e-postanın analizi yapılmaktadır. Ayrıca bu bölümde; FBI'ın konuyla ilgili açtığı soruşturmaya, Trump ve Rusya'nın müdahalelerin arkasında Kremlin'in olduğunu reddetmesine ve yine Trump'ın Demokrat Parti'yi FBI'ın e-postaları incelemesine karşı çıkışına getirdiği eleştirilere değinilmiştir.

1.Kinetik Çatışmadan Siber Çatışmaya

Çatışma yönetimi ve iyi bir yönetim için ihtiyaç duyulan çatışma analizi, geleneksel hukuk kurallarının çözmekte sıkıntı yaşadığı konularda önemli bir rol üstlenmeye başlamıştır. Çalışmanın dikkat çeken kısmı ise yapılacak olan çatışma analizinin; kinetik dünyada yaşanan bir analiz değil, siber uzayda meydana gelen bir çatışma olmasıdır. "Çatışma analizi" kavramının bile hem uluslararası ilişkiler hem de hukuk alanlarında birçok kavrama göre yeni

bir kavram olduğu düşünüldüğünde, "siber çatışma analizi" kavramının çok daha yeni bir kavram olduğu dikkat çekmektedir.

"Çatışma", "çatışma analizi" ve "çatışma yönetimi" kavramlarının birçok farklı tanımı vardır. Özellikle "çatışma" kavramının tanımı konusunda birçok farklı görüş vardır. "Siber çatışma" kavramı ise çok daha yeni bir kavramdır. Bu durumun nedenlerinin başında, "çatışma" kavramının uluslararası ilişkiler dışında birçok farklı disiplinde de kullanılan bir kavram olması gelmektedir. "Çatışma" kavramı ile ilgili Peter Wallensteen; mevcut kısıtlı kaynaklar kümesini aynı anda sahiplenmek için en az iki aktörün mücadeleye girdiği toplumsal bir durum şeklinde bir tanım yapmıştır (Wallensteen, 2002). Wallensteen, "çatışma yönetimi" kavramının ortaya çıkışını birçok düşünürün aksine Soğuk Savaş sonrasına dayandırdığı için, bu konudaki görüşleri dikkat çekmektedir.

Nezir Akyeşilmen'in "çatışma" tanımı ise şu şekildedir: çatışma; siyasi, ekonomik, kültürel, inanç ve felsefi bir hedefe ulaşmak için karşılıklı bağımlı olan örgütlü taraflarca kişi, grup, millet ve devletler gibi içsel ve çevresel potansiyel, algısal ya da gerçek tehdit ya da engellere karşı verilen yoğunluk derecesi ve şiddet düzeyi farklılık arz eden gizli ya da açık bir mücadeleden oluşan geçici bir süreçtir (Akyeşilmen, 2014).

Yukarıda verilen "çatışma" tanımlarının tamamı kinetik çatışmalar için verilmiştir. "Siber çatışma" kavramı ise siber uzayda meydana gelen bir çatışmayı kapsar ve daha farklı tanımlamalara ihtiyaç duyar.

Siber çatışmalar, kinetik çatışmalara göre çok daha yeni bir çatışma çeşididir. Teknoloji temelli hizmet sağlayıcılarına yapılan saldırılar siber saldırılardır. Siber çatışmaların doğasına bakıldığında, hem sosyal hem de ekonomik boyutunun olduğu görülmektedir. Siber çatışmalar, günümüz uluslararası sisteminin önemli bir parçası haline gelmiştir ve uluslararası ilişkilerde hesaba mutlaka katılması gereken bir olgu haline gelmiştir. Günümüzde artık tüm devletler, teknolojik gelişmelerin de ilerlemesiyle, rutin işlerinin büyük bir bölümünü dijital ortamlarda halletmektedir. Bu durum da devletleri siber platformlarda önlem almaya iterken, siber çatışmaları da beraberinde getirmektedir.

Dünyanın ekonomisi ve uluslararası güvenliği internete bağlı bir hale gelmiştir. Uluslararası rekabetler ve ihtilaflar, casusluk ve sabotaj gibi siber uzayda güvenliği sarsacak zorluklar

getirmiştir. Bununla birlikte, bilgisayar sistemlerinde sürekli yeni açıklar keşfedilmektedir. Bir birey, grup veya ulus, rakip bir bilgisayar sistemindeki güvenlik açıklarına erişebiliyorsa, kapasitesini hemen kullanıp kullanmama veya daha elverişli bir zamanı beklemenin ikileminde kalmaktadır (Axelrod ve Illiev, 2014).

