İSTANBUL TOPKAPI ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLERDE SİBER SALDIRILARIN ARAÇ OLARAK KULLANILMASI: RUSYA KAYNAKLI SİBER SALDIRILAR ÖRNEĞİ

YÜKSEK LİSANS TEZİ

CANFİDAN KABAKCI

Güvenlik Bilimleri Anabilim Dalı
Güvenlik Bilimleri ve Uygulamaları Bilim Dalı

OCAK, 2023

İSTANBUL TOPKAPI ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLERDE SİBER SALDIRILARIN ARAÇ OLARAK KULLANILMASI: RUSYA KAYNAKLI SİBER SALDIRILAR ÖRNEĞİ

YÜKSEK LİSANS TEZİ

Canfidan KABAKCI
21220701010

Güvenlik Bilimleri Anabilim Dalı
Güvenlik Bilimleri ve Uygulamaları Bilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Gökhan AK

OCAK, 2023

KABUL VE ONAY

İSTANBUL TOPKAPI ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

…./…./2023

YÜKSEK LİSANS TEZ ONAY FORMU

Güvenlik Bilimleri Anabilim Dalı, Güvenlik Bilimleri Tezli Yüksek Lisans Programı Programı 21220701010 numaralı öğrencisi **Canfidan KABAKCI'nın "ULUSLARARASI İLİŞKİLERDE SİBER SALDIRILARIN ARAÇ OLARAK KULLANILMASI: RUSYA KAYNAKLI SİBER SALDIRILAR ÖRNEĞİ"** konulu Yüksek Lisans tezi Enstitümüz Yönetim Kurulunun 26/12/2022 tarihli ve 2022/30 sayılı Yönetim Kurulu kararıyla oluşturulan jüri tarafından oybirliği/oyçokluğu ile 20.01.2023 tarihinde kabul edilmiştir.

	Unvan	Adı Soyadı	Üniversite	İmza
		ASIL ÜYELER		
Danışman	Dr. Öğr. Üyesi	Gökhan AK	İstanbul Topkapı Üniversitesi	
1. Üye	Dr. Öğr. Üyesi	Suat DÖNMEZ	İstanbul Topkapı Üniversitesi	
2. Üye	Prof. Dr.	O. Can ÜNVER	İstinye Üniversitesi	
		YEDEK ÜYE		
1. Üye	Dr. Öğr. Üyesi	Z.Banu DALAMAN	İstanbul Topkapı Üniversitesi	
2. Üye	Dr. Öğr. Üyesi	Ahmet GÖRGEN	İzmir Demokrasi Üniversitesi	

ONAY
Prof. Dr. Özlem KUNDAY
Enstitü Müdürü

(*) Oybirliği/Oyçokluğu hâli yazı ile yazılacaktır.
(**) Kabul / Ret veya Düzeltme kararı hâli yazı ile yazılacaktır.

AKADEMİK DÜRÜSTLÜK BEYANI

Yüksek lisans tezi olarak sunduğum "Uluslararası İlişkilerde Siber Saldırıların Araç Olarak Kullanılması: Rusya Kaynaklı Siber Saldırılar Örneği" başlıklı çalışmanın, bilimsel, ahlak ve geleneklere uygun olarak tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları, her yerde atıf yapıldığını belirtir ve onurumla doğrularım.

01/01/2023
Canfidan KABAKCI

TEŞEKKÜR

Tez çalışmamın planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmamı bilimsel temeller ışığında şekillendiren Sayın Hocam Dr. Öğr. Üyesi Gökhan AK'a tüm sabır, destek ve hoşgörüsünden ötürü çok teşekkür ederim. Her biri çok değerli ve çok saygın olan; bölümüzün kurucusu Sayın Prof. Dr. Celalettin YAVUZ, bölüm başkanımız Sayın Dr. Öğr. Üyesi Suat DÖNMEZ, bölüm hocalarımız Sayın Prof. Dr. Erhan BÜTÜN, Sayın Prof. Dr. Alper ERTÜRK, Sayın Dr. Z. Banu DALAMAN, Sayın Dr. Hacı Ali DURU, Sayın Doç Dr. Nesrin DUMAN, Sayın Dr. Öğr. Üyesi Ahmet GÖRGEN ve tabi ki telkinleriyle ve söylemleriyle sürekli beni cesaretlendiren Sayın Dr. Öğr. Üyesi Tayfun GÜVEN, Sayın Muhammet ÖZCAN, Sayın Mert TÜRKMEN, Sayın Merve Müge ŞENGÜL BEKTAŞ hocalarıma teşekkürü borç bilirim. Stresli ve bir o kadar da keyifli olan bu süreçte birlikte yol aldığımız değerli arkadaşlarım Medine KINIK ve Neriman KORKMAZ'a ayrıca teşekkür ederim. Çalışmam süresince her zaman manevi desteklerini hissettiğim kıymetli babam Feramuz KABAKCI, annem Nurgül KABAKCI, kardeşlerim Nuh KABAKCI, Nurhan KABAKCI, Zeynep KAMALAK, Nuran BURÇOĞLU ve değerli eşi Murat BURÇOĞLU'na ve çocuklarım Berkay ASLAN ile Hasbi Bilgay ASLAN'a çok teşekkür ediyorum.

Canfidan KABAKCI

İÇİNDEKİLER

Sayfa

AKADEMİK DÜRÜSTLÜK BEYANI ..... **iii**
TEŞEKKÜR ..... **iv**
İÇİNDEKİLER ..... **v**
KISALTMALAR ..... **vii**
ŞEKİLLER LİSTESİ ..... **viii**
ÖZET ..... **ix**
ABSTRACT ..... **x**
1. GİRİŞ **1**
2. GENEL BİLGİLER VE LİTERATÜR ÇALIŞMASI **10**
2.1. Araştırmanın Konusu 10
2.2. Araştırmanın Sorunsalı 11
2.3. Araştırmanın Amacı 12
2.4. Araştırmanın Önemi 13
2.5. Araştırmanın Literatür Taraması 14
2.6. Araştırmanın Yöntemi 15
2.7. Araştırmanın Kapsamı ve Sınırlıkları 15
2.8. Araştırmanın Hipotezleri 15
2.9. Araştırmanın Veri Toplama Yöntemleri 16
3. SİBER SALDIRILAR-KAVRAMSAL ÇERÇEVE **17**
3.1. Siber Uzay 17
3.2. Siber Saldırılar 19
3.2.1. Bilgisayar korsanlığı 22
3.2.2. Zararlı yazılımlar 23
3.2.3. Gizli-arka kapılar 25
3.2.4. Kimlik avı (yemleme) 26
3.2.5. Scanning (tarama) yöntemi ve şifre kırıcılar 28
3.2.6. Servis dışı bırakma saldırıları 29
3.2.7. Sahte (fake)-istemdışı alınan (spam) 30
3.2.8. Klavye kaydediciler 31
3.2.9. Ip aldatması 32
3.2.10. SQL Injection (enjeksiyon) yöntemi 33
3.2.11. Siber casusluk ve istihbarat saldırıları 34
3.3. Siber Güvenlik 37
4. ULUSLARARASI İLİŞKİLERDE SİBER SALDIRILAR **43**
4.1. Siber Alanın Uluslararası İlişkilere Dahil Olması 43
4.2. Uluslararası Aktörler ve Siber Mücadeledeki Yerleri 46
4.2.1. Devletler 47
4.2.2. Siber ordular 49
4.3. Devlet Dışı Uluslararası Aktörler 51
4.3.1. Uluslararası illegal yapılanmalar 52

4.3.2. Manipülatif birimler ve söylemler 52
4.4. Siber Savaşçılar 53
4.5. Uluslararası İlişkiler Açısından Siber Güvenlik 54
4.6. Ülkelerin ve Uluslararası Toplulukların Siber Güvenlik Politikaları 56
4.6.1. NATO 56
4.6.2. Avrupa Birliği 58
4.6.3. ABD 61
4.6.4. İngiltere 64
5. RUSYA KAYNAKLI SİBER SALDIRILAR 68
5.1. Rusya Federasyonu'nun Siber Güvenlik Strateji Belgeleri 68
5.2. Rus Silahlı Kuvvetleri ile Rus İstihbarat Servislerinin Siber Kapasiteleri 70
5.3. RF'nin Siber Alanının Yapısal Özellikleri 74
5.4. Rusya Federasyonu Kaynaklı Olduğu İddia Edilen ve Enformasyon Savaşı Enstrümanları Kullanılarak Yürütülen Siber Saldırılar 76
5.4.1. Estonya'ya yönelik siber saldırılar 77
5.4.2. Gürcistan'a yönelik siber saldırılar 79
5.4.3. Litvanya'ya yönelik siber saldırılar 81
5.4.4. Kırgızistan'a yönelik siber saldırılar 81
5.4.5. Ukrayna'ya yönelik siber saldırılar 83
6. SONUÇ VE DEĞERLENDİRME 88
KAYNAKÇA 94
ÖZGEÇMİŞ 104

KISALTMALAR

AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
ARPA : Advanced Research Projects Agency
ARPANET : Advanced Research Projects Agency Network
BİT : Bilgi ve İletişim Teknolojileri
BM : Birleşmiş Milletler
BT : Bilgi Teknolojileri
CISA : Cybersecurity and Infrastructure Security Agency
CCDCoE : Cooperative Cyber Defence Center of Excellence
DoS : Denial-of-Service (Hizmet Reddi)
DDoS : Distributed Denial of Service (Dağıtılmış)
ENISA : European Network and Information Security Agency
FSB : Federalnaya Slujba Bezopasnosti
GRU : Glavnoye Razvedyvatel'noye Upravleniye
ICMP : Internet Control Message Protocol
IP : İnternet Protokolu
IPb : Iinformatsionnoye Protivoborstvo
NATO : North Atlantic Treaty Organization (Kuzey Atlantik Anlaşması Örgütü)
NCIA : NATO İletişim ve Bilgi Ajanslığı
RİS : Rus İstihbarat Servisleri
RF : Rusya Federasyonu
SORM : The System for Operative Investigative Activities
SSCB : Sovyet Sosyalist Cumhuriyetler Birliği
STK : Sivil Toplum Kuruluşu
US : United States

ŞEKİLLER LİSTESİ

Sayfa

Şekil 4.1: Web Tabanlı Saldırılarda Devletlerin Küresel Etkilenme Oranları 49

ÖZET

ULUSLARARASI İLİŞKİLERDE SİBER SALDIRILARIN ARAÇ OLARAK KULLANILMASI: RUSYA KAYNAKLI SİBER SALDIRILAR ÖRNEĞİ

Günümüzde "siber uzay"; siber strateji, siber güvenlik, siber savunma ve siber savaş gibi faaliyetleri kutsayan bir uzay tiyatrosu haline gelmiştir. Siber uzay, ilgili veya ilgili aktörlerin bir çıkar tarafından teşvik edildiği küresel arenaya benzetilen bir alandır. Böyle bir alandaki zorluk, düzeni uygulayacak merkezi bir otoritenin olmamasıdır. Nitekim yeni çatışma ve zorlama yöntemleri de 21. Yüzyılın çok yönlü ve çok aktörlü uluslararası sisteminde etkin tektonik değişimlere ve hatta gücün, kurumların ve devlet davranış normlarının yeniden yapılandırılmasına yol açabilir. Bu bağlamda, son 30-40 yıldır uluslararası ilişkilerde kimi devletlerin giderek daha fazla bel bağladığı dijital altyapıyı bozan veya yok eden zorlayıcı eylemler olarak nitelendirilebilecek siber uzay tabanlı siber saldırılar görülmektedir. Bu nevi zamansız, kuralsız ve sınırsız siber eylemler, devletler arası ilişkilerde yeni bir silah ve yaptırım aracı olma potansiyeline sahiptir. Bu çalışmanın amacı Rusya'nın siber saldırı stratejileri üzerinden uluslararası ilişkilerde siber saldırıların araçsallaştırılmasını incelemektir. Bu çalışma, siber uzayda artan insan etkileşiminin onu stratejik bir alan düzeyine yükselttiği ve dolayısıyla Uluslararası İlişkiler için teorik ve pratik zorluklar doğurduğu öncülüne dayanmaktadır. Çalışmanın giriş bölümü sonrasındaki birinci bölümünde genel bilgiler ve literatür çalışması hakkında bilgi sunulacak; ikinci bölümünde siber uzay, siber savaş ve siber saldırılarla ilgili kavramsal bir çerçeve sunulacak, üçüncü bölümde uluslararası ilişkilerde siber saldırıların araç haline dönüştürülmesi incelenecek, dördüncü bölümde ise Rusya kaynaklı siber saldırılar ve uluslararası ilişkilerde etkileri tartışılacaktır.

Anahtar Kelimeler: *siber uzay, siber saldırı, siber güvenlik, uluslararası ilişkiler, Rusya Federasyonu*

ABSTRACT

USE OF CYBER ATTACKS AS A TOOL IN INTERNATIONAL RELATIONS: THE CASE OF CYBER ATTACKS FROM RUSSIA

Today, “cyberspace” could be defined as a space theater that celebrates activities such as cyber strategy, cyber security, cyber defense and cyber warfare. Cyberspace is a space likened to the global arena in which interested or related actors are promoted by an interest. The challenge in such a field is the absence of a central authority to enforce order. As a matter of fact, new methods of conflict and coercion may also lead to effective tectonic changes and even restructuring of power, institutions and norms of state behavior in the multifaceted and multi-actor international system of the 21st century. In this context, cyber-space-based cyber attacks, which can be described as coercive actions that disrupt or destroy the digital infrastructure on which some states rely more and more in international relations, have been observed in the last 30-40 years. Such untimely, unregulated and unlimited cyber actions have the potential to be a new weapon and sanction tool in interstate relations. The aim of this study is to examine the instrumentalization of cyber attacks in international relations through Russia’s cyber attack strategies. This study is based on the premise that increased human interaction in cyberspace elevates it to the level of a strategic domain and thus poses theoretical and practical challenges for international relations. Following introduction part, in the first part of the study a general information and literature work will be presented; then, a conceptual framework about cyber space, cyber war and attacks will be presented; in the third part, the transformation of cyber attacks into a tool in international relations will be examined, and in the fourth part, cyber attacks from Russia and their effects on international relations will be discussed.

Keywords: *cyberspace, cyber attack, cyber security, international relations, Russian Federation*

1. GİRİŞ

Günümüzde uluslararası ilişkilerde bazı devletlerin gerek milli hedeflerine ulaşma yolunda gerekse üçüncü taraflarla olan her nevi sorun, ihtilaf ve uzlaşmazlıklarını kendi milli menfaatleri yönünde çözebilmeyi sağlamak üzere, en başta gelen asimetrik tehdit silahı olan terör dışında, bir siber uzay içerisinde gerçekleştirdikleri siber saldırı eylemlerini son 20-30 yıllık yakın geçmiş içerisinde asimetrik bir silah olarak kullanmaya başladıkları görülmektedir. Siber saldırı kaynaklı bu nevi asimetrik tehdit ve riskleri bünyesinde barındıran evren, aslında bilişim uzmanlarının bugün "siber uzay" olarak nitelendirdikleri bir sanal âlemdir. Bu noktada akla ilk gelen husus ise, uluslararası ilişkilere ve devletlere yönelik bu nevi siber tehdit ve risklerin, asimetrik bir siber savaşı içermesi, dolayısıyla bu savaşın zamansız, kuralsız ve sınırsız (diğer deyişle, limitsiz) olmasından doğan çok hayati özellikler barındırmasıdır. Bu nedenle, son 20-30 yıldır kimi devletlerin üçüncü taraflarla olan sorun ve ihtilaflarını asimetrik bir şekilde ve "suçlanmadan" çözebilmek için sınırı olmayan ve daha da kötüsü, hiçbir şekilde herhangi bir zamana ve kurala uymayan savaşı siber evrende asimetrik bir biçimde sürdürdüklerine şahit olunmuştur.

Söz konusu asimetrik risk ve tehditlerin içerisinde yeşerdiği, yaşadığı, yaşatıldığı ve zamansız, limitsiz ve kuralsızca, kimi zaman bilinçli, kimi zaman bilinçsiz olarak gerek iyi gerekse kötü her nevi amaç için kullanıldığı ve yararlanıldığı siber alem, sanal bir siber evrenin ana nüvesini teşkil etmektedir. Dolayısıyla, "siber uzay (cyber-space)" olarak da tanımlanabilecek bu siber evren; adeta bir piramit şeklinde, en tepede devletler ve uluslararası toplum, sonrasında ulusal ve uluslararası kurum, kuruluş ve örgütler, onun altında insan toplumları (ki bunlar siyasetçilerden akademisyenlere, iletişim uzmanlarından gazetecilere, sanatçılardan edebiyatçılara ve daha nice toplumsal aktörlere) ve bu piramidin en altından da bireyler, diğer deyişle vatandaşlar arasında, inanılmaz bir karşılıklı bağımlılık ve etkileşim içerisinde modern toplumsal entelektüel söylemi tetikleyecek ölçüde büyümüştür ve halen de yapay zekâ,

robotik teknolojiler, metaverseler (kurgusal evren) ve diğer sanal âlem uygulamaları ile sayesinde akıl almaz bir hızla büyümektedir. Bu nedenle, interneti su, hava ve yiyecek gibi doğanın armağanı kadar önemli bir meta haline getiren temel doğası gereği siber evren ile ilgili konuların, günümüzde ulusal, örgütsel ve bireysel tartışmaların çekirdeğini oluşturduğunu söylemek mümkündür (Quadri & Rasgaq, 2020).

Çağdaş dünyada internet üzerinden siber uzayın kullanımı, 1980'lerden bu yana her sosyal düzeyde insanlığa hayli faydalı olmuştur. Bu durum, modern bilimsel çağın doğal bir oluşum ve sonucudur; zira internetin ortaya çıkmasından önce, faks, telefon, telgraf, basılı belge ve mektuplar ve yüz yüze sohbet gibi somut, kablolu ve/ya fiziksel iletişim biçimleri baskın iletişim araçlarıydı. Ancak, bilgisayar ve bilişim sistemleri ile birlikte internetin çığır açan yeniliği, modern öncesi iletişim araçlarından bazılarını geçersiz kılmıştır. Özellikle internetin kullanıma girmesi, kablosuz iletişim, finans, ticaret, eğlence, medya gibi neredeyse tüm geleneksel sosyal yaşam norm ve uygulamalarını değiştirmiş ve günümüzde geldiğimiz nokta itibariyle, insanlığı, adeta iki ucu keskin bir kılıç olarak nitelendirebilecek bir duruma sokan "Metaverse (kurgusal evren)" ve "Yapay Zekâ" patlamasını tetiklemiştir (Hearn, 2009).

Siber uzayın övgüye değer ve kasvetli yönü hem dünyaya faydalı hem de aynı anda dünyaya meydan okuyan bir gelişme olması nedeniyle, ulusal politikada ve geleneksel forumlarda hayati bir yer tutan siber güvenlik, siber savunma ve siber savaş ve siber atak gibi benzeri kavramların gündeme gelmesini sağlamıştır. Çağdaş dünya, devletlerin bireysel ve toplu olarak siber uzayın yıkıcı kullanımını azaltmak için politikalar veya stratejiler oluşturduğu bir siber strateji tiyatrosu haline gelmiştir (Wilson, 2007).

İnternetin yaygınlaşması, savaşın da bazı yol, yöntem ve yönlerini dönüştürmüş; bilindik konvansiyonel savaşı siber bir evrene taşıyarak sanallaştırmış ve asimetrikleştirmiş; böylece, uluslararası siyasetin önemli olgularından biri olan savaşta ve onun içinde yaşandığı uluslararası arenada ilişkilerin, yeni usul, metod, düzen, teknik, mekanizma, enstrüman, silah ve

eçhizelerle oynandığı ve tartışıldığı, kısacası uluslararası ilişkilerde savaş kartlarının yeniden karılıp dağıtıldığı yepyeni bir alan yaratmıştır.

Nitekim 1990'ların ortalarında Libicki (1995) de, savaşın yeni yön ve yöntemlerinin ortaya çıktığını ve bunların, geleneksel yönlerle bütünleştiğini iddia etmiştir. Dolayısıyla bu noktada, eski SSCB'nin dağıldığı 1991'den bugüne değin gerek savaş olgusu gerekse savaşın konsept, tarz ve yöntemleri bağlamında, değişim geçirerek dönüşen hususların; komuta ve kontrol savaşı, istihbarat temelli savaş, elektronik savaş, psikolojik harp ve operasyonlar, bilgisayar korsanları (hackers) savaşı,[1] bilgi ekonomisi savaşı, kısacası "siber savaş" olarak adlandırılan yepyeni ve sanal, bu yüzden de asimetrik bir savaş tarzı olduğunu söylemek mümkündür. Nitekim teknoloji ve iletişimdeki ilerlemeler tarafından desteklenen yeni bilgi işlem tekniklerinin adı ne olursa olsun, değişen çevre, devletler, toplumlar ve ekonomiler için hem bir fayda hem de bir kırılganlık haline gelmiştir (Quadri & Rasgaq, 2020). Bu kırılganlıklar da uluslararası toplum için yeni risk ve tehditlerin ortaya çıkmasına yol açmış, devletler arası güç mücadelelerinde savaşın daha da asimetrik hale dönüşmesine neden olmuştur. Terör gibi en temel asimetrik silah yanında, son 30-40 yılda kimi devletlerin siber âlemi (siber uzayı) kullanan siber saldırılarla, hasım olarak gördükleri taraflara karşı ucuz, sınırsız, gizli ve zamansız yöntemlerle daha geniş çaplı ve yıkıcı sonuçları alabileceklerini keşfettikleri görülmüştür.