Günümüzde siber çatışmalar ve çatışma çeşitlerini anlama yüzeysel olmaya devam etmektedir. Mevcut araştırmalar, siber çatışmalara bütünsel bir yaklaşım sunamamaktadır ve siber çatışmaların doğası hala büyük ölçüde anlaşılamamaktadır. Bugün, siber çatışmaların ne kadar tehlikeli olduğu ve hangi sonuçlar ve tehditleri getirdiği bilinmemektedir (Kosenkov, 2016). Bununla birlikte, gelecekte siber çatışmaları sınıflandırmanın daha da zorlaşacağı varsayılmaktadır. Siber opreasyonlar, tipik olarak silahlı çatışma ile ilgili fiziksel hasara neden olmadan, geniş toplumsal ve ekonomik bozulmaya neden olma potansiyeline sahiptir. Aynı zamanda doğaları gereği sınır ötesidirler, bu nedenle coğrafi nedenlere bağlı sınıflandırma yaklaşımları siber çatışmalarda çok da geçerli değildir. Ayrıca kitlesel saldırılar, tek bir kişi veya tamamen çevrimiçi olarak düzenlenen bir grup tarafından başlatılabilir (Schmitt, 2012).

Siber; ana karelerin, tellerin, sabit disklerin ve ağların sınırlarını tanımladığından beri fiziksel unsurlara sahiptir. Bu nedenle, siber çatışmanın yaşandığı savaş alanı belli sınırlar boyunca tanımlanmaktadır. Siber, bilinmeyen sınırların olan bir kavram değildir; fiziksel katman ve sözdizimsel katman arasında bölünür. Bilgi saklama kabiliyeti arttıkça, siber alan da artış göstermektedir. Siber güvenlik ise bir devletin siber alanda savunma ve saldırıma yetenekleri için kullanılan terimdir. Eğer bir ülke interneti ve bilgi akışını kendi sınırlarının içine girip çıkmasını engelleyebiliyorsa, o devletin güçlü siber savunmalara sahip olduğu varsayılabilir. Bu devletlerden biri de Amerika Birleşik Devletleri'dir. ABD'ye siber bir saldırıda bulunacak saldırganlar, iki kez düşünmektedirler. Bunun nedenlerinin başında da misilleme ihtimali bulunmaktadır (Valeriano ve Maness, 2014).

2.ABD'de 2016 Seçimleri

22 Temmuz 2016 Cuma günü, WikiLeaks'e Demokratik Ulusal Komite'den çalınan yaklaşık 20.000 e-posta gönderilmiştir. Bu e-postalar, Amerikan medya kuruluşlarında adaylardan Hillary Clinton lehine seçim sonuç tahminlerinin farklı aktarıldığını göstermiştir. Sızıntılar sonucundan Demokratik Ulusal Komite'nin başkanı Debbie Wasserman Schultz istifa

etmiştir. Bu gelişme, Demokrat Parti tarafından büyük çapta bir kriz olarak algılanmamış olsa da sonradan ortaya çıkacak farklı gelişmelerin başlangıcı olarak görülmüştür (Inkster, 2016).

Bu skandalı takip eden bir diğer olay, Hillary Clinton'ın seçim kampanyasının başındaki isim olan John Podesta'nın ve eski ABD dışişleri bakanı Colin Powell'ın e-postalarının sızdırılmasıdır. Bu gelişmelerin ardından dönemin Amerika Birleşik Devletleri başkanı Barack Obama, 2008'den bu yana Amerika'da yapılmış tüm başkanlık seçimlerinin incelenmesini istemiştir. FBI'ın soruşturma açmasını isteyen Obama, sürecin sonunda 35 Rus diplomatı sınır dışı etmiştir (Darıcılı, 2017).