Bu çerçevede olmak üzere, günümüzde bu yeni asimetrik savaş türü ve onun yine o ölçüde asimetrik silahları, siyaset bilimi ve siyaset kuramı literatürüne; "siber savaş", "siber silah", "siber saldırı", "siber mücadele", "siber korsan", "siber casus", "siber yazılım", "siber istihbarat" gibi bir takım yeni kavramlar sokmuştur. Bu bağlamda, bu yeni kavramların önünde yer alan "siber" tabiri, bilgisayar cihazları ve internet ile bağlantılı fiziksel aktivitelerin tanımı için kullanılan bir önektir. Dolayısıyla, son 30-40 yılda bilişim sistemleri alt yapısında çalışan soyut ve geniş bir âlem olarak nitelenebilecek siber evrende, özellikle çok hızlı internet ve ağ altyapılı teknolojik gelişmelerin

[1] "Hacker" terimi, bilgisayar korsanı; "hacking", bilgisayar korsanlığı faaliyeti anlamına gelmektedir (Aktaş, 2020). "Hacktivism" ise, sosyal ve siyasi aktivism için, bilgisayar korsanlığı tekniklerini kullanma işidir (Ghernaouti-Hélie, 2013).

yaşandığı 21. yüzyılda sanal âlem tabanlı; siber ticaret, siber iletişim, siber güvenlik, siber strateji, siber savaş, siber eğlence ve siber suçlar, siber ekonomi gibi canlılar ile makineler arasındaki iletişim ilişkilerini içeren yepyeni "sibernetik" sektörlerin doğması ve bilgisayarlar, akıllı cep telefonları, tabletler, sanal gerçeklik gözlükleri vb. başta olmak üzere, ağ-tabanlı her tür bilişim/iletişim aygıtıyla ilgili sanal (siber) faaliyetlerin kullanımında büyük bir artış görülmüştür.

Ancak, bu tez çalışmasının sorunsalı ile ilgili olması hasebiyle, yukarıda sayılan yeni kavramlardan özellikle "siber eylem", diğer deyişle "siber saldırı" kavramları, bireylerden öte, özellikle devletler başta olmak üzere, her nevi uluslararası aktör için yeni tehdit, risk ve düşmanca niyet/hareket durumları yaratmış; dolayısıyla da yeni güvenlik mülahazaları ortaya çıkarmıştır. Zira siber saldırı silahları, Rusya Federasyonu, Çin, İran, Kuzey Kore gibi kimi otoriter ve liberal-demokratik olmayan rejimler tarafından yeni asimetrik saldırı yöntemleri olarak kullanılarak, uluslararası ilişkileri şekillendirmede bir araç olarak kullanılmaya başlanmıştır. Bu yüzden, siber saldırıları, yetkisiz kişi veya gruplar tarafından bir devletin, kurumun, kuruluşun ya da bireyin bilişsel veri tabanına stratejik bir sızma olarak nitelendirmek mümkündür. Özelllikle uluslararası ilişkilerde, münhasır bir siber saldırı, siyasi, askeri veya ekonomik olarak amaçlanıp güdülenebilir. Nitekim Kaspersky (2020), siber saldırıyı bir siber tehdit olarak sınıflandırmış; ayrıca bunun, siyasi amaçlı bilgi toplama olduğunu da vurgulamış ve savlamıştır. Merriam-Webster (2020) ise, siber saldırı kavramını, zarar vermek için bir bilgisayara veya bilgisayar sistemine yasa dışı erişim sağlama girişimi olarak tanımlamaktadır.

Siber evrenin özelliklerinden etkilenen unsurlar arasında; temel alan kuralları, gücün münhasır ve meşru sahibi olarak devlet ve hesap verebilirlik bulunmaktadır. Bunlar, 20. yüzyılda devletler arası ilişkilerde daha düzenli gözlemlenmeleri nedeniyle öne çıkmaktadır. Devlet aktörlerinin diğer ülkelere yönelik herhangi bir saldırısı, potansiyel olarak bilgi savaşının birçok yönünü içermektedir. Bilgi savaşını basit bilişim suçlarından veya bilgi güvenliğine yönelik eylemlerden ayıran ana etmen, saldırının arkasındaki güdü, yani motivasyondur. Saldırgan bilgi operasyonları, ulusal ve devlet kurumları

tarafından diğer ülkelere karşı kullanıldığında ister devlet, isterse devlet dışı hedefler olsun, tespit ve savunma operasyonları karmaşık olabilir ve bunlar, çoğu zaman hassas uluslararası ilişkileri etkileyebilir. Zira internet, uluslararası ilişkilerin hem resmi hem de gayri resmi düzeyde oynandığı bir alan oluşturmaktadır. Dolayısıyla internet ortamı, diğer deyişle sanal âlem, hükümetler dışındaki grupların da dış ilişkilerde -resmi olmayan bir düzeyde- rol oynamasına imkân tanımaktadır (Sheldon, 2011).

Nitekim bilişim sistemlerinde ve üstün özellikli bilgisayarlardaki ticari gelişmeler, bilgi işlem, iletişim ve yazılımdaki hızlı ilerleme, kısaca hayatımızın tüm alanlarında olası geniş kapsamlı değişiklikleri mümkün kılmıştır. Bu yüzden, devletler tarafından asıl ciddi olarak ilgilenilmesi ve dikkate alınması gereken olgu, günümüzde sanal âlem (evren) olarak da bilinen "siber uzay" ve onun içindeki asimetrik ve sanal mücadele ve savaşlardır. Bunun arkasındaki temel sebep, siber evrenin bir yandan parlak bir geçmişi anımsayıp, çok daha parlak bir geleceği öngörürken, bir yandan da bu duruma, önümüzdeki yıllarda, özellikle siber uzay, bilgi teknolojileri ve sibernetik yüzünden daha kasvetli ve karanlık bir gelecek olarak yaklaşılması gerçeğidir. Bu noktada siber uzayın, özellikle bazı devletlerce son 20-30 yılda adeta bir siber savaş alanı olarak kullanılması, anılan evrenin asimetrik risk ve tehditler dolu bir platform haline dönüştürülmesi ve bu vesileyle, siber saldırı eylemlerinin uluslararası ilişkilerde birer sorun, ihtilaf veya anlaşmazlık çözücü etkin siber silahlar olarak kullanılması gibi hususlar dikkat çekici ve bir o kadar da ürkütücüdür (Tabansky, 2011). Bu yüzden de, tüm bu parlak teknolojik gelişmelerin, gerek birey, gerekse devletlerin yaşamına yeni türlü, tanımsız, zamansız, limitsiz ve kuralsız, en kötüsü de hem bireysel hem de ulusal güvenlik mülahazaları bakımından oldukça riskli ve tehlikeli değişikliklerin ithaline vesile olduğunu söylemek mümkündür.

Nitekim 1950'lerden başlayarak, özellikle 1957'de ilk uydunun uzaya fırlatılmasından bu yana, süper güçler arasında uzaya ulaşma ve uzayda kalma yolları ve yakın gezegenler üzerinde yoğun bir rekabet mevcut olagelmiştir. Bu alandaki ilerleme, bilgi işlem ve elektroniğin ortaya çıkması sonucunda ivme kazanmıştır. Bu hızlı bilgi işlem, bilişim ve iletişim teknolojileri alanlarındaki

gelişmeler, hızla değişen ve aynı zamanda da tahminlerin ötesinde inanılmaz bir şekilde gelişen alanı betimlemektedir. Bu olağanüstü alan günümüzde bilinen tanımlamasıyla "siber uzay"dır ki, siber uzay olgusu aslında doğada değil, insan tarafından fenomenal, suni ve sanal olarak yaratılan bir evrendir.

Siber uzay alanı veya evreni, insan toplulukları ve günümüz modern yaşamı için bir yandan büyük yararlar sunarken, öte yandan zamansız, normsuz ve sınırsız tehditler için de kendi potansiyelini yaratmaktadır. Bu sanal âlemde, sanal mecra ve kaynaklardan gelen yeni risk ve tehditler etkin bir şekilde ortaya çıkarken, devletler ve uluslararası aktörler son 50 yıldır bu yeni güvenlik algı ve tehdidini anlamakta büyük sıkıntı çekmektedirler. Bunun ana sebebi, bu sanal risk ve tehditlerin; öngörülemeyen, bilinmeyen ve güvenilmez oluşlarıdır. Nitekim 20. yüzyılın insancıl ve masum sibernetiğinden miras kalan günümüz siber uzayın, 20. yüzyılda yaşanan ve her alanda insanlığın en büyük düşmanlarından biri olarak türlü şekillere giren terörizm tehlikesinden bu yana, günümüzde aslında bir olgu ve silah olarak daha yeni başladığını ve siber uzaya yönelik gelişmelerin doğal olarak ulusal güvenlikler için büyük riskler oluşturduğunun görüldüğünü savlamak (Ben-Israel, 2010) pek de yanlış olmayacaktır. Dolayısıyla, günümüzde hem toplumların hem de devletlerin, siber uzayda bir hayalet gibi dolaşan ve bilinmeyen; ancak, daha da önemlisi zamansız, kuralsız ve sınırsız, bu yüzden de azami derecede asimetrik bahse konu yeni sanal risk ve tehditlere karşı oldukça savunmasız durumda olduklarını (Akarçay & Ak, 2018) vurgulamak gerekir. Zira düşmanların siber evrendeki tutum ve davranışlarını anlamak, siber savaşın teknik doğası nedeniyle çoğu zaman imkânsız olabilmektedir.

Nitekim siber savaş ve bilgi savaşı söz konusu olduğunda, günümüzde Rusya Federasyonu en gelişmiş yeteneklerden birine sahip ve aynı zamanda stratejik avantaj ve beklenen sürprizlere sürprizle karşılık verme kapasitesini taşımaktadır. Keza Rus yetkililer, herhangi bir dış güç veya saldırı ile karşı karşıya kalmaları durumunda ve savaş dışındaki durumlarda kullanılmak üzere siber teknolojilerin ve savaşın kullanımıyla iyi bir hücum sistemi oluşturmaya çalışmaktadır. Nitekim Rusya'nın bilgi güvenliği ve bilgi tehditlerine yaklaşımının temel ilkeleri, Rus beyan politikasından tutarlı bir şekilde açıklığa

kavuşturulmuştur ve bunların uygulanmasının gelişimi, bilgi güvenliği yaklaşımını ortaya koyan çok sayıda siyasi Rus belgesi aracılığıyla izlenebilir (CISA, 2022).

Rusya'nın siber savaşı, hizmet reddi saldırılarını, bilgisayar korsanı saldırılarını, dezenformasyon ve propagandanın yayılmasını, devlet destekli ekiplerin siyasi bloglara katılımını, Rusya'da faaliyet gösteren telekomünikasyon ve telefon ağlarının yasal müdahale arayüzleri için teknik şartname niteliğinde olup, spesifikasyonun mevcut formu ile hem telefon hem de İnternet iletişiminin hedeflenen gözetimini sağlamayı amaçlayan SORM (The System for Operative Investigative Activities [Operasyonel Soruşturma Faaliyetleri Sistemi]) (Ayrıntı için bkz. https://en.wikipedia.org/wiki/SORM, 2022) teknolojisini kullanan internet gözetimini, siber muhaliflere yönelik zulmü ve diğer aktif önlemleri içermektedir (Kantchev ve Strobel, 2021). Araştırmacı gazeteci Andrei Soldatov'a göre, bu faaliyetlerin bir kısmı, FSB'nin bir parçası olan ve daha önce 16. KGB departmanının bir parçası olan Rus sinyal istihbaratı tarafından koordine ediliyordu (The Wayback Machine, 2006; https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia, 2022).

Nitekim ABD Savunma İstihbarat Teşkilatı tarafından 2017'de yapılan bir analiz, Rusya'nın "Karşı Bilgi Önlemleri" veya IPb (informatsionnoye protivoborstvo) hakkındaki görüşünü, "Bilgi Karşı Önlemlerini", "Bilgisel-Teknik" ve "Bilgisel-Psikolojik" gruplar olarak iki kategoriye ayırarak, bilgi karşı önlemleri faaliyetlerinin ana ve temel misyonunu; "kendi yerel halkını kontrol etmek ve düşman devletleri etkilemek için stratejik olarak belirleyici ve kritik derecede önemli" olarak özetlemektedir. Bu bağlamda, Rus bilgisel-teknik faaliyetleri; savunma, saldırı ve sömürü ile ilgili ağ operasyonlarını ihtiva ederken, bilgisel-psikolojik faaliyetleri ise, "insanların davranışlarını veya inançlarını Rus hükümetinin hedefleri lehine değiştirme girişimlerini" kapsamaktadır (US Defence Intelligence Agency, 2017).

Nitekim bir ABD Beyaz Saray analizine göre; Rus hükümeti, geniş kapsamlı siber casusluk sağlamak, belirli sosyal ve politik faaliyetleri bastırmak, fikri mülkiyeti çalmak ve bölgesel ve uluslararası düşmanlara zarar vermek için kötü niyetli siber faaliyetlerde bulunmaktadır (The White House,

2021). Nitekim ABD Ülke Güvenliği (US Homeland Security) kurumu bağlısı CISA (Cybersecurity and Infrastructure Security Agency [Siber Güvenlik ve Altyapı Güvenliği Ajansı]) ve diğer sınıflandırılmamış kaynaklar tarafından yayınlanan son Danışmanlıklar, Rus devlet destekli tehdit aktörlerinin Amerika Birleşik Devletleri ve diğer Batılı ülkelerde şu sektörleri ve kuruluşları hedef aldığını ortaya koymaktadır: COVID-19 araştırması, hükümetler, seçim kuruluşları, sağlık ve ilaç, savunma, enerji, video oyunları, nükleer, ticari tesisler, su, havacılık ve kritik üretim. Aynı raporlama, Rus aktörleri, SolarWinds yazılım tedarik zincirinin 2020'de ele geçirilmesi, 2020'de COVID-19 aşıları geliştiren ABD şirketlerinin hedeflenmesi, 2018'de ABD endüstriyel kontrol sistemi altyapısının hedeflenmesi, dünya çapındaki kuruluşlara yönelik 2017 NotPetya fidye yazılımı saldırısı ve ABD Demokratik Ulusal Komitesi'nden çalınan belgelerin 2016 yılında sızdırılması dâhil olmak üzere bir dizi yüksek profilli ve kötü amaçlı siber etkinlikle ilişkilendirmiştir (CISA, 2022).

ABD Ulusal İstihbarat Direktörü Ofisi'nin 2021 Yıllık Tehdit Değerlendirmesi (US Office of the Director of National Intelligence, 2021) ise, bir yandan Rusya Federasyonu'nun, casusluk, etki ve saldırı yeteneklerini geliştirip kullanırken en büyük siber tehdit olmaya devam edeceğine vurgu yaparken, öte yandan Rusya'nın ABD'de ve/ya müttefik ve ortak ülkelerdeki su altı kabloları ve endüstriyel kontrol sistemleri dâhil olmak üzere kritik altyapıyı hedeflemeye devam ettiğini; ABD ve müttefiklerinin bu tür altyapı sistemlerinden ödün vermesinin, Rusya'nın bir kriz esnasında söz konusu altyapıya zarar verme yeteneğini artırabileceğini ve hatta bunu gösterebileceğini belirtmektedir. Bu değerlendirme, Rusya'nın siber saldırıları, düşmanları caydırmak, kriz sürecindeki tırmanmaları kontrol etmek ve çatışmaları kendi lehinde yönlendirmek için neredeyse kesin ve kabul edilebilir bir seçenek olarak gördüğüne ve Rusya kaynaklı oldukça asimetrik bir risk ve tehdit evrenine dikkat çekmektedir.

Siber suçlarda, siber terörizmde ve siber savaşta birçok araç, lojistik ve yöntem benzer olduğundan, Rusya kapasitesini hızlı bir şekilde genişletebilmektedir. Bu çalışmanın amacı Rusya'nın siber saldırı stratejileri

üzerinden uluslararası ilişkilerde siber saldırıların araçsallaştırılmasını incelemektir. Bu çalışma, siber uzayda artan insan etkileşiminin onu stratejik bir alan düzeyine yükselttiği ve dolayısıyla uluslararası ilişkiler için teorik ve pratik zorluklar doğurduğu öncülüne dayanmaktadır. Çalışmanın giriş bölümünü takiben birinci bölümünde araştırma ile ilgili genel bilgiler ve literatür çalışması; ikinci bölümünde siber saldırılarla ilgili kavramsal bir çerçeve sunulacak; üçüncü bölümünde uluslararası ilişkilerde siber saldırıların araç haline dönüştürülmesi incelenecek; dördüncü bölümünde ise, Rusya Federasyonu kaynaklı siber saldırılar ve uluslararası ilişkilerde etkileri irdelenerek, sonuç ve değerlendirme bölümü ile tez çalışması nihayetlendirilecektir.

2. GENEL BİLGİLER VE LİTERATÜR ÇALIŞMASI

2.1. Araştırmanın Konusu

Siber uzay, akademisyenler, siyaset bilimcileri, iletişim uzmanları, çok uluslu iş birliği, uluslar, politika geliştiriciler ve hatta piramidin altındaki vatandaşlar için de entelektüel söylemi tetikleyecek ölçüde büyümüştür. Siber evren, insanlık ve onun gelişmesi yolunda bankacılıktan eğitime, iletişimden reklamcılığa, eğlenceden ekonomiye birçok yararlılıkların yanında, kötü niyetli çevrelerce zararlı amaçlarla da kullanılmaya başlamıştır. Bunlara örnek olarak, sanal âlem dolandırıcılıkları, sahtekârlıkları, istismarcılıkları vs. gösterilebilir.

Bununla beraber, sanal evrenin, diğer deyişle siber uzayın askeri-politik amaçlarla bir savaş alanı olarak kullanılmasının, özellikle bu asimetrik tehdidin ve riskin nereden, ne zaman, ne şiddette, ne miktarda ve kuralsız, koşulsuzca geleceği belli olmadığından, hedef ülke, kurum, toplum veya birey üzerinde yıkıcı ve büyük çaplı etkileri olduğu görülmüştür. Dolayısıyla bu da uluslararası toplumla ilişkilerinde -neredeyse- sürekli uyumsuzluk ve başarısızlık yaşayan kimi devletlerce uluslararası ilişkilerde başarı kazanmanın bir yolu olarak görülmüş; siber uzaydaki siber eylem ve saldırılar söz konusu başarısız devletlerin uluslararası ilişkilerinde karşı taraflara karşı ulusal hedef, amaç ve menfaatlerini sağlama yolunda birer araç olarak kullanılması sonucunu doğurmuştur. Zira siber saldırı, yetkisiz bir kişi veya gruplar tarafından bir ulusun, kuruluşun veya bireyin veri tabanına stratejik bir sızmadır. Günümüzde siber saldırılar, uluslararası ilişkilerin merkezi konuları arasında yer almaya başlamıştır. Bu çalışmanın konusunu; Rusya kaynaklı siber eylemler örneğinden yola çıkarak, siber saldırıların uluslararası ilişkilerde birer araç olarak kullanılmasının incelenmesi oluşturmaktadır.

2.2. Araştırmanın Sorunsalı

Uluslararası ilişkilerde artan rekabet koşulları ile küresel ortama ayak uydurmak için hem ulusal hem de uluslararası düzeyde bilgi teknolojileri yaygın şekilde kullanılmaya başlanmıştır. Bunun sonucunda da kamusal işlemler bilişsel ve elektronik ortamlarda gerçekleştirilmekte ve sanal ve reel raporlamalar yapılmaktadır. Dolayısıyla bilgi teknolojileri, devletlerin hem iç hem dış ilişkilerinde birçok kolaylık sağlayarak fırsat yaratmanın yanında çeşitli tehdit ve riskleri de beraberinde getirmektedir. Zira sanal evren, diğer adıyla siber uzay büyük bilinmezlikler, zamansız, limitsiz ve kuralsız bir âlemi dikte etmektedir. Bu yüzden de çoğu toplum ve devlet için siber uzay halen bir fenomendir. Tezin temel sorunsalı; siber saldırıların bir araç olarak kullanılmasının uluslararası ilişkilerde ne derece etkili olduğunun, Rusya kaynaklı siber saldırılar örnekleri üzerinden belirlenmesidir.

Nitekim günümüzde, özellikle ulusal güvenlik bağlamında, siber uzayın ve içindeki savaşın ciddi şekilde dikkate alınması gerektiğine dair etkileyici bir tahminin altını çizebiliriz. Bunun nedeni, ulusal güvenliğin bilgi devrimi ve siber uzay olgusundan oldukça etkilendiği konusunda net bir duruş ortaya koymaktadır. Siber uzay gibi yeni bir alanın akıllıca kullanılması, yeni yöntemlerle birlikte askeri alanda niteliksel bir değişim yaratan daha önce bilinmeyen yeteneklere olanak sağlamıştır.[2] Bununla birlikte, diğer yeni yüksek teknoloji alanlarında olduğu gibi, siber güvenlik konusunda da örneğin şu anda Türkiye'de olduğu gibi, birçok ülkede kamuoyu tartışması eksiktir (Akarçay & Ak, 2018).

Siber uzay pek çok karmaşık konuyu içerdiğinden, doğası gereği gizli olan bir alanda yeni mücadele teknikleri, araçları ve normları geliştirmek daha da zor görünmektedir; dolayısıyla siber evrende meydana gelen her siber saldırıyı tespit etmek neredeyse imkânsızdır. Siber eylemlerdeki virüslerin bazıları yıllarca fark edilmeden çalışabilir; diğerleri ise kısadır, ancak, yine de algılanabilir bir iz bırakmazlar. Bu nedenle, siber saldırganlar kim olduklarını

2 Askeri meselelerde bilgi teknolojisi devriminin bir tartışması için bkz. (O'Hanlon, 2000; Johnson & Libicki, 1995; Ben-Israel, 2001)

açıklamazlar ve kurbanlar savunmasız olduklarını kabul etmek istemeyebilirler. Bu tartışma belgesi aynı zamanda devletler ve toplumlarla (işletmeler veya bireylerden ziyade) ve onların birbirine bağlılık ve bağımlılık yoluyla siber uzaydan gelen veya siber uzay tarafından kolaylaştırılan saldırgan savaş eylemlerine karşı savunmasızlığı ile ilgilenecektir. Keza siber savaş, iddia edebilirsek, gerçekten de stratejik bir sorun olarak görülmelidir (HM Government, 2010).

2.3. Araştırmanın Amacı

Siber savaş, siber uzayın en kötücül yüzü ve en zararlı yönü olarak, 1990'lardan bu yana süper güçlerin ve hatta küçük güçlerin elinde etkili bir araç haline gelmiştir. Böylece siber savaş, güçlü ve küçük güç devletleri eşit konuma getiren bir savaş türü olan asimetrik savaşı tetiklemiştir. Nitekim siber savaşlar, silahlı bir çatışma veya sosyal bir kargaşa ile ortaya çıkan yıkımdan daha önemli askeri-politik avantajlar sağlayabilecek niteliktedir. Zira kritik bilgilerin elde edilmesi, askeri komuta ve kontrol sistemlerinin devre dışı bırakılması, bilgisayar odaklı silahlara zarar verilmesi, ulusal bankalar veya borsalar gibi ekonomik kritik kurumların mahvedilmesi, kritik bilgilerin hacklenmesi gibi çeşitli ölçeklerde bilgi sistemi aracılığıyla bir dizi düşmanca siber faaliyet gerçekleştirilebilir.

Dolayısıyla, siber saldırıların uluslararası ilişkilerde daha etkili bir şekilde araçsallaştırılmaya başlandığını söylemek mümkündür. Zira milyonların etkileneceği ve ölebileceği nükleer bir patlamanın aksine, büyük bir siber saldırının veya savaşın bir toplum içinde veya bir grup için yaratacağı etkiler çok daha yıkıcı ve ciddi sonuçları olması muhtemel görünmektedir. Nitekim literatür ve sistemdeki olaylar gösteriyor ki, devlet dışı aktörler siber savaşın yürütülmesinde önemli ölçüde yer almaktadır (Klimburg, 2011).

Örneğin, Nye (2010) için: "Siber güç, siber alanın elektronik olarak birbirine bağlı kaynakları ve bilgilerinin kullanımı yoluyla tercih edilen sonuçları elde etme yeteneğidir" (ss. 3-4). Devlet dışı aktörlere ilaveten, daha fazlasının dâhil edilmesinin nedeni, gelişmekte olan bu alandaki aktörlerin en önemli özelliği, bilginin ve bilginin kullanımının tüm dünyada artmasıdır.

Ancak, bilgi kullanımı arttıkça, medeniyetin kontrolüne yönelik artan bir tehdit de bulunmaktadır (Alford, 2001).

Bu bağlamda, bu tez çalışmasının ana amacı; uluslararası ilişkilerde siber saldırıların araç olarak kullanılması durumunu Rusya kaynaklı siber saldırılar örneği üzerinden incelemek ve ortaya koymaktır. Bu bağlamda, birinci bölümde genel bilgiler ve literatür çalışmasına yer verilerek, ikinci bölümde siber saldırılarla ilgili bir çerçeve sunulacak, üçüncü bölümde uluslararası ilişkilerde siber saldırıların araç haline dönüştürülmesi incelenecek, dördüncü bölümde ise, Rusya kaynaklı siber saldırılar ve uluslararası ilişkilerde etkileri tartışılacaktır. Sonuç bölümünde ise, ana tespit, bulgu ve sonuçlara genel yorum, değerlendirme ve görüşler ile değinilecektir. Bu çalışmada elde edilen bilgi, bulgu ve belgeler ışığında, bu tez çalışmasının ulusal ve uluslararası alanda yapılacak araştırmalarda literatüre katkı sağlayacağı düşünülmektedir.

2.4. Araştırmanın Önemi

Sibernetikteki gelişmeler, yaşamın her alanında uzun erişimli değişiklikler meydana getirmiştir. Böylece, 1950'lerden sonraki bilimsel-teknolojik ilerlemeler, ulusal güvenliğin de kendisinden oldukça etkilendiği, "bilgi devrimi"ne yol açmıştır. Bilgi-işlem alanındaki hızlı gelişme, siber âlem olarak bilinen yeni bir fantastik dünya yaratmıştır. Bir fenomenel olgu olarak olarak siber âlem, büyük imkân ve avantajlarının yanında bilinmedik riskleri de içerisinde barındırma potansiyeline sahiptir. Hepsi siber âlem ile ilgili olmak üzere, uluslararsı toplumu ilgilendiren üç ana olgusal durum mevcuttur. Bunlar; (1) ulusal veya uluslararası politika ve stratejiler, (2) bilişim ve iletişim teknolojileri ve (3) ihtilaf ve anlaşmazlıklardır.

Zira siber evren çerçeveli siber savaş ve bu bağlamdaki devlet-merkezli veya birey/grup-temelli siber saldırılar, özellikle bilişim ve iletişim teknolojilerini kullanarak, ya devlet tarafından benimsenen politikalar bağlamında ulusal amaç ve hedeflere ulaşmak, ya da birey/grup tarafından kendi amaç ve hedeflerini elde etmek yönünde stratejiler benimseyerek, bireysel veya uluslararası bağlamda ortaya çıkmış ihtilaf ve uyuşmazlıkları çözmede bir araç olarak kullanılmayı dikte eder. Bu nedenle, herhangi bir devlete yönelik genel

maksatlı ve devlet destekli bir siber saldırılar zinciri veya herhangi bir devletin vatandaşlarına karşı girişilebilecek bireysel bir siber saldırının yapabileceği gerçek hasarın analizi için, bu fenomeni tam olarak anlayabilmemize yardımcı olabilecek türden bazı etkileri analiz, bunun pratik sonuçları ile başlamak temel bir gerekliliktir.

Nitekim siber evren, birbiriyle çelişkili birçok konu içerdiğinden, aslında tamemen gizli bir alanda yeni savaşma normları, araçları ve teknikleri üretmek oldukça zor bir konudur. Siber saldıranlar, kendilerinin kim olduğunu belirtmez ve kurbanlar da kendilerinin saldırılara açık olduğunu kabule pek yanaşmazlar (Akarçay & Ak, 2018).

Bu çerçevede, bu tez çalışması; özellikle zamansız, kuralsız ve sınırsız özelliklere sahip siber saldırıları bir asimetrik silah olarak kullanarak ve böylece kendi ulusal hedeflerine ulaşmada bunları araçsallaştırarak uluslararası ilişkilerde kazanç sağlamaya yönelik siber eylemleri, bu eylemleri son 20-30 yılda birçok vakada kullandığı tespit edilen Rusya Federasyonu'nun siber eylemleri üzerinden incelemek bakımından önemlidir.

Zira önümüzdeki dönemde yapay zekâ, robotik, metaverse (kurgusal evren) vb. gelişmeler de göz önüne alındığında, uluslararası ilişkilerde güç mücadelelerinin konvansiyonel savaşlardan ziyade, siber, ticari, virüs, terör gibi asimetrik savaşlarla sürdürüleceği ve bunlardan doğan zamansız, kuralsız ve sınırsız tehdit ve risklerin, gerek uluslar, gerekse uluslararası toplum ve onların güvenlikleri için konvasiyonel silahlara nazaran çok daha bütük çaplı, etkili ve yıkıcı sonuçları olacağı değerlendirilmektedir. Bu durum da bu tez çalışmasının önemini artıran başlıca etmenlerden birisidir.

2.5. Araştırmanın Literatür Taraması

Bu çalışma, esas olarak nitel (kalitatif) bir araştırma olup, tümdengelim yaklaşımını benimsemiştir. Araştırmaya temel olacak bilginin toplanmasında, üniversite ve kamu kütüphanelerinden yararlanmayı içeren veri toplama yöntemi esas olarak belirlenmiştir. Bu bağlamda, ilgili mahallerde araştırmanın sorunsalı

ve araştırma soruları ile ilgili olan azami sayıda bilimsel kitap, makale, rapor, proje ve tezler gibi ikincil veri kaynakları taranmış ve bulunmuştur.

Bu şekilde, araştırmanın bulgularını destekleyecek olan ana ve tali kaynaklar elde edilmiş, okunmuş, kaynakların içerindeki bilgiler araştırmanın geçici ana hatlarına uygun olarak tasnif edilmiş, analitik bir incelemeye tabii tutulmuş ve araştırma içerisine etik yayın kurallarına uygun olarak ithal edilmiştir. Böylece, araştırmanın giriş bölümü ortaya çıkarılmış, müteakiben araştırmanın sorunsalı kapsamında elde edilen analitik temelli bulgular detayıyla araştırmanın inceleme bölümünde ortaya konmuş ve analitik bir incelemeye tabi tutulmuş; sorunsala etki eden durumlar, etkiler ve nedenler genel tespitler olarak ortaya konulmuş; son olarak da, sorunsala yönelik elde edilen tespit ve bulgular, ana hatlarıyla bir sonuçlar, görüşler, yorumlar ve öneriler manzumesi ile vurgulanarak, araştırma nihayetlendirilmiştir.

2.6. Araştırmanın Yöntemi

Esas olarak nitel araştırma metodolojisini benimsemiş olan bu çalışmada, araştırmanın kavramsal çerçevesinde konu ele alınırken kavramlar ve ilişkileri açıklayan "tanımlayıcı", olayların arka planındaki gerçekleri bulmaya çalışan "nedensel", vuku bulan olaylardan ilkeler çıkaran "kuramsal", geçmişte yaşanan bir vakanın etkisi ve bu durumun günümüzdeki etkilerini inceleyen "tarihsel", araştırılan konu ile ilgili kütüphane, arşiv, internet gibi kaynaklardan elde edilen bilgilere dayalı çalışmaların bilimsel araştırılmasını içeren; doküman analizi, içerik analizi ve yorumsamacılık gibi bilimsel araştırma yöntemlerinden yararlanılmıştır.

2.7. Araştırmanın Kapsamı ve Sınırlıkları

Tez çalışmasının ana kapsamı; uluslararası ilişkiler, uluslararası güvenlik, siber uzay, siber güvenlik, siber eylemler, siber saldırılar, siber savaştır. Rusya kaynaklı siber saldırılar ile sınırlılığı mevcuttur.

2.8. Araştırmanın Hipotezleri

Tez çalışmasının esas olarak iki ana hipotezi mevcuttur. Bunlar;

- H0 (Yokluk Hipotezi): Rusya kaynaklı siber saldırıların uluslararası ilişkilerde siber saldırıların araç olarak kullanılması üzerine etkileri bulunmamaktadır.

- H1 (Araştırma Hipotezi): Rusya kaynaklı siber saldırıların uluslararası ilişkilerde siber saldırıların araç olarak kullanılması üzerine etkileri bulunmaktadır.

2.9. Araştırmanın Veri Toplama Yöntemleri

Araştırmada veri toplama yöntemi olarak nitel araştırmada doğrudan görüşme ve gözlem yapılması mümkün olmaması durumunda doküman inceleme ve analiz yöntemi uygulanmıştır. Çalışmada bilimsel kitap, makale, kitap bölümü, tez, bildiri başta olmak üzere birçok akademik çalışma, yerli ve yabancı kamu kurum ve kuruluşlarının hazırladığı raporlar, araştırma merkezlerinin ve sivil toplum kuruluşlarının hazırladığı bilimsel raporlar, sosyal medya, Türkiye ve dünya çapında yer alan ulusal ve uluslararası kuruluşlarının haber, köşe yazıları ve açık kaynaklardan veriler elde edilmiştir.

3. SİBER SALDIRILAR-KAVRAMSAL ÇERÇEVE

3.1. Siber Uzay

Köken olarak "siber" kavramı, eski Yunanca "kübernetes" kelimesinden türetilmiş olup, sibernetik sözcüğüne dayandırılmıştır. Sibernetik kavramı ise; "sosyolojik, biyolojik, teknolojik ve ekonomik sistemlerde, kumanda uç iletişim sistemlerini incelemeye dayanan bir amaca doğru yönlendirilmiş etki bilimi" biçiminde açıklanmaktadır (Bayraktar, 2015, s.13). Sibernetik terimi, ilk olarak 1958'de sibernetik bilimi kurucularından olan ve makineler ile canlılar arasında mevcut iletişimi incelemiş olan Louis Couffignal tarafından kullanılmıştır (Yılmaz, 2017).

Siber uzay tabiri ise, sanal hayatlar ve toplulukların yaşamış olduğu sanal alanlar şeklinde tanımlanabilir. Bunun sebebi, toplulukların ve yaşamların gerçek toplumların sahip bulunduğu fiziksel gerçekliğe sahip bulunmamalarından kaynaklanmaktadır (Jordan, 2003). Bu kapsamda, "Siber uzay" terimi ilk olarak William Gibson tarafından 1982'de yazılan "Burning Chrome" adlı kısa öyküde bilgisayar tarafından oluşturulan bir sanal gerçekliğe atıfta bulunmak için kullanılmıştır. Ancak, terim 1984 yılında Gibson'ın *Neuromancer* adlı romanında kullanılmasından sonra popüler hale gelmiştir. **"**Siber" kökü, aynı zamanda insan vücudunun ileri teknoloji cihazlarla birleştirilmesiyle elde edilen bir insan-makine sentezini tanımlayan bir terim olan 'cyborg' terimi ile de ilişkilidir. Gibson'a göre siber uzay, uzay-dışı gerçek bir dünyanın adıdır. Bu durum; "simgeler, ara noktalar ve yapay gerçeklikler" aracılığıyla insanların sanal mevcudiyeti ve insanlar arasındaki etkileşim yeteneği ile karakterize edilir. Gibson'a göre siber uzay, kentsel deneyimler ve suç, sosyal dışlanma ve yoksulluk gibi sorunlarla ilgilenen bir kentsel "ince" alandır (Akt. Kneale, 1999).

Siber uzayın sanal dünyası üzerindeki hız ve hareketlerin yeni uzamsal deneyimler için anahtar metaforlar olduğu, son derece genişlemiş ve son derece

kutuplaşmış şehirlerde meydana gelen sosyo-ekonomik çatışmaları ve coğrafi bölünmeleri yansıtır. Gibson'ın kendisi, yaratıcı hikayeleriyle, dünya çapında İnternet gibi bilgisayar ağlarının yaygın kullanımını öngörmediğini; ancak, romanlarında anlatılan hayali ve fütürist dünyaları anlamlandırmak için gerçek teknolojik gelişmeleri kullandığını kabul etmektedir (Gibson, 1996).

Siber alandan türetilen ifadelerin gelişigüzel kullanımı göz önüne alındığında, "siber uzay" teriminin kendisini netleştirmek önemlidir. "Siber uzay" ve "siber alan veya evren" burada eş anlamlı olarak ele alınacaktır. Bu nedenle, siber uzayı bir sosyal etkileşim alanı olarak kavramsallaştırmak önemlidir. Siber uzayın farklı yorumları, bilgi akışının ve siber uzayın birbirine bağlılığının geliştirildiği elektromanyetik alan hakkında daha teknik tanımlardan, sinerji içinde çalışan fiziksel ve teknik katmanların interpozisyonunu dikkate alan daha teorik tanımlara kadar uzanan bir spektrum oluşturmaktadır. Değişik "siber uzay tanımları" yelpazesinin teknik ucu, farklı ülkelerin savunma belgelerinde öne çıkmaktadır ve bunlar incelendiğinde, bu ülkelerin siber uzaya olan ilgisini göstermektedir. Farklı ülkelerden savunma kurum ve kuruluşlarının yaptığı yorumların analizi, siber uzayı beşinci stratejik alan olarak kabul etmesi nedeniyle önemlidir (Medeiros & Goldoni, 2020).

Brezilya Savunma Bakanlığı 2016 tarihli Ulusal Savunma Beyaz Bülteni, siber uzayın devlet ve devlet dışı tehditlerin ortaya çıkmasına olanak tanıdığını kabul etmektedir. Siber alan, bir siber saldırının neden olabileceği kritik altyapıya olası zarar nedeniyle stratejik bir alan olarak kabul edilir. Almanya'nın Beyaz Kitabı 2016 ise, siber uzayı; terörizm, siber suçlular, sahte kimlik kullanımı, endüstriyel casusluk ve altyapıya zarar verme gibi devlete bağlı olmasa da yeni tehditler için bir alan olarak kabul eder. Söz konusu belge, ayrıca siber uzayın kısa bir tanımını da sağlar; "Siber alan, küresel ölçekte veri düzeyinde bağlantılı ve bağlanabilir tüm bilgi teknolojileri sistemlerinin sanal alanıdır." Bu bağlamda, siber uzayın temeli, herhangi bir sayıda ek veri ağı ile tamamlanabilen ve daha da genişletilebilen evrensel ve halka açık bir bağlantı ve ulaşım ağı olarak internettir (Akt. Medeiros & Goldoni, 2020).

Rattray'in (2009) yaklaşımı, siber uzayı fiziksel ve yapay bir alan olarak gördüğünü dikkate alarak teknik ve teorik yönler arasında bir köprü görevi

görür; "Ancak, siber uzay aslında fiziksel bir ortamdır; yazılım ve iletişim protokollerinde belirlenen kurallarla yönetilen fiziksel sistemlerin ve ağların bağlantısıyla oluşturulur." (s.254)

Cohen (2007), siber uzayın en iyi şekilde "gerçek, somutlaşmış kullanıcıların yaşadığı ve deneyim yoluyla kavrandığı, ağ bağlantılı bir alanla bağlantılı ve bu alan içinde kapsandığı" (s.255) olarak anlaşıldığını savunur. Yaklaşımı, kullanıcıların deneyimlerine dayalı bir siber uzay anlayışı sunması açısından dikkate değerdir. Bu bakış açısı göz önüne alındığında, birden fazla aktörün kendine özgü özelliklerini kullanması siber uzayı dönüştürür. Çeşitli aktörlerin kritik altyapının, kamu ağlarının ve silah sistemlerinin yerleşik olduğu operasyonel alan olan siber uzayı dönüştürme ve kullanma yeteneği, daha sonra gösterileceği gibi, devletin kendisini tek güç sahibi olarak varsaymasının istikrarsızlaşmasına katkıda bulunur.

Libicki (2009) de, siber uzayın farklı katmanlar arasındaki etkileşimin sonucu olduğu görüşünü benimser. Libicki'ye göre, fiziksel bir katman (donanım), kutular ve kablolardan oluşan siber uzayın temelini temsil eder. Başka bir deyişle, her tür akıllı ve birbirine bağlı cihazda temsil edilen fiziksel elektronik bileşenlerdir. İkinci katman, geliştiriciler tarafından cihazlara programlarına uymaları ve birbirleriyle iletişim kurmaları için verilen talimat ve komutlardan oluşan sözdizimseldir. Son olarak, makinelerde bulunan bilgileri temsil eden semantik katman gelir. Libicki'nin yaklaşımı, siber alanı, sözdizimsel ve anlamsal katmanları oluşturan ikili veriler biçimindeki maddi olmayan öğeler tarafından yapılandırıldığından, kara, hava ve deniz ile karşılaştırıldığında daha az somut bir ortam olarak kabul eder.

3.2. Siber Saldırılar

Siber saldırıları ele almak için yerel ve uluslararası hukukun nasıl kullanılabileceğini değerlendirmedeki ilk zorluk, karşılaştığımız sorunun niteliğini ve kapsamını belirlemektir. Siber uzaydaki faaliyetler, savaş hukuku kapsamında silahlı çatışmayı yöneten birçok geleneksel kategoriye ve ilkeye meydan okumaktadır. Siber saldırı, siber suç vb. terimlerinin çeşitli tanımları

uluslararası literatürde bulunabilir ve hepsinin ortak amacı verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini tehlikeye atmaktadır (Şahinaslan, 2013).

Teknolojik evrim aynı zamanda siber suçların ilerlemesini de beraberinde getirmekte, böylece saldırılar gerçekleştirmek, daha da zor olan hedeflere ulaşmak ve takip edilmemek için sürekli yeni yollar geliştirilmektedir. Bununla birlikte, geleneksel siber tehditler en yaygın saldırıların kaynağı olmaya devam etmektedir (Şahinaslan, 2013).

Dünyada İnternet ve bilgisayar kullanımının hızlı bir şekilde yaygınlaşmaya başlaması kullanıcılara belirli kolaylıkları sağlarken beraberinde birtakım tehditler de getirir. Bu tehditler arasında, devletlerin ve kurumların siber saldırılara maruz kalması bulunmaktadır. Siber güvenliği ilgilendiren diğer terimler gibi siber saldırılarla ilgili de üzerinde uzlaşılmış bir tanım bulunmamaktadır. Lin (2010), siber saldırıyı; "düşman bilgisayar ağlarını, sistemlerini ya da bir bütün şeklinde bu ağların ve sistemlerin kapsamında yer alan programlar ve bilgileri aldatmak, bozmak, değiştirmek veya yok etmek amacıyla gerçekleştirilen uzun veya kısa süreler boyunca yapılabilen kasıtlı işlem ve eylemlerin kullanımını" ifade etmektedir (s.63).

Clarke, siber savaşı "bir devletin, zarar vermek veya kesintiye uğratmak amacıyla başka bir ulusun bilgisayarlarına veya ağlarına sızmaya yönelik eylemleri" olarak tanımlamaktadır. Birleşik Devletler Siber Komutanlığı ise, siber saldırıyı şu şekilde tanımlar; "Bilgisayarı veya ilgili ağları veya sistemleri kullanan ve bir rakibin kritik siber sistemlerini, varlıklarını veya işlevlerini bozmayı ve/veya yok etmeyi amaçlayan düşmanca bir eylemlerdir. Siber saldırının amaçlanan etkileri, mutlaka hedeflenen bilgisayar sistemleri veya verilerle sınırlı değildir; örneğin, altyapıyı veya C2 (komuta-kontrol) kabiliyetini düşürmeyi veya yok etmeyi amaçlayan bilgisayar sistemlerine yönelik saldırılardır. Bir siber saldırı, çevresel cihazlar, elektronik vericiler, gömülü kod veya insan operatörler dâhil olmak üzere ara dağıtım araçlarını kullanabilir. Bir siber saldırının etkinleştirilmesi veya etkisi, teslim edilen saldırıdan zamansal ve coğrafi olarak geniş ölçüde ayrılabilir." (Akt. Hathaway & Rebecca, 2012)

Genel olarak siber saldırı, "bir bilgisayardan bir web sitesine, bilgisayar sistemine veya bireysel bilgisayara karşı başlatılan ve bilgisayarın veya üzerinde depolanan bilgilerin gizliliğini, bütünlüğünü veya kullanılabilirliğini tehlikeye atan bir saldırıdır. Siber saldırı, zarar vermek amacıyla bir bilgisayara, bilgi işlem sistemine veya bilgisayar ağına yetkisiz erişim sağlama girişimidir. Siber saldırılar, bilgisayar sistemlerini devre dışı bırakmayı, bozmayı, yok etmeyi veya kontrol etmeyi ya da bu sistemlerde tutulan verileri değiştirmeyi, engellemeyi, silmeyi, manipüle etmeyi veya çalmayı amaçlar (Vida, 2005).