Bu gelişmelerin ardında Demokratik Ulusal Komite daha önce de bir sızıntı olup olmadığında şüphe duymaya başlamış ve konuyla ilgili araştırma yapması için CrowdStrike isimli bir siber güvenlik şirketinden yardım istemiştir. Yaptığı araştırmalardan sonra CrowdStrike komiteye iki ayrı tarihte izinsiz giriş yapıldığını tespit etmiştir. Bu gelişme üzerine FBI konuyla ilgili soruşturma başlatma kararı almıştır. 22 Temmuz olayından iki gün sonra Hillary Clinton'ın kampanya yöneticisi Robby Mook, e-postaların rakipleri Cumhuriyetçi Parti'nin adayı Donald Trump'a yardım amacıyla Ruslar tarafından sızdırıldığını iddia etmiştir. Bu iddia, hem Trump hem de Rusya cephesi tarafından reddedilmiştir. Ancak Donald Trump, ele geçirilen dosyaların tamamının halkla paylaşılması gerektiğini söylemiştir (Inkster, 2016).

Hillary Clinton 28 Temmuz 2016'da Demokrat Parti'nin adayı olarak gösterildiğinde, birçok insan tarafından çok da benimsenmiş bir siyasi figür değildi. Soğuk ve robotik tavırları dikkat çekiciydi ve basınla çok da iyi anlaşamıyordu. Kampanyasını başlattıktan sonra adaylığa giden yol kendisi için çok da çetin geçmedi. Belki Bernie Sanders gibi sol oylara talip bir rakip demokrat oyları için bir problem olabilirdi. Ancak; e-posta skandalı ve sonrasında FBI soruşturmasını engellemeye varan tutumu kendisini seçmenin gözünde oldukça antipatikleştirdi (Savoy, 2017).

Rusya'nın seçimlere müdahalesini analiz etmenin en açık yolu, yalnızca belirli bilgisayar ağlarına ve beliri e-posta hesaplarına yapılmış olan yasadışı ve yetkisiz girişimlere odaklanmaktır. 2016 seçimlerinin hikayesi sadece siber güvenlik ve siber çatışmalar için değil; aynı zamanda kampanya hazırlamadan, uluslararası hukuk kurallarına kadar uzanan geniş bir yelpazedir. Ancak bu çalışma bu krizin bir siber çatışmaya dönüşmesi durumu üzerine odaklanmaktadur.

2016 seçimlerinde, siber alanın her köşesinden çevrimiçi kampanyaya ilişkin iletişim patlaması yaşanmıştır. Sahte haberler, sosyal medya botları, her türlü platformda olabilecek otomatik hesaplar ve Amerika Birleşik Devletleri içinden ve dışından propaganda kullanımlarının yanı sıra kazanan kampanyanın yeni medyasının somut adımlarının, başkanlığa nasıl etkilerinin olduğu bir bütünün parçalarıdır (Persily, 2017). 2016 ABD seçimlerine müdahale konusunda hem Hillary Clinton hem de Donald Trump mağdur olduklarını iddia etmişlerdir.

ABD seçimlerine müdahale konusunda elde olan deliller Kremlin'i bu aktiviteden sorumlu tutmak için yeterli değildir. Buna rağmen, birçok kaynak bu iddiayı destekler niteliktedir. FBI, CIA ve NSA Rusya'nın seçimleri etkilemek karmaşık bir kampanya yürüttüğüne inandıklarını ancak bunun yalnızca bir varsayım olduğunu belirtmişlerdir. Department of Homeland Security, haziran ayında Kremlin'e bağlı kişilerin 20'den fazla eyalette seçimle ilgili bilgisayarlar sistemlerine sızmaya çalıştıklarını tespit ettiklerini söylemiştir. Şubat 2018'de ise özel yetkili savcı Robert Mueller ve yanına aldığı birçok federal savcı, 2016 başkanlık seçimleri de dahil olmak üzere Amerika Birleşik Devletleri'nin siyasi sistemine müdahale etme çabalarıyla ilişkili suçlardan bazı Rus şirketlerini suçlamışlardır. ABD'li hukuk insanları, Rus hackerlarının aslında hem Cumhuriyetçi Parti'nin hem de Demokrat Parti'nin sistemlerine sızıldığı inancındalar. 2016'da Demokrat Parti'den çalınan e-postalardan çok önce sisteme sızıldığına inanılmaktadır. Ancak ortada sorulan bir başka soru var: bu müdahaleler, Kremlin bağıyla yapılmış olsun olmasın, Amerika Birleşik Devletleri'nde 2016 yılında yapılan başkanlık seçiminin sonucunu ne ölçüde etkiledi (Masters, 2018)?

Rusya'nın müdahaleleri yalnızca yasa dışı siber faaliyetlerden oluşmamaktadır. Müdahale içersine dahil edilen ve soruşturma kapsamında değerlendirilen aktivitelerden biri de devlet destekli olarak sosyal medya üzerinden trollerin açık faaliyetlerdir. 2017'de yayınlanan Amerikan istihbarat raporunda, Rusya Federasyonu'na bağlı olan Sputnik ve Russia Today gibi kuruluşların bu işin içinde olduğu iddia edilmiştir. Kremlin'in birçok troll kiraladığı ve Facebook, YouTube ve Twitter gibi sitelerden sahte haberlerle manipülasyon yaptığı da iddialar arasında bulunmaktadır (Masters, 2018).

ABD'li yetkililer, yapılan iki saldırının da Rusya kaynaklı olduğuna emin olduklarını ancak şaşırtıcı şekilde yapılan işlemin bağımsız olduğunu söylemektedirler. Konuyla ilgili Vladimir Putin de müdahalenin resmi bir şekilde yapılmış olmasının mğmkün olmadığını, ancak vatansever bazı Rus hackerların yapmış olabileceğini, bu durumun da resmi olarak Kremlin'e bağlanamayacağını söylemiştir. Peki neden asıl hedef olarak Hillary Clinton ve Demokrat Parti seçildi? Aslında bu sorunun cevabı için Hillary Clinton'ın dışişleri bakanlığı döneminde Rusya'ya karşı uyguladığı diplomasiye bakmakta fayda var. Clinton'ın dışişleri bakanlığı döneminde uyguladığı politika sonucu Washington ve Moskova arasındaki ilişkiler neredeyse sıfırlanmıştı. Aynı zamanda 2011'de Putin'in üçüncü kez başkanlığa aday olmasının ardından kendisini protesto etmek için sokağa dökülen göstericileri Clinton'ın finanse ettiği iddia edilmektedir. Peki Donald Trump'ın seçilmesiyle Moskova'nın nasıl bir çıkarı olabilir? Bu sorunun net bir cevabı olmamakla birlikte, Kremlin'in seçimlere müdahale ederkenki asıl amacının da Donald Trump'ı başkan seçtirmek ya da Hillary Clinton'a seçimi kaybettirmek olmadığı düşünülebilir. Belki de Putin yalnızca seçimleri baltalamak ve bir kaos yaratarak Rusya'nın bu tarz bir kudretinin olduğunu göstermek istemiştir. Amerikan istihbaratı, Rus hackerların Cumhuriyetçi Ulusal Komiteyi de hacklediğini, ancak herhangi bir belgeyi yayınlamadıklarını da belirtmiştir (Harding, 2016).

2.Rusya'nın Siber Stratejileri: Tarih, Eylem ve Amaç

2000 yılında, 2. Çeçen Savaşı olarak bilinen askeri kampanya öncesinde, Kremlin için başarısızlıkla sonuçlanmış olan 1. Çeçen Savaşı'nın kaybedilmesinin nedenleri öğrenilmek istenmiştir. Rusya başkanı Vladimir Putin, 1. Çeçen Savaşı'nın kaybedilmesinin sorumlusu olarak Rusya'daki bağımsız gazetecileri suçlamıştır. 1990'ların sonunda liberal Rus gazetecilerinin ve yabancı meslektaşlarının, Rusya'nın savaş çabalarını baltaladığını ileri sürmüş ve bu durumun savaşın kaybedilmesindeki bir numaralı etken olduğunu dile getirmiştir. İkinci savaşın kazanılması için ise bağımsız bilgi kaynaklarının daha sıkı kontrol altına alınması gerektiğini iddia etmiştir. Bu durum, Rusya'nın bilginin doğasına bakışını değiştirip, bilginin bir silah haline getirilmesine neden olmuştur. Daha sonradan bu "sorun" her seviyede ele alınmıştır ve terörle mücadele eylemlerinin medya kapsamına ilişkin kuralları sıkılaştırılmıştır. Kremlin'in internet söylemleri de bu durumdan etkilenmiş ve "bilgi güvenliği", "bilgi savaşları" gibi terimler yaygınlaşmıştır. Rusya Federal Güvenlik Servisi'nin Bilgisayar ve Bilgi Güvenliği Müdürlüğü (UKIB) olarak bilinen Siber İstihbarat Departmanı,

2002 yılında Bilgi Güvenliği Merkezi (ISC) olarak olarak değiştirildi (Soldatov ve Borogan, 2018).