Siber saldırılar, aşağıdakiler de dâhil olmak üzere birçok türde olabilir (Farhat vd., 2017, ss. 1-2):

- Bir bilgisayar sistemine veya verilerine yetkisiz erişim elde etmek veya elde etmeye çalışmak,
- Verilerin yetkisiz bir kişiye veya konuma çevrimiçi olarak sızdırılması gibi veri hırsızlığı,
- Tüm web sitelerinin kaldırılması da dâhil olmak üzere istenmeyen kesinti veya hizmet reddi saldırıları,
- Bir bilgisayar sistemine virüs veya kötü amaçlı kodun (kötü amaçlı yazılım) yüklenmesi,
- Verileri işlemek veya depolamak için bir bilgisayar sisteminin yetkisiz kullanımı,
- Sahibinin bilgisi, talimatı veya onayı olmadan bir bilgisayar sisteminin donanımının, donanım yazılımının veya yazılımının özelliklerinde yapılan değişiklikler,
- Çalışanlar, eski çalışanlar veya başkaları tarafından bilgisayar sistemlerinin uygunsuz kullanımı.

Yeni çatışma ve zorlama yöntemleri, gücü, kurumları ve devlet davranış normlarını yeniden yapılandırarak uluslararası sistemde tektonik kaymalara neden olabilir. Bu bağlamda, devletlerin giderek daha fazla güvendiği dijital

altyapıyı bozan veya yok eden zorlayıcı eylemler olan siber saldırılar, böyle bir araç olma potansiyeline sahiptir. Siber saldırılar uluslararası ilişkilerde artan bir öneme sahiptir. 20 yıl önce duyulmamış bir yetenek, her şirket, devlet hizmeti, kamu hizmeti ve bilişime bağımlı hale gelen askeri yetenek ile birlikte yıkıcı potansiyeli arttıkça ön plana çıkmıştır. Bu artan yaygınlık göz önüne alındığında, tıpkı insanların denizde seyrüsefer ve uçuşta ustalaştığı zamanlarda olduğu gibi, bu yeni ortamın, internet veya siber uzayın, şimdi devletler arasında bir rekabet ve zorlama yeri olması beklenmektedir (Caveltry, 2008).

3.2.1. Bilgisayar korsanlığı

İlk anlam olarak İngilizce'de "Hack" kavramı bir baltayla ya da bıçakla kesmek, doğramak anlamını taşımaktadır. Bilişim kültüründe kavramın kökenleriyse kısa yollar bulmak işlemleri kestirmeden yapmak anlamını taşır. Bu bağlamda, İngilizce'de "hacker" tabiri, "hack" olayını icra eden kimse anlamında kullanılmaktadır. Türkçe'de ise "hacker" tabiri, "bilgisayar korsanı" olarak isimlendirilmektedir (Altınkaynak, 2017 s.1).

Bilgisayar korsanlığı, bilişim sistemleriyle etkileşimin alışılmadık herhangi bir yolunu, diğer deyişle tasarımcı tarafından bir standart olarak öngörülmeyen şekilde etkileşimi içerebilir. Bu siber tabir, esas olarak modern teknolojiler, bilişim teknolojileri ve bilgisayarlı cihazlarla bağlantılıdır. Bu nedenle, genel manada bilgisayar korsanlığı, bir bilgisayara yetkisiz veya yetkili erişimi aşarak kasıtlı olarak erişme eylemi olarak tanımlanır. Her durumda ve hepsinden önemlisi, bilgisayar korsanı, eylemlerinin yasal sonuçlarından sorumludur. Bilgisayar korsanlığı eylemi, bilgisayar kaynaklarına yetkisiz erişim elde etmeye veya başarılı bir şekilde elde etmeye çalışma sürecidir (Çıtak, 2018).

Bilgisayar korsanlarının temel amacı, herhangi bir kötü niyet olmaksızın sistemi kendi içinde tanımaktır. Bununla birlikte, bu amaç kimi zaman bilgisayarı ilk dizayn edenin asıl amacı dışında bir amacı gerçekleştirmek için bilgisayar donanımını ve yazılımını değiştirme uygulaması gibi farklı bir güdüden beslenebilir. Dolayısıyla, günümüzde bilgisayar korsanlarının, sistemsel zafiyet ve zayıflıkları ortadan kaldırmaya yardımcı olmak için analiz ve değerlendirmeden ziyade, çoğunlukla kâr, protesto, meydan okuma ve/ya

keyif alma gibi daha kötü niyetli istemlerden güdülendikleri (Kara, 2013) görülmektedir.

Bu kapsamda, Siyah-şapkalı Bilgisayar Korsanı (Black-Hat Hacker), bilgisayar güvenlik açıklarını bulmaya çalışan ve bunları kişisel mâli kazanç veya diğer kötü niyetli nedenlerle istismar eden kişidir. Beyaz-şapkalı Bilgisayar Korsanı (White-Hat Hacker) ise, bilişim dünyasında "iyi niyetli", "ahlaklı korsan" olarak bilinir ki, bu nevi korsanlar, bilişim sistem ve altyapılarının güvenliklerini test etmek ve değerlendirmek için korumalı sistemlere ve ağlara giren bir bilgisayar güvenlik uzmanıdır (Çıtak, 2018, s. 3). Beyaz-şapka Korsanları (iyi niyetli, ahlaklı), Siyah-şapka Korsanları olarak bilinen kötü niyetli bilgisayar korsanları onları tespit edip istismar etmeden önce güvenlik açıklarını açığa çıkararak, becerilerini bilişim sistem ve altyapılarının güvenliğini artırmak için kullanırlar. Ancak, bilgisayar korsanlarının dünyası yalnızca siyah-beyaz değildir (Kara, 2013). Ayrıca, üçüncü büyük grup olan Gri-şapkalı Korsanlar (Gray-Hat Hacker) da mevcuttur. Gri-şapkalı Korsan, etik standartları veya ilkeleri ihlal edebilen; ancak, Siyah-şapkalı Korsanlara atfedilen kötü amaç, niyet ve imajı olmayan kişidir. Gri-şapka Korsanları, genellikle kamu yararı için çalışırlar (Bülbül ve Bingöl, 2017).

Öte yandan, bilgisayar korsanları (hackers) bilgi ve becerilerine göre birkaç gruba ayrılabilir. En üst düzey, ne yaptığını tam olarak bilen, sisteme çok aşina olan ve virüsler ve diğer kötü amaçlı yazılımlar da dâhil olmak üzere uygun yazılımı oluşturabilen bilgisayar korsanlarından oluşur. Orta seviye, yazılım ve donanım pazarında satın alınabilecek araçları kullanabilen sözde "teknisyenler"den oluşur. Üçüncüsü, en düşük seviyedeki bilgisayar korsanları, sözde "senaryo çocukları"ndan oluşur (Altınkaynak, 2017).

3.2.2. Zararlı yazılımlar

Kötü amaçlı yazılım; "sistemin amaçlanan işlevini bozmak veya kasıtlı olarak zarar vermek için bir yazılım sistemine eklenen, değiştirilen veya kaldırılan herhangi bir kod" olarak tanımlanır. Kötü amaçlı yazılımın bilgi, para ve yaşam kaybına neden olabileceği gerçeği, teknolojik gelişmeler için büyük bir tehdit oluşturur. Kötü amaçlı yazılımın sınıflandırılması, programın yürütme

özelliklerine bağlıdır. Kötü amaçlı yazılım ayrıca yüküne, sistemi nasıl kullandığına veya sistemi nasıl savunmasız hale getirdiğine ve nasıl yayıldığına bağlı olarak sınıflandırılır (Sikorski & Honig, 2012).

Kötü amaçlı yazılımların en sık rastlanı olan "bilgisayar virüsleri", kendi kendini kopyalayan kötü amaçlı programlardır. Virüsler, yürütülebilir bir dosya olarak bulunur ve kendilerini diğer ana bilgisayar sistemlerine kopyalayarak yayılır. Virüsler, pasiftirler ve dosyalar veya medya dosyaları veya ağ dosyaları aracılığıyla aktarılmaları gerekir. Virüsler, kodun ne kadar karmaşık olduğuna bağlı olarak, kendisinin çoğaltılmış kopyalarını değiştirebilirler (Skoudis & Zeltser, 2004).

"Solucan", sistem güvenlik açıklarından yararlanarak ağ üzerinden yayılabilen, kendi kendini kopyalayan ve etkin bir kötü amaçlı programdır. İşletim sistemindeki veya yüklü yazılımdaki hedeflenen güvenlik açıklarını kullanır. Zararlı rutinler içerir; ancak, aktif taşıyıcılar olarak hizmet veren iletişim kanallarını açmak için kullanılabilir. Solucan, sürekli tarama yoluyla çok fazla bant genişliği ve işlem kaynağı tüketir ve ana bilgisayarı kararsız hale getirir ve bu da bazen sistemin çökmesine neden olabilir. Ayrıca, verileri çalarak, dosyaları silerek veya virüslü sistemin bir botnet'in parçası olmasına yol açabilecek bir bot oluşturarak, bilgisayarı etkilemek için yazılmış kod parçaları olan bir özel yazılım içerebilir (Koret & Bachaalany, 2015).

"Truva atı" ise bir program olup, indirildiğinde ve yürütüldüğünde ana bilgisayara kötü amaçlı rutinler veya dosyalar yerleştiren meşru bir yazılım olarak sunar. Çoğu durumda, Truva atı çalıştırıldığında sisteme bir virüs yükleyecektir. Kendi kendini kopyalayamaz ve etkinleştirmek için sistem operatörlerine güvenir. Bununla birlikte, daha sonra kendilerini ilgilendiren herhangi bir kötü amaçlı etkinliği gerçekleştirebilecek bir saldırgana uzaktan erişim sağlayabilir. Truva atı programları, kendilerine bağlı olan yüke bağlı olarak ana bilgisayarı farklı şekillerde etkiler ve genellikle sosyal mühendislik yoluyla yayılır (Sikorski & Honig, 2012).

"Casus yazılım", bilgisayarda kullanan kötü amaçlı bir programdır. Kullanıcı etkinliğini gözetlemek amacıyla işletim sistemidir. Bazen, virüslü

sistemdeki güvenlik ayarlarını değiştirmek için ağ bağlantılarına müdahale etmek gibi ek yeteneklere sahiptirler. Kendilerini meşru yazılımlara, Truva atlarına bağlayarak ve hatta bilinen yazılım açıklarından yararlanarak yayılırlar. Casus yazılım, kullanıcı davranışını izleyebilir, tuş vuruşlarını, internet kullanım alışkanlıklarını toplayabilir ve bilgileri program yazarının bilgisayarına gönderebilir (Aycock, 2011).

Reklam destekli yazılımların kısaltması olan "adware", özellikle web sitesi açılır reklamlarında görülen ve yazılımlar tarafından görüntülenen reklamları otomatik olarak iletir. Çoğu, reklam verenler tarafından gelir getirici araçlar olarak kullanılmak üzere tasarlanmıştır. Bazı reklam yazılımları, kullanıcı etkinliğini izleyebileceği ve kullanıcı bilgilerini çalabileceği için, bunu çok tehlikeli hale getiren casus yazılımlarla paketlenmiş olarak gelebilir (Thomas, 2015).

"Kök Kiti", bir sistemde algılamayı önlemek için bir dizi araç kullanan bir programdır. Araçlar çok gelişmiş ve karmaşık programlar olup, virüslü bilgisayardaki yasal süreçler içinde saklanmak için yazılmıştır, bu nedenle çok istilacıdır ve kaldırılması zordur. Sistemin tam kontrolünü ele alma ve diğer olası kötü niyetli faaliyetler arasında makinede mümkün olan en yüksek ayrıcalıkları kazanma yeteneği ile tasarlanmıştır. Kök kitler tarafından kullanılan kaçınma teknikleri nedeniyle, güvenlik sağlayıcı çözümlerinin çoğu bunları algılamada ve kaldırmada etkili değildir ve bu nedenle, bunların algılanması ve kaldırılması büyük ölçüde manuel çabalara dayanır. Bunlar, anormal faaliyetler için bilgisayar sistem davranışını izleme, depolama dökümü analizi ve sistem dosyası imza taramasını içerebilir; ancak, bunlarla sınırlı değildir (Namanya vd., 2018).

3.2.3. Gizli-arka kapılar

Arka kapı saldırıları, rakibin bir tetikleyici (küçük bir yama) seçtiği, tetikleyiciye dayalı olarak bazı zehirli veriler geliştirdiği ve kurbana derin bir modeli eğitmesi için sağladığı farklı bir saldırı türüdür. Eğitimli derin model, düzenli temiz veriler üzerinde doğru sonuçlar üretecek ve böylece kurban, modelin güvenliğinin ihlal edildiğini fark etmeyecektir. Ancak, saldırgan tetikleyiciyi kaynak görüntüye yapıştırdığında model, bir kaynak kategori

görüntüsünü hedef kategori olarak yanlış sınıflandırır. Buna popüler bir örnek olarak, tetikleyici, tahmini "dur işareti"nden "hız sınırı"na değiştiren bir trafik işareti üzerindeki küçük bir çıkartma olabilir (Russakovsky vd., 2015).

Önceden eğitilmiş bir modelin küçük eğitim verilerini kullanarak diğer görevlere kolayca aktarılabileceği gösterilmiştir. Örneğin, ImageNet üzerinde önceden eğitilmiş bir derin modeli indirmek ve aynı zamanda eldeki sorunu çözmek için modele ince ayar yapmak için bazı ilgi çekici görüntüleri web'den indirmek yaygın bir uygulamadır. Arka kapı saldırıları, bu tür uygulamalarda etkilidir; zira saldırgan, kurbanların indirip eğitimde kullanması için web üzerinde bazı zehirli veriler bırakabilir. Büyük veri ortamında olduğu gibi bu tür saldırıları azaltmak kolay değildir, tüm verilerin güvenilir kaynaklardan toplandığından emin olmak zordur (Saha vd., 2020).

En iyi bilinen arka kapı saldırısı, tetikleyiciyi kaynak verilere yapıştırarak ve etiketlerini hedef kategoriye değiştirerek zehirli veriler geliştirir. Ardından, ince ayar sırasında model, tetikleyiciyi hedef kategoriyle ilişkilendirir ve test zamanında, tetikleyici kaynak kategoriden bir görüntü üzerinde saldırgan tarafından sunulduğunda model hedef kategoriyi tahmin eder. Bununla birlikte, kurban yanlış etiketi veya küçük tetikleyiciyi bulmak için görüntüleri görsel olarak inceleyerek onları tanımlayabileceğinden, bu tür saldırılar çok pratik değildir (Russakovsky vd., 2015).

3.2.4. Kimlik avı (yemleme)

"Kimlik avı" kelimesi aslında, ilk internet suçlularının, büyük bir şüphelenmeyen internet kullanıcıları denizinden şifreler ve finansal veriler için "balık tutmak" için yemler kullanma benzetmesinden gelmiştir. Kimlik avı, hedeflenen kişiyle, yasal bir kurum gibi davranan biri tarafından, banka bilgileri, kredi kartı bilgileri ve şifreler gibi hassas bilgileri sağlamaya ikna etmek için e-posta veya telefon yoluyla iletişime geçilmesi sürecini ifade eder (Syiemlieh vd., 2015).

Kişisel bilgiler daha sonra kişinin hesabına erişmek için kullanılır ve kimlik hırsızlığına ve mali kayıplara neden olabilir. Kimlik avı, yanlış bir şekilde meşru bir kuruluştan geldiğini iddia eden e-posta gönderme eylemidir.

Genellikle bir hesabın kapanması, bir bakiyenin ödenmesi veya bir hesapta bilgi olmaması gibi bir tehdit veya bilgi talebi ile birleştirilir. E-posta, alıcıdan banka hesap bilgileri, PIN'ler veya şifreler gibi gizli bilgileri vermesini isteyecektir; bu ayrıntılar daha sonra web sitesinin sahipleri tarafından dolandırıcılık yapmak için kullanılır. Ayrıca, bir takma adla güvenliği atlama veya tuzağa düşürme eylemi olarak da tanımlanabilir (Syiemlieh vd., 2015).

Kimlik avı kelimesinin kendi başına birçok anlamı vardır, bazıları bunun bir marka sahtekârlığı, taraklama, pharming, dolandırıcılık saldırısı, anlamsal saldırı olduğunu söyler; ancak sonuçta, kimlik avcısının hedefinin kurbanları kandırmayı başarmrak olduğu aynı anlama gelir. Şifrelerini veya hesap numaralarını ya da kimlik avcısı için faydalı olacak her türlü kişisel bilgiyi vermektir (Cranor vd., 2016).

Cranor ve arkadaşlarına (2016) göre, kimlik avı semantik bir saldırı olarak tanımlanmıştır. Kurbanların kişisel bilgilerini yasa dışı bir siteye vermeleri için kandırıldığı yerdir. Sitenin yasal olup olmadığı konusunda kesin sonuçlar verecek araç çubukları oluşturularak buna bir çözüm getirilmiştir. Pek çok türde kimlik avı önleme araç çubuğu geliştirilmiştir ve bunlar aşağıdaki gibidir (ss. 4-5):

- Cloudmark Dolandırıcılıkla Mücadele Araç Çubuğu,
- Yer Bağlantısı Araç Çubuğu,
- eBay Araç Çubuğu,
- GeoTrustTrustWatch Araç Çubuğu.

Kimlik avı, kurbanlardan çalarak milyonlarca dolar kazandırdığından ve çoğunlukla Doğu Avrupa, Asya, Afrika ve Orta Doğu'da bu tiksindirici dolandırıcılığın birçok grubu olduğu için, kimlik avı bir iş haline gelmiştir. Saldırganların kullanıcıları yenilikçi fikirleriyle dolandırmak için yeni yollar ve araçlar bulduğu ve sitelerini daha iyi göstermek için piyasada ortaya çıkan en son teknolojilerle kendilerini güncellediği son birkaç yılda gelişen farklı kimlik avı türleri vardır (Henkoğlu, 2014).

Bunlardan aldatıcı Kimlik Avı, kullanıcının yanlış yönlendirilmesine ve doğru olmayana inanmasına neden olur. Saldırgan, kullanıcıya finansal hesapları ve karşılaştıkları sorunlar hakkında farkında olmadığı bir e-posta göndererek, şifrelerini ve diğer kişisel bilgilerini güncellemesi için bir bağlantı göndererek ilerler ve bundan sonra kullanıcıdan aldığı bilgilerle kullanıcının finansal hesaplarına sızıp kendi amaç ve çıkarları için istismar edebilir (Syiemlieh vd., 2015).

Kötü Amaçlı Yazılım Tabanlı Kimlik Avı, özellikle yazılımın uzun süre güncellenmediği küçük bir firmada kullanılan bir yazılım ise, kullanıcının yazılımına zarar verecektir. Saldırgan bunu yaparak hiçbir şey kazanmaz, yalnızca başkalarının acı çekmesini izleme arzusunu yerine getirir, genellikle kötü niyetli bir suç olarak adlandırılır. Keyloggerlar ve Screenloggers, saldırganın klavyeden girişleri takip ettiği ve ilgili bilgileri internet üzerinden diğer bilgisayar korsanına göndereceği bir kötü amaçlı yazılım saldırısıdır. Hijacking ise, saldırganın kullanıcının sistemini takip ettiği ve her şeyin izlendiği bir tür kötü amaçlı yazılım saldırısıdır, böylece kullanıcı banka bilgilerine veya saldırgan için yararlı olan diğer bilgilere giriş yaptığında saldırgan tarafından ele geçirilir (Çıtak, 2018).

3.2.5. Scanning (tarama) yöntemi ve şifre kırıcılar

Tarama saldırılarında saldırganlar, güvenliğini zayıflatmak için karmaşık saldırılar başlatmadan önce bu cihazların ağ bilgilerini toplamak için cihazları tarar. Bilgisayar ağı bilgilerini toplamak için yaygın olarak kullanılan tarama teknikleri arasında IP adresi taraması, bağlantı noktası taraması ve sürüm taraması bulunur (Alioğlu, 2019).

Bağlantı noktası taraması, saldırganların bir ana bilgisayardaki belirli bağlantı noktalarına paketler göndererek ve güvenlik açıklarını bulmak ve bir ana bilgisayarda hangi hizmetlerin ve hizmet sürümlerinin çalıştığını anlamak için yanıtları kullanarak hedef ortamlarının kapsamını belirlemek için kullandıkları bir yöntemdir. İlk olarak, saldırganların ağdaki ana bilgisayarları bulmaları gerekir; ardından saldırganlar, bu ana bilgisayarları amaçlarına hizmet edebilecek bağlantı noktaları için tarayabilir. Genel olarak, bağlantı noktası

taraması, bağlantı noktalarını üç kategoriden birinde sınıflandırmaya çalışır (Benzer, 2014).

Şifre kırma, bilgisayar parolalarını keşfetmek için kullanılan çeşitli önlemleri ifade eder. Bu genellikle, bir bilgisayar sisteminde depolanan veya bir bilgisayar sisteminden taşınan verilerden parolaların kurtarılmasıyla gerçekleştirilir. Şifre kırma, parolayı tekrar tekrar tahmin ederek, genellikle sistemin giriş şifresi başarıyla keşfedilene kadar sayısız kombinasyon denediği bir bilgisayar algoritması aracılığıyla yapılır. Şifre kırma çeşitli nedenlerle yapılabilir; ancak en kötü neden, bilgisayar sahibinin haberi olmadan bir bilgisayara yetkisiz erişim elde etmektir. Bu kötü girişimler, genellikle kullanıcının bankacılık bilgilerine erişmek amacıyla şifrelerinin çalınması gibi siber suçlarla sonuçlanır (Alioğlu, 2019).