Siber saldırılar ise yeni bir yaklaşım halinde gelişmiştir. Kremlin; eylemciler, suç grupları ve meşruluğu soru işareti olan siber teknoloji firmalarına kaynak sağlamaya başlanıştır. Daha sonrasında ise makul bir inkar edilebilirlik yaratmak ve itibarını da zedelememek açısından bazı önlemler alınmıştır. Hatta bazen farklı gizli servislerle de temas halinde olumuştur. Rusya'daki muhalefet liderlerinin gizli videolarına ve telefon konuşmalarına sızılması olayında bu durum ayyuka çıkmıştır. Ancak birçok farklı olayda, Kremlin yetkilileri kendi izlerini ustalıkla gizlemeyi başarabilmişlerdir. Siber çatışmaların en önemli özelliklerinden biri de kuşkusuz budur. Çatışma taraflarıkağıt üzerinde belirgin olsa da ispatlamak neredeyse imkansızdır. Rusya da izlerini örterek bu durumu daha da sert hale getirmektedir. Bunun en önemli örneklerinden biri 2007 yılında yapılan Estonya saldırısı olmuştur. Rus hackerlar Estonya parlamentosu, bankaları, bakanlıkları ve yayıncı kuruluşlarına sistemaktik bir saldırı gerçekleştirmişlerdir. Bu saldırılar sonrası Estonya dış işleri bakanı Urmas Paet, bu saldırıların arkasında sıradan Rus hackerlarının değil, doğrudan Kremlin'in olduğunu iddia etmiştir. Ancak, Estonya, bu iddiayı destekleyecek yeterli kanıtı bulamamıştır (Soldatov ve Borogan, 2018). Daha sonra, mayıs 2009'da Rusya'daki Naşi Hareketi'ne bağlı olan Konstantin Goloskokov Estonya saldırılarının ardında Kremlin'in olduğunu Financial Times'a itiraf etmiştir ("Kremlin Kids: We Launched The Estonian Cyber War", 2009).

Estonya müdahalesi ve Goloskokov'un itirafları, Kremlin merkezli siber saldırıları iddialarının çoğalmasına neden olmuştur. Siber çatışmaların bir diğer problemlerinden biri de kuşkusuz bilgi kirliliği ve kanıtlamakta zorlanılan iddiaların devamlı ortaya atılmasıdır. Geriye dönüp bakıldığında, Estonya saldırısının, Kremlin'in müdahalelerinin bir başlangıcı olduğu düşünülebilir. Kremlin kaynaklı olduğu iddia edilen siber saldırıların ortak noktalarına bakıldığında, saldırıların genellikle NATO ülkelerine yapıldığı görülmektedir. Burada da önemli nokta, seçimlerde Rusya'nın lehine dış politika izleyecek adayları ön plana çıkartmak olarak görülmüştür. Ancak büyük resme bakıldığında, Kremlin'in yalnızca NATO ülkeleri ya da batı bloğuna saldırmadığı görülmektedir. 2008 Gürcistan müdahalesi de bunun bir göstergesidir.

2008 yılında Rus ordusunun Gürcistan'ı işgal etmesinin ardından, bu askeri kampanyaya birçok farklı siber saldırı da eşlik etmiştir. Bu müdahalenin en önemli özelliği, büyük bir kara

operasyonuyla paralel bir şekilde sürdürülen bir siber saldırı yürütülmüş olmasıdır. Tıpkı diğer birçok siber saldırı gibi, bu saldırının da Kremlin ile doğrudan bir ilişkisi tespit edilememiştir; fakat, bu saldırıların psikolojik etkisi oldukça büyük olmuştur. Konuyla ilgili farklı siber güvenlik şirketleri, Gürcistan'a yapılan siber saldırıların iki aşamalı olduğunu tespit etmişlerdir. İlk aşama, 7 ağustosta Rus hackerların Gürcü haber ajanslarını hedef almasıyla başlamıştır. Bu saldırılar "hizmet reddir" (DDoS) saldırılarıdır. İkinci aşamada ise Gürcü haber sitelerine saldırılar devam ederken, saldırı listesi genişletilmiş ve finansal kurumlar, işletmeler, eğitim kurumları ve BBC ile CNN gibi batı medyalarına saldırılar yapılmıştır. Bu saldırılar ise DDoS saldırılarıyla sınırlı kalmamış, siteleri bozmaya kadar ilerlemiştir (Shakarian, 2011).

Rusya'nın Estonya ve Gürcistan müdahaleleri, siber saldırı konusunda ne kadar başarılı olduğunu gözler önüne sermektedir. Bu gelişmeler, Rusya'nın ve Rusya vatandaşlarının uluslararası kamuoyundaki algısını da değiştirmiştir. Rusya birden bire, işsiz süper-hacker diyarı ve siber suç merkezi olarak algılanmaya başlanmıştır. Burada Rus toplum yapısının durumu da oldukça önemlidir. Rus bilgisayar korsanları, işsiz olduktan sonra yasa dışı faaliyetlere zorlanan yüksek eğitimli ve yetenekli insanlardır. Amerikalı uzmanlar da Rusya'daki siber suçların yaşanma nedenleri olarak, kendileri için çok az iş olduğu için, donanımlı Rus vatandaşlarının suça yöneldiğini iddia etmektedirler. Tüm bu durumlar neticesinde, Rusya sürekli belli karmaşalardan sorumlu tutulan bir süper-hacker ülkesi olarak görülmeye başlanmıştır (Karatgozianni, 2010).

Rusya kökenli siber saldırıların Kremlin ile olan bağı daima sorgulanmıştır. Ancak Rusya kökenli saldırıların Kremlin kökenli olup olmadığını anlamak bir başka problemdir. Rusya'daki en önemli hacker grubunun adı Fancy Bear'dır. Fancy Bear grubu; APT28, Pawn Storm, Sofacy Group, Sednit, Tsar Team ve STRONTIUM isimleriyle de aktiviteler gerçekleştirmiştir. Fancy Bear'ın Kremlin ve Rus istihbaratıyla bağlantısını kurulması ise CrowdStrike isimli bir Amerikan siber güvenlik şirketi tarafından yapılmıştır. Amerika'da yapılan 2016 seçimlerindeki Rus müdahalesinin ardında da Fancy Bear ismi bulunmaktadır ("Cozy Bear and Fancy Bear: Did Russians Hack Democratic Party And If So, Why?",

Fancy Bear'ın önemli saldırılarından biri de Fransız TV5Monde'ye yapılan saldırılardır. Demokratik Ulusal Komite'den sızdırılan 20.000 e-postanın ise Fancy Bear tarafından değil; Cozy Bear isimli farklı bir Rus örgütü tarafından gerçekleştirildiği belirtilmiştir. Cozy Bear ve

Fancy Bear, görünürde birbirine rakip iki hacker örgüt olarak görülse de özellikle farklı devletlere yapılan saldırılarda her iki örgütün de amaçlarının aynı olduğu görülebilir. Cozy Bear ise Office Monkeys, CozyCar, The Dukes, Volexity, CozyDuke ve F-Secure gibi farklı isimlerle de aktivitelerde bulunmuştur. Cozy Bear örgütünün Demokratik Ulusal Komite'ye yaptığı müdahale öncesinde yaklaşık bir yıldır komitenin ağında beklediği görülmüştür.

Kremlin'in, Cozy Bear ve Fancy Bear isimli hack grupları aracılığıyla 2016 ABD seçimlerine müdahale ettiği iddiaları, Rus hükümeti tarafından kesin bir dille yalanlanmıştır. Kremlin'in dışişleri bakanlığı sözcüsü Mariya Zaharova, Demokrat Parti ve Hillary Clinton'ın yaşadığı yenilgiyi hazmedemediğini söylemiştir. Bu demeç, Demokrat Parti'nin Rusya, Donald Trump ve WikiLeaks'e karşı attığı hukuki adımlar sonucu verilmiştir ("Rus Dışişleri: Demokratlar Seçimlerde Aldıkları Yenilgiyi Haklı Çıkarmaya Çalışıyor", 2018). Demokrat Parti açtığı davada Rusya'yı "ekonomik casuslukla" suçlamış, Donald Trump, Trump'ın damadı Jared Kushner, Trump'ın seçim danışmanı Roger Stone ve WikiLeaks'in kurucusu Julian Assange'a milyonlarca dolarlık tazminat davası açmıştır ("Demokrat Parti Rusya, Trump'ın Seçim Ekibi ve WikiLeaks'e Dava Açtı", 2018).