3.2.6. Servis dışı bırakma saldırıları

"Servis Dışı Bırakma", bir makineyi veya ağı kapatarak hedeflenen kullanıcılar tarafından erişilemez hale getirme amaçlı bir saldırıdır. DoS (Denial-of-service attack) saldırıları olarak da bilinen Servis Dışı Bırakma saldırıları, hedefi trafikle doldurarak veya bir çökmeyi tetikleyen bilgiler göndererek bunu başarır. Her iki durumda da Servis Dışı Bırakma saldırısı meşru kullanıcıları bekledikleri hizmet veya kaynaktan mahrum bırakma amacı güder (Guirguis vd., 2005).

Servis Dışı Bırakma saldırılarının kurbanları genellikle bankacılık, ticaret ve medya şirketleri gibi yüksek profilli kuruluşların veya devlet ve ticaret kuruluşlarının web sunucularını hedef alır. Servis Dışı Bırakma saldırıları tipik olarak önemli bilgilerin veya diğer varlıkların çalınması veya kaybolması ile sonuçlanmasa da kurbana işlemesi çok fazla zaman ve maliyet kaybına yol açabilir. Servis Dışı Bırakma saldırılarının iki genel yöntemi bulunmakta olup, bunlar, hizmetleri taşırma veya hizmetleri çökertmedir. Flood saldırıları, sistem sunucunun arabelleğe alması için çok fazla trafik aldığında meydana gelir ve bu da sunucunun yavaşlamasına ve sonunda durmasına neden olur (Kuzmanovic & Knightly, 2003).

Arabellek taşması saldırıları, en yaygın servis dışı bırakma saldırısıdır. Bu saldırılarda ana konsept, bir ağ adresine, programcıların sistemi işlemek için oluşturduğundan daha fazla trafik göndermektir. Arabellek taşması saldırıları, yukarıda belirtilen ve belirli uygulamalara veya ağlara özgü hatalardan yararlanmak için tasarlanmış diğer saldırı türlerine ilave olarak, daha farklı türde saldırı teknikleri de içermektedir. Bu bağlamda, İnternet Kontrol Mesajı Protokolü [Internet Control Message Protocol (ICMP)] taşması saldırısı, yalnızca belirli bir makine yerine hedeflenen ağdaki her bilgisayara ping gönderen sahte paketler göndererek yanlış yapılandırılmış ağ cihazlarından yararlanır. Ağ daha sonra trafiği yükseltmek için tetiklenir. Bu saldırı aynı zamanda smurf saldırısı veya ölümün pingi olarak da bilinir. SYN taşması (SYN Flood) saldırısı ise, bir sunucuya bağlanmak için bir istek gönderir; ancak, el sıkışmayı asla tamamlamaz. Tüm açık bağlantı noktaları isteklerle dolana ve meşru kullanıcıların bağlanabileceği hiçbir bağlantı kalmayana kadar devam eder (Alioğlu, 2019).

3.2.7. Sahte (fake)-istemdışı alınan (spam)

İstenmeyen ve ilgisiz içeriği yayma eylemi olan spam gönderme, e-posta, anlık mesajlaşma, web sayfaları, internet ortamı vb. gibi birçok farklı alanda gözlemlenmiştir. En yaygın olarak tanınan spam biçimi e-posta spam'ıdır. Ancak "spam" terimi, diğer medya ve ortamlardaki benzer suistimalleri tanımlamak için kullanılır. Spam, tamamı büyük ölçüde aynı içeriğe sahip olan, daha büyük bir ileti koleksiyonunun parçası olarak gönderilen veya yayınlanan bir veya daha fazla istenmeyen iletidir (Abdoh vd., 2009).

Sahte e-postaların gönderilmesindeki amaç, hedef kullanıcının e-posta şifresini kontrol altına almak olup, bu saldırı türünde öncelikle e-posta şifresi ele geçirilmek istenen kullanıcıya sanki e-posta hizmeti aldığı Mynet, Gmail, Hotmail, Yahoo ve benzeri internet hizmet sağlayıcısından geliyormuş gibi bir e-posta gönderilmektedir. Kullanıcı, yine sahte hazırlanmış bir internet adresinden gönderilen sahte e-postayı yanıtlamak amacıyla yönlendirilir ve hedef kullanıcı adını ve şifresini girdiğinde, kullanıcının bilgileri üçüncü kişilerin eline geçmektedir (Abdoh vd., 2009).

3.2.8. Klavye kaydediciler

Keylogger, sinsi bir casus yazılım biçimidir. Kimsenin izlemediğine inanarak hassas verileri klavyenize girersiniz. Aslında, keylogging yazılımı, yazdığınız her şeyi günlüğe kaydetmek için çok uğraşır. Keylogger'lar, bilgisayar korsanlarının kişisel verilerinize erişmesini sağlayan etkinlik izleme yazılım programlarıdır. Keylogger, bir bilgisayar kullanıcısının bir bilgisayarla etkileşime girerken etkinliğini kaydedebilen ve raporlayabilen bir araçtır. Ad, tuş vuruşu kaydedicisinin kısa bir versiyonudur ve tuş kaydedicilerin sizi takip etmesinin ana yollarından biri, yazarken yazdıklarınızı kaydetmektir. Ancak görüleceği gibi, farklı türde keylogger'lar vardır ve bazıları daha geniş bir girdi aralığı kaydeder. Tuş vuruşu kaydı için kullanılan ekipman tuş kaydedici, ATM PIN'i, oturum açma gizli anahtarı ve benzerlerini içeren kazazedenin tuş vuruşlarını kaydetmek için bir tekniktir (Umarani & Sengupta, 2020).

Ekipman keylogger'ı ve programlama keylogger'ı olmak üzere iki tür keylogger vardır. BIOS düzeyindeki bellenim tarafından gerçekleştirilebilir veya bir bilgisayar konsolları ile bir bilgisayar arasındaki aygıt bağlantılı bir hat aracılığıyla kullanılabilirler. Programlama tuş kaydedicileri, nesnel çalışma çerçevesi içindeki tuş vuruşlarını ve bilgileri günlüğe kaydeder ve görüntüler, bunları sabit çemberde veya uzak alanlarda saklar ve saldırgana gönderir. Programlama keylogger gözlemleme çoğunlukla çalışma sistemine bağlıdır (Akarslan, 2015).

Keylogger, bir müşterinin konsol vuruşlarının tamamını yakalamayı ve daha sonra bunları bir müşteriyi para alışverişinde taklit etmek için kullanmayı amaçlayan bir üründür. Bu tür keylogger'ların tehlikesi kaçınılmazdır ve hem PC'lerde hem de halka açık stantlarda bulunabilir. Programlama tabanlı tam daire şifrelemede en kırılgan bağlantı, günümüzde onay sistemidir. İşin en korkunç yanı, düzenli olarak root'lanan keylogger'ları, ayak işleri direktörü ölçü listesinde görünmeyeceklerinden ayırt etmenin zor olmasıdır (Nyang vd., 2015).

Keylogger saldırısını hafifletmek için, düzensiz konsol eylem planlarına sahip sanal veya ekran konsolları genellikle tarafından ve tarafından kullanılır. İki strateji, harfleri rastgele sırayla değiştirerek basit tuş kaydedicileri

şaşırtabilir. Trajik bir şekilde, tüm PC üzerinde güce sahip olan keylogger, her işlevi çok fazla zorlamadan yakalayabilir ve enstantaneler ile yeni harf seti arasında bir planlama yapmak için video yastığını okuyabilir. Diğer bir hafifletme prosedürü, konsolun vektör tablosu ile karışmasını rahatsız ederek konsol snaring tahmin yöntemini kullanmaktır (Umarani ve Sengupta, 2020).

3.2.9. Ip aldatması

IP sahtekârlığı, gönderenin kimliğini gizlemek, başka bir bilgisayar sisteminin kimliğine bürünmek veya her ikisini birden yapmak için değiştirilmiş bir kaynak adresine sahip İnternet Protokolü (IP) paketlerinin oluşturulmasıdır. Genellikle kötü aktörler tarafından bir hedef cihaza veya çevresindeki altyapıya Dağıtılmış Hizmet Reddi (Distributed Denial of Service-DDoS) saldırıları başlatmak için kullanılan bir tekniktir. IP paketlerinin gönderilmesi ve alınması, ağa bağlı bilgisayarların ve diğer cihazların iletişim kurmasının birincil yoludur ve modern internetin temelini oluşturur. Tüm IP paketleri, paketin gövdesinden önce gelen ve kaynak adresi de dâhil olmak üzere önemli yönlendirme bilgilerini içeren bir başlık içerir. Normal bir pakette kaynak IP adresi, paketi gönderenin adresidir. Paket sahteyse, kaynak adres sahte olacaktır (Vlajic vd., 2019).

Bilgisayarlara yetkisiz erişim sağlamak için kullanılan, davetsiz misafirin, mesajın güvenilir bir ana bilgisayardan geldiğini belirten bir IP adresine sahip bir bilgisayara mesajlar gönderdiği bir tekniktir. Bir bilgisayar korsanı, IP sahtekârlığına girişmek için önce güvenilir bir ana bilgisayarın IP adresini bulmak için çeşitli teknikler kullanarak ve ardından paket başlıklarını, paketlerin o ana bilgisayardan geliyormuş gibi görünecek şekilde değiştirmektedir. IP sahtekârlığının diğer bir yaygın kullanımı, IP adresi veya bölgeye dayalı kullanıcı kimlik doğrulamasının atlanmasıdır. Örneğin, birçok şirket bir intranet kullanır. Bu intranetteki tüm içeriğe erişmek için, erişim talep eden makinelerin, güvenilir bir makine olarak tanındığını veya makineye güvenilir bir konumdan erişildiğini gösteren belirli bir geçerli aralık içinde bir IP adresine sahip olması gerekir (De Donno, 2019).

IP Spoofing, bir saldırganın yanlış iade adresi listelenen birine paket göndermesine benzemektedir. Paketi alan kişi, gönderenin paket göndermesini

durdurmak istiyorsa, iade adresi kolayca değiştirilebileceği için tüm paketleri sahte adresten engellemek pek bir işe yaramayacaktır. Buna bağlı olarak, alıcı iade adresine cevap vermek isterse, cevap paketi gerçek göndericiden başka bir yere gidecektir. Paket adreslerini taklit etme yeteneği, birçok DDoS saldırısı tarafından kullanılan temel bir güvenlik açığıdır (Vlajic vd., 2019).

DDoS saldırıları, kötü niyetli kaynağın kimliğini maskeleyerek, azaltma çabalarını önleyerek bir hedefi trafiğe boğmak amacıyla genellikle kimlik sahtekârlığını kullanır. Kaynak IP adresi tahrif edilirse ve sürekli rastgele seçilirse, kötü niyetli isteklerin engellenmesi zorlaşır. IP sahtekârlığı, kolluk kuvvetleri ve siber güvenlik ekiplerinin saldırının failini bulmasını da zorlaştırır (De Donno, 2019).

3.2.10. SQL Injection (enjeksiyon) yöntemi

Web uygulamalarına yönelik birçok saldırı türü arasında SQL Enjeksiyon Saldırısı (SQLIA), bunlara yönelik en büyük tehditlerden biridir. SQL olarak da bilinen SQL enjeksiyonu, görüntülenmesi amaçlanmayan bilgilere erişmek için arka uç veritabanı manipülasyonu için kötü amaçlı SQL kodu kullanan yaygın bir saldırı vektörüdür. Bu bilgiler, hassas şirket verileri, kullanıcı listeleri veya özel müşteri ayrıntıları dâhil olmak üzere herhangi bir sayıda öğeyi içerebilmektedir. SQL enjeksiyonunun bir işletme üzerindeki etkisi geniş kapsamlıdır. Başarılı bir saldırı, kullanıcı listelerinin yetkisiz olarak görüntülenmesine, tüm tabloların silinmesine ve bazı durumlarda saldırganın bir veri tabanı üzerinde yönetici hakları kazanmasına neden olabilmektedir ve bunların tümü bir işletme için son derece zararlıdır (Halfond vd., 2006).

SQL Injection, arka uç veritabanı kullanan web uygulamalarını hedefler. Tipik bir web uygulamasının çalışması şu şekildedir: Kullanıcı; kullanıcı adı, şifre, hesap numarası vb. bazı parametreler olabilecek web tarayıcıları aracılığıyla istek gönderir. Bunlar daha sonra arka uç veritabanından gerekli verileri almak için bazı dinamik SQL sorgularının oluşturulduğu web uygulama programına iletilir (Halfond & Orso, 2006).

SQL Injection saldırısı, özel hazırlanmış kullanıcı girdileri aracılığıyla başlatılır. Diğer deyişle saldırganların normal kullanıcılar gibi istek vermesine

izin verilir. Daha sonra kasıtlı olarak web uygulama koduna iletilen bazı hatalı giriş kalıpları oluştururlar. Uygulama SQL Injectiona karşı savunmasızsa, özel olarak oluşturulan bu girdi, arka uç veritabanında yürütülen SQL sorgusunun amaçlanan yapısını değiştirecek ve veritabanında depolanan bilgilerin güvenliğini etkileyecektir. Sorgu yapısını değiştirme eğilimi, SQL Injection'nun önlenmesi için de kullanılan en karakteristik özelliğidir (Halfond vd., 2006).

3.2.11. Siber casusluk ve istihbarat saldırıları

Devletler arasındaki casusluk, çok eski çağlara dayanan bir olgudur; ancak, son birkaç on yılda dünya tamamen yeni bir casusluk alanı ile tanışmıştır. Bu alan, siber casusluk dünyasıdır. Bu yeni casusluk biçimi, devletler arasındaki ekonomik ve siyasi ilişkileri etkilediği gibi modern savaşın şeklini de değiştirmektedir. Bu nedenle, modern teknolojinin getirdiği avantajlara rağmen, yepyeni birtakım sorunlar da vardır. Siber savaşla ilgili en zor sorunlardan biri siber casusluğu tanımlamaktır. Birçok ülke ve uluslararası kuruluş kendi tanımlarını oluşturmuştur, ancak bunu tek bir fikir birliğine indirgemek zor olmuştur. Saldırının neden olduğu hasarın kapsamı ve niteliği, saldırıların kimliği ve çalınan bilgilerin nasıl kullanıldığı gibi faktörlerin tümü, siber casusluğun nasıl algılandığını etkilemektedir (Rubenstein, 2014).

Siber casusluk hem bir tehdit hem de bir güdü olarak kabul edilir ve "Genellikle bir hükümet veya başka bir kuruluş tarafından tutulan gizli bilgilere yasadışı erişim sağlamak için bilgisayar ağlarının kullanılması" olarak tanımlanmaktadır. Siber casusluk veya siber istihbarat, yetkisiz bir kullanıcının ekonomik kazanç, rekabet avantajı veya siyasi nedenlerle hassas veya sınıflandırılmış verilere veya fikri mülkiyete (IP) erişmeye çalıştığı bir tür siber saldırıdır (Schmitt, 2013).

Siber casusluk öncelikle, saldırgan tarafından rekabet avantajı yaratmak için kullanılabilecek veya finansal kazanç için satılabilecek hassas veya sınıflandırılmış verileri, ticari sırları veya diğer fikri mülkiyet biçimlerini toplamak için bir araç olarak kullanılır. Bazı durumlarda, ihlalin amacı, özel bilgileri veya şüpheli ticari uygulamaları ifşa ederek mağdurun itibarına zarar vermektir (Baker, 2012).

Siber casusluk, siber saldırı ve siber savaş arasında ayrım yapan Russinovich'e (2014) göre siber casusluk bilgi toplama veya fikri mülkiyet hırsızlığı anlamına gelirken, bir siber saldırı bilgisayar ağının işlevini baltalar ve siyasi veya ulusal güvenlik amacına ve siber savaşa sahiptir. Sadece devlet aktörlerini içerir, aynı zamanda bilgisayar ağının işlevini baltalar, siyasi veya ulusal güvenlik amaçlıdır ve silahlı saldırıya eşdeğerdir veya silahlı çatışma bağlamındadır.

NATO'nun 2013 yılında yayınladığı el kitabında siber casusluk; "gizli olarak veya sahte iddialar altında siber yetenekleri kullanarak bilgi toplamak amacıyla kullanılan bir eylem" olarak tanımlamaktadır. Çoğu insan siber casusluğu özellikle gizli bilgileri kötü amaçlı amaçlarla hedef almak olarak nitelendirse de bu tanım saldırının amacını veya çalınan bilgilerin niteliğini ele almamaktadır (Akt. Schmitt, 2013).

Bu gereksiz yere belirsiz görünebilir; ancak, uluslararası hukuk açısından bu tanım uygun olmaktadır. En azından, yabancı siber saldırıların kurbanı olan ülkeler için daha faydalıdır. Modern dünyada devletlerin siber saldırılara karşı kendilerini savunmasını zorlaştıran teknik engeller değil, daha çok yasal ve politik engellerdir. Bu nedenle, NATO'nun el kitabında verilene benzer her şeyi kapsayan bir siber casusluk tanımı önemlidir; zira bu, kurban ülkelerin en ufak bir izinsiz giriş için bile uygun karşı önlemleri almalarına olanak tanımaktadır (Schmitt, 2013).

Siber casusluk saldırıları parasal kazançla motive edilebilir; ayrıca askeri operasyonlarla bağlantılı olarak veya siber terörizm veya siber savaş eylemi olarak da konuşlandırılabilmektedir. Siber casusluğun etkisi, özellikle daha geniş bir askeri veya siyasi kampanyanın parçası olduğunda, kamu hizmetlerinin ve altyapısının bozulmasına ve ayrıca can kaybına yol açabilmektedir (Baker, 2012).

Günümüzde devletlerin birçok farklı türde siber casusluk aracı kullandıkları görülmektedir. Bunların birçoğu, kişinin kendi ev bilgisayarına karşı görebileceği, çok daha büyük bir ölçekte uygulanan saldırılardan farklı değildir. Birincisi, esas olarak kurban olan devletin iletişim sistemlerini bozmak

için kullanılan DDoS saldırılarıdır. DDoS saldırıları tercih edilir; zira bir saldırgan bunları daha büyük ve daha güçlü bir kurbana karşı çok sınırlı kaynaklarla uygulayabilmektedir (Rubenstein, 2014).

Virüsler, solucanlar ve Truva atları gibi kötü amaçlı yazılımlar da normal bilgisayar işlemlerini bozmak, gizlice veri toplamak veya verileri tamamen yok etmek için kullanılan popüler araçlardır. Diğer saldırı türleri arasında, belirli bir zamana veya belirli bir olay tarafından tetiklenene kadar uykuda kalmak üzere tasarlanmış kötü amaçlı yazılımlar olan "Mantık Bombaları" ve bir saldırganın özel bilgilere veya güvenli bilgilere erişmek için kendini gizlemeyi başardığı IP Spoofing yer almaktadır (Rubenstein, 2014, s. 4).

Bu saldırılar, aslında yaygın saldırı türleri olsa da, savaşan devletler tarafından büyük çapta gerçekleştirildiği takdirde yıkıcıdır. Ayrıca, dijital teknoloji siber casusluğu beklenmedik şekillerde etkilemektedir. Fotoğraf ve video manipülasyonundaki ilerlemeler nedeniyle, bir saldırgan kurbanının ağlarına erişim sağladığında, saldırgan kurbanın gördüklerini gerçek zamanlı olarak manipüle edebilmekte, böylece diğer ulusun karşı istihbaratının güvenilirliğini tehlikeye atabilmektedir (Watney, 2015).

Siber casusluğun en yaygın hedefleri arasında, başka bir kuruluş veya hükümet için rekabet avantajı yaratabilecek değerli IP ve teknik verilere sahip büyük şirketler, devlet kurumları, akademik kurumlar, düşünce kuruluşları veya diğer kuruluşlar bulunur. Hedefe yönelik kampanyalar, önde gelen siyasi liderler ve hükümet yetkilileri, şirket yöneticileri ve hatta ünlüler gibi kişilere karşı da yürütülebilmektedir (Nakashima, 2013).

Siber casusluk, özellikle devletler tarafından organize edildiğinde ve yürütüldüğünde, büyüyen bir güvenlik tehdidi̇dir. Bu tür faaliyetleri engellemeye yönelik bir dizi iddianame ve mevzuata rağmen, suçluların çoğu, ülkeler arasında suçluların iadesi anlaşmalarının olmaması ve bu konuyla ilgili uluslararası hukukun uygulanmasının zorluğu nedeniyle hala serbest durumdadır (Baker, 2012).

Günlük internet kullanımının çoğu için, uluslararası siber casusluğun gizli dünyası, gerçek bir önem taşıyamayacak kadar uzak görünebilir. Bireysel

vatandaşların çoğuna, siber casusluk hayatlarını çok fazla etkilemiyor gibi görünebilir, ancak bir devlet üzerindeki maliyetleri önemlidir. Etki, parasal kayıptan fiziksel altyapı hasarına ve sivil kayıplara kadar önemli ölçüde değişebilir ve maliyet önemsizden yıkıcıya kadar değişebilir (Rubenstein, 2014).

Siber casuslukla ilişkili maliyetin miktarı ve türü değişebilse de aşırı durumlarda çok yüksek olabilir. Siber saldırılar, Rusya'nın tercih ettiği stratejide olduğu gibi gerçek savaşla birleştiğinde, iletişim sistemlerinin kaybı, kurban ülkenin kendisini ve vatandaşlarını savunma yeteneğini ciddi şekilde kısıtlayabilir. Bu durumda böyle bir saldırı mülk, altyapı ve insan hayatı kaybına neden olur. Rusya bu stratejiyi Estonya, Gürcistan ve Ukrayna üzerinde kullandığında, üç kurban ülke kendilerini savunma veya dış dünyaya ulaşma ve itiraz etme yeteneklerinin çoğunu kaybetti. (Rubenstein, 2014).

Bu sorun, siber suçluların ve bilgisayar korsanlarının artan karmaşıklığıyla birleştiğinde, elektrik şebekesinin işletilmesinden finans piyasalarına ve büyük seçimlere kadar herhangi bir sayıda modern hizmetin kesintiye uğramasına neden olabilecek koordineli ve gelişmiş bir saldırı olasılığını açık bırakmaktadır (Nakashima, 2013).

3.3. Siber Güvenlik

Siber uzayın ortaya çıkışı, devletlerin hem kullanıcıları hem de ulusal güvenlikten sorumlu resmi kurum ve kuruluşları için birçok yeni güvenlik sorununu beraberinde getirmiştir. Siber saldırganlar, finansal kurumları hedef alarak, ulusal sırlara erişerek ve sızdırarak ve İran nükleer tesislerine karşı Stuxnet solucanı da dâhil olmak üzere birçok örneğin gösterdiği gibi, ulusal altyapıya kinetik bir saldırıya benzer gerçek fiziksel hasara neden olarak hasara yol açma potansiyeline sahiptir. Saldırganlar nadiren iz bıraktıklarından ve aslında kökenlerini gizlemeye çalıştıkları için siber saldırıların atfedilmesi daha zordur. Çoğu durumda, siber saldırganlar pahalı ve nadir ekipmanlara ihtiyaç duymazlar; bu, genel kamunun bilgi teknolojilerine (BT) erişiminin artmaya devam etmesi ve BT'nin hem kamu hem de özel sektör yönetimindeki rolünün artması ve böylece daha fazla güvenlik açığı yaratması gerçeğiyle

desteklenmektedir. Bu bağlamda siber güvenlik ve siber savunma, esas olarak siber casusluğun artması ve söz konusu internet tabanlı tehditler nedeniyle hükümetlerin savunma gündemlerinde öncelik haline gelen iki alandır (Bıçakçı, 2019).

Donanım, yazılım ve veriler dâhil olmak üzere internete bağlı sistemler tarafından siber saldırılara karşı korunmaktadır. Bilgi işlem bağlamında güvenlik, siber güvenliği içerir ve fiziksel güvenliğin her ikisi de işletmeler tarafından veri merkezlerine ve diğer bilgisayarlı sistemlere yetkisiz erişime karşı güvenlik sağlamak için kullanılır. Verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için tasarlanan güvenlik, siber güvenliğin bir alt kümesidir. Siber güvenlik operasyonları, bilgi ve sistemleri büyük siber tehditlerden korumayı içerir (Korkmazer, 2013).

Dünyanın birçok yerindeki toplumlar, temel hizmetlerin sağlanması için dijital teknolojilerin kesintisiz çalışmasına güvenmektedir. Bu bağımlılık yeni güvenlik endişelerini beraberinde getirmiştir. Sonuç olarak, dijital teknolojilerin rutin işleyişinin aksaması olarak anlaşılan siber olaylar, devlet aktörlerinin yeni tehdide karşı yeterli cevaplar bulmaya çalışmasıyla ulusal ve uluslararası güvenlik politikasında önemli bir yer edinmiştir (Collier, 2018).

"Siber güvenlik" terimi, konuya büyük ölçüde belirli bir perspektiften bakan akademik ve popüler literatürün konusu olmuştur. Amoroso'a (2006) göre siber güvenlik, yazılımlara, bilgisayarlara ve ağlara yönelik kötü niyetli saldırı riskini azaltmayı içerir. Buna, izinsiz girişleri tespit etmek, virüs kullanımlarını durdurmak, kötü niyetli erişimi engellemek, kimlik doğrulamasını uygulamak, şifreli iletişimleri etkinleştirmek ve devam etmek için kullanılan araçlar dâhildir (Rubenstein, 2014).

ITU-Uluslararası Telekomünikasyon Birliği'nin (2011) tanımına göre siber güvenlik, siber ortamı ve organizasyonu ve kullanıcı varlıklarını korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplamıdır (ITU, 2011).

Canongia ve Mandarino'ya (2014) göre siber güvenlik, bir ulusun bilgi toplumunun varlığını ve devamlılığını sağlama, siber uzayda bilgi, varlık ve kritik altyapısını garanti altına alma ve koruma sanatıdır.

Siber güvenlik kavramı, Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı'nda; "Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi" biçiminde tanımlanmıştır (Akt. Alioğlu, 2019).

Siber güvenlik, uluslararası ilişkilerde çok önemli bir rol oynamaktadır ve hükümet politikasında önemli bir unsur olmaya devam edecektir. Siber güvenlik önlemleri, sistemin aşılmaz ve sağlam olması nedeniyle siber saldırıları önleyen güvenli bir sistem tasarlamayı içerir. Uluslararası ilişkilerde kullanılan benzer stratejiler, yıldırma aracı olarak caydırıcılık gibi siber güvenlik önlemleri için de geçerlidir. Birçok şirket ve kuruluş, ekonomiyi desteklemek için işlerini çevrimiçi ortama taşıdıkça, ağları, kendi çıkarları için sisteme sızmak isteyen siber suçlular için risk altındadır. Siber saldırılar, bireyleri, işletmeleri ve hükümetleri tehdit eden daha gelişmiş saldırılardır. Siber suçun tüm ağlarda ve sistemlerde sahip olduğu geniş etki nedeniyle, doğal olarak dünya liderleri bu sorunla mücadele etmek zorundadır (Kshetri, 2014).

Siber güvenlik, teknolojinin uluslararası güvenlik üzerindeki etkisine ilişkin görüşmelerde politika danışmanlarıyla birlikte her hükümetin savunma politikasında ayrılmaz bir rol oynar. Her işletmenin, işverenlerin uyması için iyi yapılandırılmış bir siber güvenlik politikası ve en iyi uygulamalar kılavuzu ile birlikte siber güvenlik önlemlerine sahip olması gerekir. Dünya, günlük yaşamlarını sürdürmek için çevrimiçi hizmetlere bağımlı olmaya devam ederken, işletmeler müşterilerini korumaktan sorumlu tutuluyor. Bunun, uluslararası iş birliğinin artmasına yol açan siber suçları önlemek için birlikte çalışmak zorunda kalan işletmeler, hükümetler ve kuruluşlarla uluslararası ilişkiler üzerinde önemli bir etkisi vardır (Singer & Friedman, 2014).

2016 yılı, siber güvenliğin tüm dünyada siyasetin zirvesi haline gelmesine yol açmıştır. Bunun nedeni, Rus hükümetinin 2016 ABD Başkanlık seçimleri sırasında gizli e-postaları hacklemesiydi. Uluslararası ilişkiler disiplinindeki uzmanlar, ulusal ve uluslararası güvenlik için teknolojinin etkilerine odaklanıyor; Ayrıca, artan tehdit düzeyi, hükümetin ve paydaşların benimsemesi gereken uygun politika yanıtlarına duyulan ihtiyacı öngörmektedir; Siber suç deneyimi, siber güvenliğin uluslararası ilişkilerde en önemli gündem olmaya devam edeceğini ortaya koymaktadır (Collier, 2018).

Bu bölümde öncelikle siber evrenin kavramsal boyutu üzerine odaklanılmıştır. Bu yüzden, tez çalışmasının sorunsalı bağlamında da olmak üzere, siber uzay, siber saldırı teknik ve yöntemleri ve siber güvenlik kavramları irdelenmiş ve tanımlanmaya çalışılmıştır. Bu kapsamda, siber güvenliğe kuramsaldan ziyade kavramsal boyutlar öncellenerek yaklaşılmasında, siber saldırıların zaman sınırı olmadan ani, gizli, kuralsız ve limitsiz güvenlik risk ve tehditleri yaratmasından dolayı daha uygun olacağını savlamak mümkündür. Zira günümüzde siber saldırılara başvurulmasında temel kuramsal argümanların; bireyden gruba, devletden terör örgütlerine ekonomik-politik ve askeri-siyasi mülahazalar ve menfaatler olduğu görülmektedir. Bu yüzden siber saldırılar son 20-30 yılda devletlerce milli çıkar ve hedefleri için kullanılır olmuş, böylece uluslararası ilişkilerde sonuç-odaklı güç ve kazanç mücadelerinin asimetrik bir aracı, deyiş yerindeyse silahı haline gelmiştir.

Nitekim insanlık tarihi boyunca güvenlik kavramı, özellikle kavramsal boyutta tüm canlı toplulukları için en önemli olguların başında gelmiştir. Bu durum, insan toplulukları için de en başta gelen kritik olgudur; zira güvenlik kavramı, insanların doğrudan yaşamına dokunan, onların varoluşuna doğrudan etkide bulunan bir faktördür. Bu nedenle, hiçbir canlı organizma güvenlik olgusunun teorik boyutunu pek fazla öncelemez; bilakis kavramsal çerçevesine– pratik ve pragmatik bağlamda- daha çok odaklanır. Aynı zamanda, güvenliğin sosyal boyutu derken, bunun hem toplum güvenliği hem de milli güvenlik ile doğrudan ilgili bir olgu olduğunu göz ardı etmemek gerekir. Keza milli güvenliğin gerek kamu güvenliği, sosyal güvenlik, gerek askeri güvenlik, gerekse siber güvenlik gibi birçok veçhesi mevcuttur.

Nitekim siber güvenlik, özellikle bilişim sistemleri ile internetin; siyasetten askeriyeye, ekonomiden finansa, eğitimden kültüre, iletişimden uluştırmaya, maliyeden medyaya küresel toplumun her alanına girmesiyle hem devletler hem de uluslararası toplum için en önemli güvenlik mülahazalarından birisi haline dönüşmüştür. Bunda temel faktör, bilişim sistemleri ve İnternetin yaşam bulduğu evrenin, sanal ve siber bir âlem olması ve bu sanal dünyadaki tüm faaliyetlere ait kimlik, bilgi, izler vb. olguların gerçek hayattaki gibi gözlemlenme, deneylenme, ölçülme ve benzeri bilimsel araştırma yöntemlerine pek de tabi olmamasıdır. Bu siber evren, -istenildiği her fırsatta- limitsizlik, sorumluksuzluk, kuralsızlık ve zamansızlığa kolayca tabi olabilir.

Dolayısıyla, internet dâhil tüm bilişim alt/üst yapıları ile sistemlerini ihtiva eden siber teknolojilerin milli güvenlik üzerine olabilecek etkilerine ilişkin tartışmalar, kimi zaman alan araştırmacıları tarafından "Rorschach testi"ne de benzetilir. Bu teste göre, siber teknolojilerin gerçek sonuçları, sanki bunlardan çok siber teknolojileri kullananların profesyonel geçmiş ve kişiliklerinden daha çok söylemektedir. Zira günümüzde siber teknolojilerin silah gibi kullanılması olgusu, artık her yerde ve her mecradadır (Cilluffo & Clark, 2016). Uluslararası ilişkiler de bunlardan birisidir. Nitekim en son olarak Ukrayna'daki Rus saldırıları sonrası Almanya'nın Ukrayna'ya Leopard-2 tankları teslim etme kararı sonrasında, Almanya Federal Siber Güvenlik Ajansı tarafından yapılan açıklamada, 25 Ocak 2023 tarihinden itibaren Almanya'daki bazı kamu kurumlarını, perakende veya finans şirketlerini, medyayı veya diğer kuruluşları hedef alan ve Almanya Federal Siber Güvenlik Ajansı'nın tespitlerine göre Rusya Federasyonu orjinli hacker sitesi Killnet tarafından yoğun Dağıtılmış Hizmet Reddi (Distributed Denial of Service-DDoS) saldırıları gerçekleştirildiği, ancak bu aşamada Rus hackerların pek de zarar veremedikleri bildirilmiştir. Nitekim Dağıtılmış Hizmet Reddi saldırıları, bir web sitesinin normal şekilde çalışmasını durdurmak veya tamamen bozmak için tasarlanmış siber saldırı yöntemlerinden birisidir (Yeniakit, 2023).

Dolayısıyla, bu bölümü kapatırken ve yeni bölüme geçerken, devletlerin bir yandan son 30 yılda meydana gelen teknolojik gelişmelere, bunların modern sosyal yaşam içerisinde yeri doldurulamaz kritik bir altyapı haline gelmesine

teşekkür ederken, öte yandan bunların devletleri oldukça savunmasız hale getirdiklerini de söylemek mümkündür (Darıcılı & Çelik, 2021). Zira siber evren, herkes için bilinmez, tanımsız ve kuralsız bir âlemdir. Nitekim devletlerin, siber uzay ve buradan kaynaklı siber saldırı tehditlerine karşı ulusal kritik altyapılarının siber güvenliğini yeni güvenlik model ve politikaları çerçevesinde ele aldıkları ve siber âlemden ortaya çıkabilecek ve gerek ulusal gerekse uluslararası ilişkiler bağlamında ülke güvenliklerine ve menfaatlerine yönelebilecek bu nevi asimetrik tehditlere karşı son 15-20 yılda yoğun ve detaylı bir şekilde yeni ulusal güvenlik stratejileri geliştirdikleri görülmektedir.

4. ULUSLARARASI İLİŞKİLERDE SİBER SALDIRILAR

4.1. Siber Alanın Uluslararası İlişkilere Dahil Olması

Hemen herkes siber uzayın günlük hayatın bir gerçeği olduğunun farkındadır. Nitekim internet, bağlandığı milyarlarca bilgisayar, yönetimi ve sağladığı deneyimler de dâhil olmak üzere siber uzay, her yerde bulunması, ölçeği ve kapsamı göz önüne alındığında, içinde yaşadığımız dünyanın merkezi bir özelliği haline geldi ve temel olarak yeni bir gerçeklik yaratmıştır. Siber uzayın gelişiminin, artan sayıdaki sosyal ve politik faaliyetlerle artan ilgisi nedeniyle küresel siyasetin gidişatı üzerinde etkili olmaya başlamıştır (Collier, 2018).

Siyaset kavramı, "kimin neyi, ne zaman, nasıl alacağının toplumsal ilişki yoluyla belirlenmesi" olarak tanımlanacak olursa, siber uzay olgusu da sosyal aktivitenin hızla büyümesi ve bu alandaki ilişkilerin uluslararası güvenlik için artan önemi, küresel ekonomi, politik ve sosyal organizasyon ve fikirlerin gelişimi ve yayılması için potansiyel bir dönüştürücü olarak görülebilir (Duić vd., 2017).

Choucri'ye (2012) göre, günümüzde siber uzayın etkisi, çağdaş toplumun tüm yönlerinde, dünyanın hemen hemen her yerinde belirgindir. Bildiğimiz haliyle savaşın sınırlandırılmasının zor, daha uzun, daha örtülü, ölçeği, hedefleri ve temposu açısından daha şaşırtıcı ve nihayetinde ayırt edilmesinin daha zor olduğu "Siber Çatışma" çağının eşiğindeyiz. Gelecekteki tüm çatışmalar, ufuk açıcı olayların gerçekleşmesi için siber mekanizmalara ihtiyaç duyacağından "siber" olacaktır.

Collier'in (2018) de vurguladığı şekilde, bu yeni ortaya çıkan mücadele biçiminde "siber" düşmanlar, herhangi bir açık krizden, kamuya açık düşmanlık ilanından veya kilit iç unsurları devre dışı bırakmaya yönelik doğrudan çabalardan çok önce, çeşitli diğer devlet ve devlet dışı aktörlerin sistemik direncini baltalamak için siber uzayı kullanacaklardır.

Hathaway ve Rebecca'ya (2012) göre ise, yeni dijital çağda uluslararası ilişkilerin bilim insanları siber uzayı keşfetmeye başlamıştır. Geleneksel uluslararası ilişkiler teorisi, fiziksel mekânlardaki etkileşimlere dayanır ve bunlara atıfta bulunur. Uluslararası ilişkilerde her türlü alan, dünya siyasetinde güç ve etkiyi genişletmek için fırsatlar sunmaktadır. Siber uzay, casusluktan savunmaya ve bilgisayar korsanlığına kadar her devlet için önemli bir dış politika aracı haline gelmiştir. Farklı devletler, kendi sınırları içinde İnternet'i farklı şekilde düzenlemiş ve birkaç yıl önce tasavvur edilen küresel açık internetin aksine, giderek daha fazla parçalanmış bir küresel internet üretmiştir.

Siber alanın uluslararası ilişkiler disiplini içerisine dâhil olması ya da devletlerin son yıllarda önemli derecede çalışmalar yürütmesinde devletlerin hissettikleri güvenlik kaygısı ve devletlere yapılan saldırılar etkili olmuştur. Devletlerin önceden var olan risk durumunun tehdide dönüşmesi, güvenlik politikalarını üretmesine neden olmuştur. Bir devletin, diğer devletlerin egemenliğini, istikrarını ve güvenliğini tehdit ettiği bir alan olarak görmesinden sonra uluslararası ilişkiler için kritik bir noktaya gelmiştir. Uluslararası ilişkiler içine siber uzayın girmesi ile siber güvenlik, siber tehdit kavramları da hızla gündem içindeki yerini almıştır. Uluslararası ilişkilerin yeni, siber boyutu, gücün korunması ve yıldırma teorileri için büyük bir zorluk olmaktadır (Choucri, 2012).

Duić ve arkadaşlarına (2017) göre, siber uzayda uluslararası ilişkilerin yoğun gelişimi, teknolojilerin gelişim hızı ve bunların devletler, kuruluşlar ve bireyler arasındaki ilişkilerde uygulanmasıyla koşullandırılan ve desteklenen bu alan her zaman ilginç ve zorlu olacaktır. Bu sonuç, siber tutumların ve bilişim teknolojilerinin sürekli değişmesinden kaynaklanmaktadır. Bu bağlamda, Amerika Birleşik Devletleri, Rusya ve Çin'deki askeri stratejistler, 1990'lı yıllardan itibaren ağ bağlantılı bilgisayarlar savaşının önemi ve olası etki ve sonuçları üzerine daha yoğunlukta düşünmeye başlamışlardır. 1990'lar boyunca, ordular siber uzayı teoride ve pratikte "savaş alanı" olarak ele almışlar ve 2000'li yılların ilk on yılında Rusya kaynaklı siber saldırıların çeşitli kriz ve çatışmalarda vuku bulması, 2011 yılında ABD Pentagon kurumunun, kara, deniz, hava ve uzayın yanına siber uzayı da "beşinci" savaş alanı olarak

eklemesine sebep olmuştur. Aslında bu "beşinci boyutlu savaş alanı" perspektif ve savı, başından beri önce bahsedilen iki ucu keskin kılıç algısı ile karakterize edilmiştir. Nitekim stratejistler, teknoloji destekli "bilgi hâkimiyeti" yoluyla savaşları kazanmak için büyük fırsatlar görmüşler; ancak aynı zamanda hem gerçek hem de sanal dünyada artan güvenlik kaygı ve mülahazaları nedeniyle, hedef kitle ve devlete risk ve tehdit yaratabilecek daha fazla güvenlik zafiyet ve açıklarını öngörmüşlerdir (Berkowitz, 2003).

Her zamankinden daha sıkı birbirine bağlılığın bir sonucu olarak artan güvenlik açıkları fikri, 1990'ların ikinci yarısında askeri ağlardan tüm topluma, modern toplumların omurgası olan "kritik altyapılara" bir bağlantı yoluyla genişletildiği dijital teknolojilerin siyasi önemi, bilgi altyapılarının ekonominin, hükümetin, ordunun ve genel olarak toplumun işleyişi için önemli hizmetleri desteklediği ve sağladığına dair artan bir farkındalığı yansıtmaktaydı. Bir yandan, kritik altyapılara karşı tek başına, beklenmedik siber saldırılar olarak anlaşılan stratejik siber savaş veya siber terörizm, beklenen görünümü veremezken, diğer yandan düşük düzey siber çatışmalar uluslararası ilişkilerle daha alakalı hale gelmiştir (Dunn Cavelty & Kristensen, 2008).

Carr (2010), siber savaşın 2000'li yıllardan itibaren var olduğunu; ancak, hala tam olarak tanımlanmadığını belirtmektedir. Siber saldırı eyleminin yasal bir tanımını oluşturacak geçerli bir uluslararası anlaşma yoktur. Aslında, uluslararası siber hukukun tüm alanı hala belirsizdir. Bilgi ve iletişim teknolojilerinin gelişimi ve mevcudiyeti ile siyasi ve ideolojik olarak farklı devletler arasında sürekli var olan gerilimler, siber uzayda uluslararası ilişkileri koşullandırmıştır. Siber uzayda stratejik hâkimiyet henüz uluslararası ilişkilerin hiçbir kuruluşu tarafından sağlanamamıştır. Çok sayıda uluslararası kuruluş siber uzayda varlıklarını ve hareket etme isteklerini göstermiştir.

Bu, tahakküm veya blok bölünmesinin gerçekleşmesinin pek olası olmadığı siber uzayın çok kutuplu bir boyutunu ortaya koymaktadır. Sebepler, savunma sistemlerinin birbirine bağlanması durumunda karşılıklı güvensizlik ve casusluk korkusunda yatmaktadır. Ancak en etkili olan ülkeler, ekonomik ve askeri olarak en güçlü ve aynı zamanda siber altyapıya en bağımlı olan ülkelerdir (Hathaway & Rebecca, 2012).

4.2. Uluslararası Aktörler ve Siber Mücadeledeki Yerleri

Dünya siyasetinin başlıca aktörleri ulus-devletlerdir; ancak, tek aktör onlar değildir. Uluslararası sistem, ulus-devletler, uluslararası kuruluşlar ve özel aktörlerden oluşur. İkinci Dünya Savaşı sonrası dönemde binlerce uluslararası örgüt kurulmuş olmasına rağmen, uluslararası ilişkiler alanı; araştırmacıları, öğrencileri ve taraftarları tarafından küçümsenmiştir (Ataman, 2003).

Uluslararası kuruluşların sayısının artması, bireyler, toplumlar ve devletler arasındaki ekonomik, siyasi, sosyal ve kültürel ilişkilerin artan seviyelerine paraleldir. Pek çok türde devlet dışı aktörün büyümesi, uluslararası siyasetin "devlet merkezli" kavramına meydan okur, onu zayıflatır ve onun yerine, ilişkilerin daha karmaşık olduğu "ulus-ötesi" bir sistem koyar.