WikiLeaks kurucusu Julian Assange ise seçimlere yapılan müdahalede Kremlin'in payı olmadığını gösteren kanıtlar olduğunu iddia etmiştir. İşin farklı bir boyutu da Demokrat Parti'nin, Trump'ın da kendilerini davet ettiği üzere, kendi e-postalarını inceletmemesi olayıdır. FBI direktörü James Comey, FBI'ın Demokratik Ulusal Komite'nin e-postalarına erişmek ve incelemek istediği ancak Demokrat Parti'nin buna izin vermediğini söylemiştir. FBI, komitenin e-postalarına farklı siber güvenlik şirketleri aracılığıyla erişim sağlayabilmiştir ("FBI: Demokratlardan Defalarca Bilgisayarlarına Ulaşma İzni İstedik, Kabul Edilmedi", 2017). Demokratik Ulusal Komite'nin bu tutumuna Donald Trump da sert bir tepki vermiştir. Trump; Demokratların e-postalarını FBI'a inceletmeden nasıl Rusya'nın bu işin arkasında olduğu sonucuna varıldığını soran tweetler atmıştır ("Trump'tan 'Rusya'nın Hacklediği Bilgisayarlarını' İnceletmeyen Demokratlara Tepki", 2017).

Sonuç

Siber çatışmalar günümüzde oldukça sık karşılaşılan bir çatışma çeşidi haline gelmiştir. Hatta o kadardır ki nerdeyse her an birçok farklı ülkedeki kurumların altyapılarına siber saldırılar gerçekleşmektedir. Bu saldırılar, bilginin artık tamamen siber ortamdan aktarılan bir olgu

olduğu günümüzde kaçınılmaz durumdadır. Siber uzay, gelenekselleşmiş güvenlik önlemlerini ve birçok varsayımı da beraberinde değiştirmiştir. Artık hiçbir ülke "saldırılamaz" ya da "saldırmaz" değildir. Siber kullanımı ve kapasitesi arttıkça, ülkelerin bu konudaki zaafları da artış göstermektedir.

Çalışmada da değinildiği üzere, siber çatışmaların en büyük sorunu, saldırgan tarafı herhangi bir resmi kuruluşla bağlantılı kılamamaktır. Saldırıları yapan hackerların milliyeti, saldırıların o ülke tarafından yapıldığı anlamına gelmemektedir. 2016 Amerika Birleşik Devletleri başkanlık seçimlerinde yaşanan olayda da aynı durum geçerlidir. İlk bakışta saldırıyı düzenleyen Cozy Bear ve diğer örgüt Fancy Bear ile Kremlin arasında bir bağ olduğu net bir şekilde ortada gibi gözükse de derinlemesine araştırıldığında bu örgütleri Kremlin'e ve Rus istihbaratına bağlayacak yeterlilikte deliller bulunamamaktadır. Ancak şu bir gerçektir ki Rus bir hacker grubu olan Cozy Bear örgütü Amerika'daki 2016 seçimleri öncesi sızdırdığı 20.000 e-postayla seçimlerin sonucuna etki etmişlerdir.

Demokrat Parti'nin ve Hillary Clinton'ın bu konuda net tavır takınamamaları da olayın bir başka boyutudur. FBI'ın Demokratik Ulusal Komite'nin e-postalarını incelemesini reddeden demokratlar, ironik bir şekilde belki de olayın çözülmesinin önündeki en büyük engel konumunda görülmektedirler. 2016 seçimlerinin galibi Donald Trump ise bir müdahale olmuş olma ihtimalinin bulunduğu ancak bunu Kremlin'e bağlamanın paranoyaklık ve hazımsızlık olduğu görüşündedir. Vladimir Putin ise Kremlin'in seçimlere müdahil olduğu iddiasını tamamen reddetmiştir. Netice itibariyle, siber çatışmalar ve müdahaleler, demokrasinin beşiği olan Amerika Birleşik Devletleri'nde bile demokratik seçimlerin yönünü etkilemiştir. Bu durum, siber güvenlik konusunda paranoyakça önlemler alan ülkelerin, bu konuda ne kadar haklı olduğunun göstergesidir. Tüm dünyanın takip ettiği, sonucunun tüm dünyayı etkilediği bir seçimi bile etkileyebilen siber ataklar, uluslararası ilişkilerin artık çok daha farklı boyutlarda işleyen bir disiplin olma yolunda ilerlediğinin en önemli göstegesidir.