Devlet dışı aktörlerin çoğalması, son zamanlarda bazı uluslararası ilişkiler gözlemcilerinin, devletlerin öneminin azaldığı ve devlet dışı aktörlerin statü ve etki kazandığı sonucuna varmasına yol açmıştır. Devletlerin kendi içerisinde oluşturdukları siber ordular ve uzmanlaşmış personeller siber güvenliğe ilişkin yeni aktörlerdir ve adeta devletler için vazgeçilmez unsurların başında gelecektir. Uluslararası alandaki yapılanmalar ise daha çok illegal gruplanmalara kaymıştır ve karşılıklı çıkar bağlamında iş birlikleri oluşmuştur. Artan kanıtlar, devlet ve devlet dışı aktörlerin daha geniş bilgi alanını siyasi anlaşmazlıklar veya çatışmalardan önce ve bunları etkilemeye çalışmasının rutin hale geldiğini ve bazen hafif yıkıcı saldırılarla birleştiği görülmektedir (Ataman, 2003).

Normalde siber uzay, resmi ve özel kurum, kuruluş, şirket ve işletmeler gibi tüm devlet aktörlerinin faaliyetlerini yürüttüüğ, sınırları olmayan sanal ve soyut bir alandır. Siber uzayın modern toplum için artan önemi nedeniyle, siber devlet dışı aktörlerin rolü ve faaliyetleri de çok önemli hale gelmiştir; bununla birlikte, bu faaliyetlerden bazıları kötü niyetlidir. Zira günümüzde siber saldırıların sayısı ve karmaşıklık düzeyleri, özelllikle devlet dışı aktörler yüzünden artmaya devam etmektedir. Bu nedenle, siber arenadaki her aktörün davranışı, her hükümet için ulusal güvenlik endişesi haline gelmektedir. Siber saldırıların asimetrik doğası, atıf sorunu, devletler tarafından farklı yasal

çerçevelerin benimsenmesi, giriş engellerinin düşük olması siber uzayı hem devlet aktörleri hem de siber devlet dışı aktörler için çekici bir arena haline getirmektedir.

4.2.1. Devletler

Uluslararası ilişkiler alanı uzun zamandır küresel siyasetin en önemli aktörleri olarak devletlere odaklanmıştır. Devletler, bir başkan gibi siyasi görevliler ve vatandaşlarının siyasi, sosyal ve ekonomik etkileşimlerini düzenlemekten sorumlu ordu gibi bürokratik kurumlar topluluğudur. Devletler, vatandaşları üzerinde siyasi otoriteye sahiptir, davranışlarını yasalar yazarak ve uygulayarak yönlendirir. Devletler, siyasi otoritelerinin coğrafi kapsamını sınırlayan tanımlanmış bir bölgesel yargı yetkisini denetler. Devletlerin egemenliği veya yönetme hakkı, devlet olmayı başarmak için sistemdeki diğer devletler tarafından tanınmalıdır. Devletler, uluslararası ilişkilerde önemli aktörlerdir; zira hükümetleri, vatandaşlarının dünyanın her yerinden insanlarla nasıl etkileşime gireceğini yapılandıran kuralları belirlemektedir (Barkham, 2001).

Devletlerin kontrolsüz egemen otoritesine birçok alanda meydan okunduğu bir zamanda, devlet sorumluluğu uluslararası güvenliğin önemli bir siperi olmaya devam etmektedir. Ancak uluslararası hukukta devlet sorumluluğunu tanımlamak için uygulanabilir bir rejim inşa etmenin zor olduğu kanıtlanmıştır. Devlet destekli terör eylemlerinin örnekleri, Soğuk Savaş'ın sona ermesinden bu yana artmıştır, ancak bu tür eylemler için devletin sorumluluğunu kanıtlamak son derece zor olmaya devam etmektedir. Bu sorun, siber saldırıların hızı ve anonimliği ile siber uzayda büyütülür ve Beyaz Saray'a göre teröristlerin, suçluların ve devletlerin eylemleri arasında ayrım yapmayı zorlaştırmaktadır (Shackelford, 2010).

Siber savaş, tipik olarak bir devletin diğerine siber saldırılar gerçekleştirmesini içerir, ancak bazı durumlarda saldırılar, düşman bir ulusun hedefini ilerletmek isteyen terör örgütleri veya devlet dışı aktörler tarafından gerçekleştirilir. Yakın tarihte birkaç siber savaş iddiası örneği vardır; ancak, bir siber saldırının nasıl bir savaş eylemi oluşturabileceğine dair evrensel, resmi bir tanım yoktur (Shackelford, 2010).

Devletler, orduları ve hükümet yetkilileri aracılığıyla doğrudan bilgisayar korsanlarını istihdam edebilir. Bunları dolaylı olarak da finanse edebilirler. Bu, saldırının tespit edilmesi durumunda devletin müdahalesinin inkâr edilmesini kolaylaştırır. Bu da bu saldırıların sahip olabileceği diplomatik yansımaları azaltabilmektedir. Aynı zamanda suç örgütleri ve hükümet grupları arasındaki çizgiyi de bulanıklaştırmaktadır (Roskin & Berry, 2014).

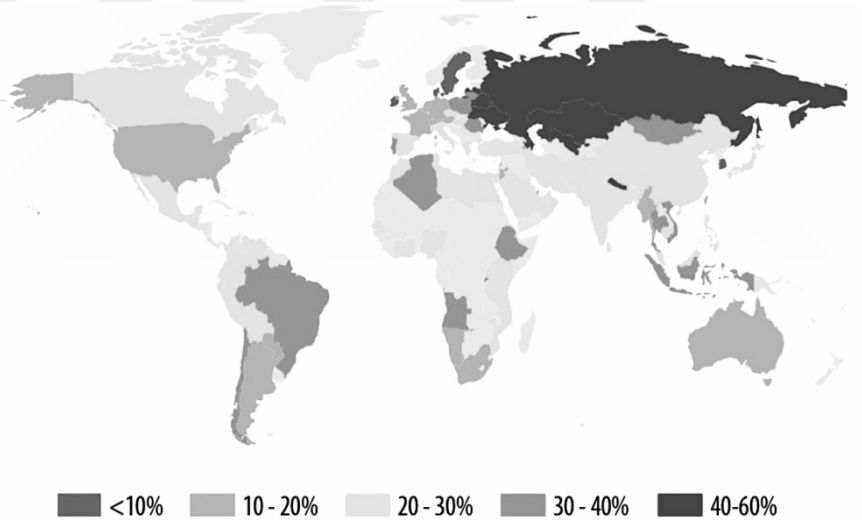
2007'de Estonya'ya yapılan siber saldırıda görüldüğü gibi, potansiyel bir sponsor devlet, kendi adına suç veya terör eylemleri gerçekleştirenlerin soruşturulması, yakalanması ve iade edilmesinde iş birliği yapamamıştır. Siber uzayın gizli doğası göz önüne alındığında, Devletler böylece sınırları içindeki sivil grupları siber saldırılar yapmaya teşvik edebilir ve daha sonra ne kadar şeffaf olursa olsun makul bir inkâr edilebilirlik perdesinin arkasına saklanabilir ve böylece sorumluluktan kaçabilmektedir (Davis, 2007).

Devletler, piyasa ve sosyal güçleri hesaba katmadan siber uzayı kendi başlarına güvence altına alamazlar; yine de büyük güçler arasında sorumlu davranış konusunda daha fazla yakınlaşma olmadan istikrarlı bir siber yönetişim çerçevesi ortaya çıkmayacaktır. Büyük güçler, devlet etkileşimlerinde siber operasyonların sorumlu kullanımını neyin temsil ettiği ve bu nedenle siber uzay yoluyla diğer devletlerin siyasi süreçlerine hangi tür casusluk ve müdahalelerin kabul edilebilir olduğu konusunda anlaşamadığı sürece, yukarıdan aşağıya çok az ilerleme gerçekleşecektir. Aşağıdan yukarıya ilerleme ise, çok paydaşlı bir çerçevede birlikte başarılı bir şekilde çalışmak için aktörlerin birbirleri için daha görünür hale gelmesini gerektirir (Shackelford, 2010).

Kendi aralarında olmasa da devletler farklı aktörlerin sahaya inmesiyle siber alanlardan etkilenmekte ve bu düzeyler siber ortamlara bağlılık çerçevesinde farklılık arz edebilmektedir. Sınırları uluslararası ilişkiler bakımından belirlenmiş olan devletler etkilenme açısından sosyal, kültürel, coğrafi ögeler üzerinde durulmaksızın ciddi bir farklılık taşımaktadır. Birbirleri arasındaki çatışma kültürüyle bu saldırılardan etkilenme oranlarının direkt bir şekilde ilintili bulunmadığı anlaşılmaktadır. Rusya ve çevresindeki devletlere ait oranların yüksek olmasında devlet kurumlarına ait verilere ulaşılmaya

çalışılması, bankalara saldırılar, illegal aktivitelerin siber ortamlarda yoğunlaşması benzeri ögeler belirleyici olmuştur (Klimburg & Healey, 2012).

Uluslararası sahada güç ilişkisinin her şeyi ile etkili bulunmadığı siber ortam yalnızca dış dinamiklerin etkisi ile devletler üzerinde baskı teşkil etmemektedir. Devletin küresel bir aktör şeklinde farklı fiziki araçlarla da sınırları çerçevesinde olan ve dolaşmakta olan siber tehditler etkinliğini arttırabilmektedir. Görsel 4.1'de devletlere göre yerel siber tehditlerin küresel dağılımı oransal şekilde sunulmuştur. Yerel siber tehditler Web tabanlı saldırılar çerçevesinde etkinlik bakımından daha dengeli durmaktadır. Fiziksel bir şekilde devletlerin bağlı olduğu teknolojik araçlar ve altyapı her geçen gün etkinliğini arttırmak ve kimi zaman bu araçların varlığı bir caydırıcılık dahi oluşturması bunun en temel sebebidir (Güntay, 2016, ss. 68-69).



Şekil 4.1: Web Tabanlı Saldırılarda Devletlerin Küresel Etkilenme Oranları

Kaynak: Kaspersky Lab. (2015). *Kaspersky Security Bulletin 2015 Final Report.* [Report No: 34]. Kaspersky. https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin2015_FINAL_EN.pdf

4.2.2. Siber ordular

Bir ulus, kendisini düşman bir ulusun siber saldırılarından, siber terörizmden ve siber suçlardan koruyarak siber egemenliğini sürdürmek zorundadır. Ordunun, düşman bir ulustan gelebilecek bir siber saldırıya karşı koruma ve savunma yapma ve savaş zamanlarında saldırgan siber saldırılar başlatma hedefi vardır. Bu, kendi kuvvetlerinin hareket özgürlüğü ve nihai

zaferi sağlamak için savaş alanı içinde karşılaştırmalı ve büyük bir inisiyatif elde etmektir. Temelde askeri kuvvetler, bir ulusun egemenliğini ve bütünlüğünü, sivil toplumu da dahil olmak üzere, kötü niyetli bir düşman devlete karşı korumak için vardır (Aschmann vd., 2015).

Bir askeri siber ordu, çok yetenekli bir bilgi teknolojisi asker grubudur, diğer deyişle siber beceriler konusunda geniş bir anlayışa sahip olan, askeri ve stratejik hükümet kritik altyapısını savunabilen ve siber saldırılar başlatabilen "siber savaşçılar" dan oluşur. Bir siber ordu, siber becerilere sahip bilgi teknolojisinde oldukça yetenekli bir grup askerdir. Siber ordular, ülkelerin ulusal siber güvenliği sağlamak için kullanması gereken görünmeyen askeri siber güçtür. Ordudaki siber savunma, askeri ve hükümet bilgisayar ağlarının güvenliğini sağlayan ve iç veya dış tehditler yoluyla tehlikeye atılmamasını sağlayan bir savunma rolünü içerir. Siber ordular, Devlet eliyle yetiştirilen ve resmi olarak kullanılmakta olan birimlerden ve gönüllülerden oluşup devlet tarafından desteklenen, resmi olmayan birimlerden oluşabilmektedir (Clarke & Knake, 2010).

Saldırgan rolü, düşmanlara karşı siber silahlar kullanarak, imha etmek, istismar etmek, bozmak veya istihbarat için bilgi toplamak için saldırgan siber saldırıların proaktif ve reaktif olarak başlatılmasını içerir. Bir siber ordunun görevi, ordu için bu rolleri yerine getirmektir (Sharma, 2010). Dolayısıyla siber ordu, siber savunmayı yürütmek ve düşman bir ülkeye karşı siber saldırı saldırıları başlatmak için askeri ve hükümet siber alanındaki bilgi toplama, teknolojinin sağlamlaştırılması ve iletişim bilgisayar sistemleri açısından savaş alanında belirleyici bir avantaj sağlayabilecektir (Clarke & Knake, 2010).

Siber ordu, siber politika ve siber strateji geliştirme konusunda stratejik yön belirlemeye yardımcı olarak bir devlete değer katabilecektir. Ulusal kritik altyapıları etkin bir şekilde koruma ve ulusal siber tehdit analizlerini yürütme ve bunlara katkıda bulunma yeteneğine sahip olacaktır. Siber ordular, siber barışı sağlamak için ulusal siber uzayın korunmasına da yardımcı olabilecektir. Siber ordular, siber silahlar ve siber tehditlere hızlı tepki verme ve askeri ve devlet ağlarında gelen ve giden verilerin proaktif siber polisliğini yürütecek ve siber saldırı tahmin portföyleri geliştirecektir (Aschmann vd., 2015).

Siber uzayın küresel patlaması tehdidi nedeniyle devletlerin ordusunda bir siber orduya sahip olma meşruiyeti haklı çıkar. Bir devlet, bir siber saldırı yoluyla saldırıya uğradığında kendini koruma ve başka bir devlete karşı savunma hakkına sahiptir. En büyük sorun, bir siber saldırının ne zaman savaşa dönüşeceğini ve saldırganın kim olduğunu nasıl ilişkilendireceğini belirlemektir. Bir devlete karşı bir siber saldırı başlatmak için ayrıntılı planlama hayati önem taşımaktadır, bu nedenle bilgi toplanması kritik öneme sahiptir ve istihbarata yakınsama hayati önem taşımaktadır (Sharma, 2010).

Siber ordular, bir ulusun siber altyapısının kontrolünün ve savunmasının kötü niyetli amaçlara karşı korunabileceği bir uus devletin stratejik askeri cephaneliği içinde meşru olarak görülmelidir. Araştırma ve geliştirme ve saldırı yetenekleri de bir siber ordu içinde esastır (Aschmann vd., 2015).

4.3. Devlet Dışı Uluslararası Aktörler

Siber uzay, savaşla ilgili diğer alanların aksine, yüksek düzeyde anonimlik sağladığından, saldırganlar bu alandaki eylemleri çok az veya hiç ilişkilendirme riski olmadan gerçekleştirebilir. Bu nedenle, devletlerin, hareket özgürlüklerini sınırlayacak yasal olarak bağlayıcı bir siber savaş tanımını destekleme veya gerçekleştirilen siber saldırılar için resmi sorumluluk alma konusunda çok az teşviki vardır. Eğer bir devlet bu tür saldırıları gizlice başlatabilir, finanse edebilir veya kontrol edebilir ve saldırıların yerine devlet dışı aktörlere güvenebilir ise, zaten düşük olan siyasi sonuçların riskini azaltabilir ve potansiyel olarak hedeflerine ulaşabilir. Bu, özellikle kinetik bir savaş alanında üstünlük sağlayamayan daha küçük ülkeler için, bir saldırgana muazzam bir asimetrik avantaj sağlar. Sonuç olarak, siber uzay operasyonlarında devlet dışı aktörlerin istihdam edilmesi, özellikle sınırlı stratejik hedefler peşinde koşarken, devletler veya eşdeğer bir organ için muhtemelen çok çekici bir seçenektir (Sigholm, 2013).

Siber devlet dışı aktörler, küreselleşen dünyamızın kilit figürleridir ve operasyonlarının uluslararası ilişkiler, siyaset ve ekonomi üzerinde devletler kadar önemli bir etkisi olabilir. Devlet dışı aktörler arasında çok uluslu şirketler, bilgisayar korsanları kolektifleri, sivil toplum kuruluşları (STK'lar),

siber suç sendikaları, özel askeri kuruluşlar, medya kuruluşları, terörist gruplar, işçi sendikaları, organize etnik gruplar, lobi grupları, suç örgütleri, özel işletmeler ve diğerleri bulunmaktadır. Bazıları siber suç çeteleri gibi finansal olarak motive olurken, diğerleri devlet destekli bilgisayar korsanları ve bilgisayar korsanları gibi politik olarak motive edilir. Siber devlet dışı aktörlerin devlet karar verme süreçlerini etkileme yetenekleri, kendi kategorilerine bağlıdır (Sharma, 2010).

4.3.1. Uluslararası illegal yapılanmalar

Aktör şeklinde illegal-yasadışı organizasyonların varlığı ve uluslararası alanlardaki etkinliği, devlet dışı gruplar şeklinde bir faaliyet alanı oluşturmaktadır. Haberleşme ve bilgisayar teknolojileri ile ilgili bilgi sahibi olan ve aynı zamanda bu konularda standartların üzerinde beceri ve bilgiye sahip bulunan organizasyonlar devletler ve kimi özel kuruluşlarla iş birliği halinde uluslararası sistemin aktörleri durumuna gelmişlerdir (Broadhurst vd., 2014).

Son dönemde yaşanmakta olan politik gelişmelerle beraber gündemde sıkça farklı gruplar, isminden söz ettirmeye başlamıştır. Anonymus benzeri yapılanmaların son zamanlarda faaliyetleri, Panama ve Wikileaks belgelerinin sızdırılmasıyla ilgili olaylarda farklı grupların etkinlikleri, bireyler ve devletlerle olan iş birlikleri kamuoyunda ses gelirmiştir. Uluslararası illegal yapılarla başta ABD olmak üzere önde gelen ülkelerin de eylem ve mücadele stratejilerine ilişkin girişimler ve askeri bakımdan gerçekleştirilen önlemler siber ortamda mücadele alanı oluşturan aktörler bakımından oldukça önem taşımaktadır. Uluslararası yapılanmaların kapasitesi ve faaliyet alanları bu gerçekliği ve önemi de ortaya koymaktadır (Güntay, 2016).

4.3.2. Manipülatif birimler ve söylemler

Siber güvenliğe ilişkin son dönemlerde gelişmelerden en önemlisi uluslararası sahada yaşanmakta olan manipülatif gelişmeler ve meydana getirdiği neticeler olmuştur. Endüstriyel sistemlerde yaşanmakta olan güvenlikle ilgili zafiyetlerin daha fazla kendisini hissettirmesinden sonra kurumların sahip bulunduğu verilerin de değiştirilmek suretiyle daha etkili saldırıların

yaygınlaşması öngörülmektedir. Devletlerin özellikle günümüz dünyasında kırılgan noktaları bulunan krizler ve krizleri oluşturan gelişmelerle ilgili manipülatif anlık söylemlerin ciddi maddi kayıplara da yol açtığı ifade edilmektedir (Güntay, 2016).

Her geçen gün siber saldırı araçları ve hizmetleri krizlerin gelişiminde olağan bir hal almaktadır ve önemli ölçüde herhangi bir organizasyon ve kuruluşa saldırı düzenlemenin maliyeti düşmekte ve birincil odak noktası şeklinde bu da daha fazla sayıda saldırının gerçekleştirilebileceğini göstermektedir. Bu gelişme dâhilinde devletlerin verecekleri alana ilişkin kararlar işlemektedir. Bilinçsiz ya da bilinçli bir şekilde verilerin manipüle edilmesi durumunda söz konusu kararlarla ilgili yanlış adımlar atılabilir ve zorlayıcı unsurlara da başvurması mümkündür. Üretim süreçleri ve kontrol sistemlerinde verilerin yanlış yorumlanması durumunda yıkıcı neticeler doğurması mümkündür (Nath, 2012 akt. Güntay, 2016, s. 74).

4.4. Siber Savaşçılar

Genel olarak siber alt yapılar çerçevesinde konvansiyonel silahlar bünyesinde yer alan sibernetiğe bağlı bütün sistemleri korumakta olan, siber saldırı ve siber güvenlik konuları ile ilgili uzmanlara, bu savunma ve saldırı kabiliyetlerinde olan kişiler siber savaşçı olarak isimlendirilmektedir. Hava, deniz ve kat kuvvetleri unsurları ile birlikte başta NATO olmak üzere çok sayıda devlet yeni bir çatışma alanı olarak siber alanı kabul ederek bu düzlemdeki siber savaşçıların varlığını ve önemini kabul etmişlerdir (Güntay, 2016).

Bir siber savaşçı, bilgisayar ağı operasyonlarından sorumlu olan geleneksel bilgi teknolojisi veya bilgi güvenliği uzmanıdır. Üstlendikleri rol, ağ saldırıları, ağ savunması ve ağ istismarı ile uğraşmayı içerebilir. İnternet, suçlular, yabancı askerler ve diğer kötü aktörler için hazır erişim sağlar ve bu da kritik altyapı ve bilgilerin finansal kazanç için tehlikeye atılmasına ve fikri mülkiyet hırsızlığına neden olabilmektedir. Siber savaşçılar, bilgi teknolojisini kullanarak savaş açarlar. Bilgisayarlara veya bilgi sistemlerine, bilgisayar korsanlığı veya diğer ilgili stratejiler yoluyla saldırabilir veya onları

benzerlerinden koruyabilirler. Siber savaşçılar ayrıca, bilgisayar korsanlığı ve diğer yollarla güvenlik açıklarını bularak ve diğer bilgisayar korsanları onları bulup istismar etmeden önce bu güvenlik açıklarını kapatarak bir sistemi güvence altına almanın daha iyi yollarını bulabilirler. (Sigholm, 2013).

Stuxnet'in ülkenin nükleer kapasitesinin yaklaşık %20'sini mahvetme konusundaki göreceli başarısının ardından, Tahran "siber savaşçılar" yetiştirmek için iddialı bir programa daha fazla yatırım yapmaya başlamıştır. Programında ve bu siber savaşçılar arasında "İran'da oldukça önemli bir bilgisayar korsanlığı topluluğu vardır. Bu bilgisayar korsanlarının becerileri, zaten bilinen güvenlik açıklarından yararlanmak için geliştirilmiş yazılım araçlarını kullanabilen vasıfsız amatörlerden, yeni güvenlik açıkları ve istismarlar bulan yetenekli bilgisayar korsanlarına kadar uzanmaktadır (Ülgen, 2015).