Kaynakça

Kremlin kids: We launched the Estonian cyber war. (2009, March 11). *Wired.*

Akyeşilmen, N. (2014). Çatışma yöntemi: Kavramsal ve kuramsal bir analiz. Akyeşilmen (Eds.), *Barışı Konuşmak: Teori ve Pratikte Çatışma Yönetimi* (pp. 18-45). Ankara: ODTÜ Yayıncılık

Axelrod, R. & Iliev, R. (2013). Timing of cyber conflict. *National Academy of Sciences,* 111, 1298-1303. doi: 10.1073/pnas.1322638111

Kosenkov, A. (2016). Cyber conflict as a new global threat. *Future Internet,* 8, 2-9. doi: 10.3390/fi8030045

Schmitt, M. (2012). Classification of cyber conflict. *Journal of Conflict & Security Law,* 17, 245-260. Doi: 10.1093/jcsl/krs018

Valeriano, B. & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research*, 51, 347-360. Doi: 10.1177/0022343313518940

Inkster, N. (2016). Information warfare and the US presidential election. *Survival: Global Politics and Strategy.* 58, 23-32. Doi: 10.1080/00396338.2016.1231527

Persily, N. (2017). The 2016 U.S. election: Can democracy survive the internet? *Journal of Democracy,* 28, 63-76. Doi: 10.1353/jod.2017.0025

Soldatov, A. & Borogan I. (2018). Russia's approach to cyber: the best defence is a good offence. Popescu & Secrieru (Eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies* (pp. 15-25). Paris: Instute for Security Studies

Shakarian, C. P. (2011). The 2008 Russian cyber campaign against Georgia. *Military Review.* https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20111231_art013.pdf

Karatzogianni, A. (2010). Blame it on the Russians: tracking the portreyal of Russians during cyber conflict incidents. *Digital Icons: Studies in Russian, Eurasian and Central European New Media,* 4, 127-150. https://www.researchgate.net/publication/259850767_Blame_it_on_the_Russians_Tracking_the_Portrayal_of_Russians_During_Cyber_Conflict_Incidents

Rus Dışişleri: Demokratlar Seçimlerde Aldıkları Yenilgiyi Haklı Çıkarmaya Çalışıyor. (2018, 21 Nisan). *Sputnik Türkiye*

Demokrat Parti Rusya, Trump'ın Seçim Ekibi ve WikiLeaks'e Dava Açtı. (2018, 20 Nisan). *Sputnik Türkiye*

FBI: Demokratlardan Defalarca Bilgisayarlarına Ulaşma İzni İstedik, Kabul Edilmedi. (2017, 10 Ocak). *Sputnik Türkiye*

Trump'tan 'Rusya'nın Hacklediği Bilgisayarlarını' İnceletmeyen Demokratlara Tepki. (2017, 6 Ocak). *Sputnik Türkiye*

https://www.theguardian.com/technology/2016/jul/29/cozy-bear-fancy-bear-russia-hack-dnc

Darıcılı, A. B. (2017). Demokrat parti hack skandalı bağlamında ABD ve RF'nin siber güvenlik stratejilerinin analizi. *Ulisa: Uluslararası Çalışmalar Dergisi* (pp. 1-24), https://dergipark.org.tr/ulisa/issue/30947/335296

Savoy, J. (2017). Trump's and Clinton's style and rhetoric during the 2016 presidential election. *Journal Of Quantitative Linguistics.* Doi: 10.1080/09296174.2017.1349358

Masters, J. (2018), *Russia, Trump and the 2016 U.S. Elections,* Şubat 26, 2018, https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election

Harding, L. (2016). *What we know about Russia's interference in the US elections,* Aralık 16, 2016, https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election