4.5. Uluslararası İlişkiler Açısından Siber Güvenlik

Güvenlik, tüm devletler için önemli bir endişe kaynağıdır. Aslında günümüz teknolojilerinin çoğu, ulusal savunma sanayilerindeki araştırma ve geliştirmenin doğrudan bir sonucudur. Bununla birlikte, zaman zaman diğer alanlardaki teknolojik gelişmeler devletlerin güvenlik endişelerini etkiler. Bilgi ve İletişim Teknolojileri'ndeki (BİT) devrim, bu nevi önemli bir örnek teşkil etmektedir. 21. yüzyılın başında küresel siber uzayın ortaya çıkmasıyla Yüzyılda ulusal siber güvenlik, devletlerin dış ve iç politikalarında önceliğini artırmıştır. Uluslararası bir rejim olmadığı için açık denizler veya dış uzay rejimi gibi siber uzayı yöneten devletler, ulusal güvenlikleri için bir tehdit olarak algıladıkları siber uzayın ihlali konusunda kendilerini giderek artan bir şekilde çatışma içinde bulunmaktadır (Stadnik, 2017).

Devletlerin siber uzay ve uygun kullanımı konusunda da çok farklı bakış açıları vardır ve sayıları giderek artan saldırgan siber yetenekler geliştirmektedir. Siber güvenlik, hükümetlerin ulusal savunmasının yanı sıra dış ve güvenlik politikaları ve doktrinlerinin ayrılmaz bir parçası haline geldi ve siber güvenliğin yeni bir savaş alanı olarak inşasına katkıda bulunmuştur. Siber uzaya giden yolun kurallarını geliştirmeye yönelik çabalar, mevcut uluslararası

hukukun uygulanabilirliğine, potansiyel boşluklara, normların geliştirilmesine, güven artırıcı önlemlere ve caydırıcı duruşların varsayılmasına odaklanmaktadır. Dolayısıyla, Joseph Nye'nin kısa ve öz bir şekilde öne sürdüğü gibi, politika tepkilerini şekillendirmede çok önemli roller oynayan çok sayıda bölgesel ve uluslararası kurumu kapsayan bir siber güvenlik rejimi kompleksi gelişmiştir (Choucri, 2012).

Siber alan, uluslararası güvenliğin ve güvenlik kavramının dönüşümü üzerinde büyük bir etkiye sahiptir. Pek çok yazar, siber doktrinlerin gerektiği gibi anlaşılmasının ve kurulmasının gerekliliğini vurgulamaktadır. Uluslararası ilişkilerin yeni, siber boyutu, gücün korunması ve yıldırma teorileri için büyük bir zorluktur. Siber tehditler ciddi, istikrarsızlaştırıcı ve artmaktadır. Soğuk Savaş döneminde tasarlanan ve uygulanan yıldırma teorileri ve stratejileri siber alanda uygulanamaz. Birçok bilim insanı, uluslararası ilişkilerde siber devrimin anlaşılması üzerine çalışmaktadır (Duić vd., 2017).

Siber uzay ve bilgi alanı, temel anlamlarında önemli ölçüde farklılık göstermektedir. Ülkelerin algıladıkları siber/bilgi tehditlerinin içerik analizi, bir yanda ABD tarafından desteklenen değerler ile diğer yanda Rusya ve Çin arasındaki fay hattını ortaya çıkarmıştır. ABD, serbest bilgi akışı ve ifade özgürlüğü ile aynı anda açık, güvenli İnternet sağlayan güvenli bilgisayar ağlarıyla ilgilenirken, aynı zamanda mevcut statükoyu korumak için saldırgan siber yetenekler geliştirmektedir. Rusya ve Çin, bilgi güvenliğine ve topluma, siyasi rejime ve bir devletin istikrarına zarar verebilecek tehditlerle mücadeleye yüksek öncelik vermektedir (Stadnik, 2017).

Siber güvenlik, tek bir uluslararası rejim için çok karmaşık, çok bileşenli bir konudur. Uluslararası siber güvenlik rejimi, bir norm oluşturma aşaması olan inşasının ilk aşamalarındadır. Ancak, bu rejimin sınırları hala belirsizdir. Daha fazla gelişme için iki olası senaryo vardır, mevcut uluslararası hukukun siber uzay özelliklerine göre ayarlanması veya özel yönetişim mekanizmalarının geliştirilmesi gerekmektedir (Stadnik, 2017).

4.6. Ülkelerin ve Uluslararası Toplulukların Siber Güvenlik Politikaları

Siber güvenlik politikası oluşturma, Birçok ülkede, daha güçlü bir liderlik tarafından desteklenen bir ulusal politika önceliği haline gelmiştir. Yeni nesil ulusal siber güvenlik stratejileri, ekonomik ve sosyal refahı artırmayı ve siber uzaya bağımlı toplumları siber tehditlere karşı korumayı amaçlamaktadır.

4.6.1. NATO

Eski savaş sistemlerin etkisinin azalması ile beraber gün geçtikçe karmaşıklaşan be hızla büyüyün siber tehditler ve savaşlar ulusal güvenlikleri bakımından ülkelere daha çok zarar vermeye başlamıştır. Soğuk savaşların bitmesiyle birlikte bir güvenlik teşkilatı olan NATO ittifakı da hibrit savaşın parçası olarak görülen bu siber saldırılardan önemli boyutlarda etkilenmiştir. Bu saldırıların ardından NATO, son yirmi yılda yeni ortaya çıkan bu tehditlere karşı korunmak amacı ile farklı yöntemler ve stratejiler üretmiştir (Bıçakçı, 2012).

İttifak, siber güvenlik ve savunmayı güçlendirme ihtiyacını ilk kez 2002 Prag Zirvesi'nde kabul etmiştir. İttifak'ın siber güvenliğinin sağlanması konusu ilk kez, Kasım 2002'de Prag'da yapılan zirve sırasında, üye ülkelerin liderlerinin bilgi saldırılarına karşı koyma yeteneklerini güçlendirmeye hazır olduklarını ifade ettiklerinde, mevcut NATO siyasi gündemine girmiştir. Bu tarihten itibaren, örneğin İttifak'ın siber terörizme karşı ilk savunma hattı olarak nitelendirilen NATO İletişim ve Bilgi Ajansı (NCIA) gibi özel NATO organlarının oluşturulması başlamıştır (Geers, 2011).

Estonya, Nisan ve Mayıs 2007'de bir dizi siber saldırıya maruz kaldıktan sonra, NATO'da İnternet alanından kaynaklanan tehditlerin stratejik olarak önemli olarak algılanması konusunda bir fikir birliği ortaya çıkmıştır. NATO'nun resmi siber savunma politikası Ocak 2008'de NATO savunma bakanları tarafından onaylandı ve Nisan 2008'de Bükreş zirvesinde örgüte sunulmuştur. 2008 yılında NATO ilk siber savunma politikasını benimsemiştir. Zirvenin sonuç bildirgesine göre, bu belgenin, istek üzerine Müttefik ülkelere bir siber saldırıya karşı koymalarına yardımcı olma yeteneği sağlaması amaçlandı. Böylece 2008 yılında Siber Savunma Yönetim Otoritesi oluşturuldu.

İşlevsel olarak, Siber Savunma Yönetim Otoritesinden NATO üye devletlerinden herhangi birine veya NATO'nun kendisine yönelik bir siber saldırı olması durumunda müdahale eylemlerini başlatması ve koordine etmesi istenmiştir (Davis, 2019).

Ekim 2008'de NATO akreditasyonu ve uluslararası askeri örgüt statüsünü alan Estonya'nın başkenti Tallin'deki Cooperative Cyber Defence Center of Excellence (CCDCoE) operasyonel bir işleve sahip değildir ve siber bilimin doktrinel ve kavramsal temellerinin atıldığı bir araştırma ve eğitim merkezi olarak hizmet vermektedir. Bu yapı kendisini, NATO Müttefiklerini ve İttifak dışındaki ortakları bir araya getiren, teknoloji, strateji, operasyonlar ve hukuk gibi odak alanlarını kapsayan siber savunma araştırmaları, eğitimleri ve tatbikatları alanında benzersiz disiplinler arası uzmanlığın ana kaynağı olarak konumlandırmaktadır (Bıçakçı, 2012).

Ancak, önemli dönüm noktası, İttifak'ın Gelişmiş NATO Siber Savunma Politikası'nı kabul ettiği 2014 yılındaki Galler Zirvesi'nde gelmiştir. NATO liderleri, diğer kilit kararların yanı sıra, bir siber saldırının 5. Maddenin uygulanmasına yol açabileceğini açıkça belirtmişlerdir. Galler Zirvesi'nden bu yana NATO ve Müttefikler siber güvenlik, savunma ve caydırıcılığı NATO'nun temel görevlerinin açık bir parçası haline getirdiler ve bunu gerçeğe dönüştürmek için adımları uyguladılar. Brüksel'deki 2018 NATO Zirvesi'nde, Müttefik liderler bir kez daha bu taahhüdünü yinelediler. NATO'nun savunma yetkisini yeniden teyit ederek, hibrit bir harekâtın parçası olarak yürütülenler de dâhil olmak üzere tüm siber tehditleri caydırmak, bunlara karşı savunma yapmak ve siber tehditlere karşı koymak için siber de dâhil olmak üzere tüm yetenekleri kullanmaya kararlı olunduğu vurgulanmıştır (Darıcılı, 2015).

Ortaklıklar, siber zorlukların etkin bir şekilde ele alınmasında kilit bir rol oynamaktadır. NATO, uluslararası örgütler, endüstri ve akademi dâhil olmak üzere çok çeşitli ortaklarla çalışmaktadır. Siber savunma, iki örgütün hibrit tehditlere karşı giderek artan koordineli çabalarının bir parçası olarak NATO ve Avrupa Birliği arasındaki güçlendirilmiş iş birliği alanlarından biridir. NATO ve AB, siber olaylara müdahale ekipleri arasında bilgi paylaşıyor ve en iyi

uygulamaları paylaşmaktadır. NATO ayrıca ortak ülkelerin siber savunma zorluklarıyla mücadele etmesine yardımcı olmaktadır (Davis, 2019).

4.6.2. Avrupa Birliği

Siber güvenlik, Avrupalıların güvenliğinin ayrılmaz bir parçasıdır. İster bağlı cihazlar ister elektrik şebekeleri ister bankalar, uçaklar, kamu idareleri veya hastaneler kullandıkları veya sık kullandıkları olsun, insanlar siber tehditlerden korunma güvencesi içinde bunu gerektirmektedir. AB'nin ekonomisi, demokrasisi ve toplumu, her zamankinden daha fazla güvenli ve güvenilir dijital araçlara ve bağlantıya bağlıdır. Bu nedenle siber güvenlik, esnek, yeşil ve dijital bir Avrupa inşa etmek için çok önemlidir. Ulaşım, enerji ve sağlık, telekomünikasyon, finans, güvenlik, demokratik süreçler, uzay ve savunma, giderek daha fazla birbirine bağlanan ağ ve bilgi sistemlerine büyük ölçüde bağımlıdır. Sektörler arası karşılıklı bağımlılıklar çok güçlüdür; keza ağlar ve bilgi sistemleri de işleyebilmek için sabit bir elektrik kaynağına bağlıdır. Bağlı cihazların sayısı zaten gezegendeki insanlardan fazla ve sayılarının 2025 yılına kadar 25 milyara çıkacağı tahmin edilmektedir. Bunların dörtte biri Avrupa'da olacağından tahmin edildiğinde AB açısından siber güvenlik konusu son derece önem taşımaktadır (UC, 2020).

Bu bağlamda, 2008 küresel ekonomik krizinin ardından, Avrupa ekonomisinin kırılganlığını azaltmak ve AB'nin rekabet gücünü artırmak için 2010 yılında Avrupa Komisyonu, beş ana hedeften oluşan "Avrupa 2020" başlıklı bir strateji açıklamıştır. Bu hedefler sütunlara ve alt sütunlara dayanmaktadır. İlk sütun, Avrupa için Dijital Gündem'i içeren kilit büyümeye odaklanmıştır. Avrupa Dijital Gündeminin temel amacı, tüm Avrupa vatandaşları için sürdürülebilir ekonomik ve sosyal faydalara dayanan, AB üye devletleri için birleşik bir dijital pazar yaratmaktır. Gündem, Avrupa Birliği'nin mevcut ekonomik, sosyal zorluklarını ve eksikliklerini (diğer deyişle dijital pazarın bölümlenmesi, birlikte çalışabilirlik zorlukları, siber suçun yayılması, ağ yatırımlarının olmaması, düşük Ar-Ge (Araştırma-Geliştirme) seviyesi, düşük seviyeli) araştırmak ve analiz etmektir. Avrupa Dijital Gündemi'nin yukarıda belirtilen bulgularına dayanarak, toplumun ve ekonominin tüm kesimlerinde mevcut olan bilgi teknolojisine ve bilgi sistemlerine olan

bağımlılığa atıfta bulunan AB Siber Güvenlik Stratejisi, 2013 yılında tamamlanmıştır (Kovac, 2018).

Bu yeni strateji, birleşik Avrupa siber güvenliğinin temellerini atmaya yönelik ilk etkili ve çok önemli adımdır. Anılan Strateji dokümanı, AB'nin Avrupa telekomünikasyon sistemlerinin arızalarını önleme ve bunlara yanıt verme stratejik vizyonunu ve bu tür vakalara tepkileri içermiştir. Oldukça uzun ve tartışmalı bir müzakere ve koordinasyon sürecinin ardından Şubat 2013'te strateji önerisi iki bölüm halinde yayınlanmıştır. Birinci bölüm Avrupa Komisyonu ile Dış İlişkiler ve Güvenlik Politikası Yüksek Temsilcisi'nin stratejinin kendisi olan AB Siber Güvenlik Stratejisi konulu Tebliği, ikinci bölüm ise Avrupa Komisyonu'nun ağ ve bilgi güvenliğine ilişkin direktif önerini kapsamaktadır (Kovac, 2018).

Siber güvenlik, fiziksel alandaki güvenlik kadar önemlidir. Avrupa Komisyonu 2013 Stratejisi'nin resmi metnine uygun olarak ve siber güvenlik bağlamında tanımlanan beş ilke şunlardır (Avrupa Komisyonu, 2013, s. 4):

- Siber dayanıklılığa ulaşmak,
- Siber suçları büyük ölçüde azaltmak,
- Ortak Güvenlik ve Savunma Politikası (CSDP) ile ilgili siber savunma politikası ve yeteneklerinin geliştirilmesi,
- Siber güvenlik için endüstriyel ve teknolojik kaynakları geliştirmek,
- Avrupa Birliği için tutarlı bir uluslararası siber uzay politikası oluşturun ve temel AB değerlerini teşvik etmek".

Bu stratejik belgenin ardından Avrupa Ağ ve Bilgi Güvenliği Ajansı'nı (ENISA) üye devletlerin siber saldırılarla başa çıkmasına yardımcı olacak şekilde genişletme çabasıyla, 2017'de AB Siber Güvenlik Yasası önerilmiştir. Birliğin Durumu konuşmasında Başkan Jean-Claude Juncker şunları söylemiştir: "Son üç yılda Avrupalıları çevrimiçi ortamda güvende tutma konusunda ilerleme kaydettik. Ancak, konu siber saldırılar olduğunda Avrupa

hala iyi donanımlı değil. Bu nedenle, bugün Komisyon, bizi bu tür saldırılara karşı savunmaya yardımcı olacak bir Avrupa Siber Güvenlik Ajansı da dâhil olmak üzere yeni araçlar öneriyor" (Avrupa Komisyonu, 2017, ss. 2-4).

Rapor, 2016 yılında 4.000'den fazla fidye yazılımı saldırısının gerçekleştiğini ve Avrupalı şirketlerin yüzde 80'inin en az bir siber olay yaşadığını belirtmiştir. AB Siber Güvenlik Yasası, Avrupa Birliği'nin siber altyapısının hazırlık durumunu iyileştirmek amacıyla tehdit istihbaratı paylaşımını iyileştirmek için "Pan-Avrupa Siber Güvenlik Tatbikatları" başlıklı yıllık siber tatbikatlar önermektedir. 2017 tarihli AB Siber Güvenlik Yasası, AB'nin siber güvenlik kapasitesini beş adımlı bir planda artırmayı hedeflemiştir. Planın ilk adımında AB, siber suçlular tarafından siber saldırılarda kullanılan siber silahlara karşı AB'yi savunmak için gerekli araçları ve teknolojiyi sağlamak için ulusal düzeyde üye devlet koordinasyonunu geliştirecek bir Avrupa Siber Güvenlik Araştırma ve Yeterlilik Merkezi kurmayı hedeflemiş Planın ikinci adımında AB, iyileştirme için bir operasyonel plan planı hazırlamayı planlamıştır (Demircan, 2019).

AB'nin siber kapasitesini artırma planının üçüncü adımı, kriz anında üye devletlere yardım etmek için önerilen yeni bir 'Siber Güvenlik Acil Müdahale Fonu' aracılığıyla üye devletler arasında dayanışmanın artırılmasını içermektedir. Birlik çerçevesi. Planın Dördüncü adımı, siber savunma girişimlerini desteklemek için Avrupa Savunma Fonlarından hibeler sağlayarak AB'nin siber savunma yeteneklerini artırma çabalarını açıklamaktadır. Planın bu adımı aynı zamanda NATO ile iş birliği içinde eğitim ve tatbikat platformları oluşturarak siber savunmadaki 'beceri açığını' gidermeyi amaçlıyor. Planın son adımında AB, "siber uzayda çatışma önleme ve istikrar için stratejik bir çerçeveyi destekleyerek, Kötü Amaçlı Siber Faaliyetlere Ortak AB Diplomatik Müdahale Çerçevesini uygulayarak" uluslararası iş birliğini artırmayı amaçlamaktadır (Demircan, 2019, ss. 63-64).

AB'nin 2017 Siber Güvenlik Stratejisi, bu politika alanındaki birincil sorumluluğun Üye Devletlere ait olduğunu ve AB'nin rolünün destekleyici, koordine edici ve tavsiye niteliğinde olduğunu açıkça ortaya koymaktadır. Bu yaklaşım kendi içinde kendi içinde sorunlar doğururken, asıl AB dış

ilişkilerinde stratejik özerklik ve teknolojik egemenlik meseleleriyle mücadele etmeye devam ettiği için zorluk çok daha büyüktür. Bununla birlikte, yeni 2020 AB'nin Dijital On Yıl için Siber Güvenlik Stratejisi, politika içinde ve diğer politika alanlarıyla tutarlılığı artırmaya yönelik iddialı bir planı yansıtmakta, AB'nin dünyanın geri kalanıyla angajmanının tonunu belirgin bir şekilde belirleyerek, siber güçlerini göstererek ve tanımlayarak siber güvenliğe yönelik askeri olmayan ancak boyun eğmeyen bir yaklaşım benimsenmiştir (Kasper & Vernygora, 2021).

Dijital On Yıl için 2020 Siber Güvenlik Stratejisi daha da ileri giderek siyasi ve askeri tehditleri ele alıyor ve daha bütünleşik ve birçok açıdan dışa yayılan bir politika tasarlarken aynı zamanda AB'yi dış bağımlılıklardan ve tehditlerden korumayı amaçlamaktadır. Bu yaklaşım, Stratejinin ikinci bölümünün başlığında sergilenmektedir, "Küresel düşünmek, Avrupalı davranmaktır." Direnç oluşturma ve iç pazara odaklanmanın AB'nin karakterine uygun olarak baskın olmaya devam ettiği yerlerde, AB düzeyinde operasyonel kapasite geliştirme konusundaki girişimleri ve uygulamalı uluslararası angajman, önceki stratejik stratejiye kıyasla hem nicelik hem de derinlik açısından önemli ölçüde artmıştır (Kasper ve Vernygora, 2021).

4.6.3. ABD

Siber güvenlik konusuna ulusal bir bakış açısıyla yaklaşan Cavelty (2014), siber güvenlik açıklarının her geçen gün arttığını ve buna paralel olarak kişisel ve ulusal siber güvenliğin azaldığını savunmaktadır. Eyaletler daha merkezi ve katı kurallar koymak için adımlar atarken, kritik altyapıları korumak ve siber güvenliği artırarak güvenlik açıklarını azaltmak, bireyler kendi özgürlükleri için siber uzaydaki hareket özgürlüklerini korumak istemektedir (Cavelty, 2014).

Amerika Birleşik Devletleri (ABD) için siber uzayda bireylere ve şirketlere (özellikle yazılım şirketlerine) sunulan özgürlük, ulusal siber güvenlik açısından genişleyen güvenlik açıklarını da beraberinde getirmektedir. Bu ikileme çözüm olarak, geniş tanımları ve birbirine bağlı değişkenleri içeren siber güvenlik politikası, bireysel ve ulusal güvenlik öncelikleri dikkate alınarak belirlenerek mutabakat temelinde oluşturulacaktır (Bashir vd., 2017).

ABD, ekonomik ve teknolojik üstünlüğünün de katkısıyla günümüzde siber uzaya hâkim olan en önemli siber güçlerden biridir. ABD'nin siber gücünün temelinde, Soğuk Savaş döneminde Sovyetler Birliği ile askeri rekabet sonucunda geliştirilen ağ teknolojilerinin yeni nesil türevleri bulunmaktadır. ABD'nin siber güvenlik politikasını anlamak için öncelikle bu politikanın hangi bileşenlerden ve aktörlerden oluştuğunu tespit etmekte fayda vardır. ABD'de siber güvenlik konusunda yayınlanan ilk kapsamlı belge, Beyaz Saray tarafından 2003 yılında yayınlanan "Secure Cyberspace" belgesidir. Belge, siber güvenlikle ilgili ulusal ve federal kurumların yönergelerini içeriyor ve toplu siber güvenliği iyileştirmek için eyalet ve yerel hükümet kurumları, özel sektör şirketleri, sivil toplum kuruluşları ve vatandaşların atacağı adımları belirtmektedir. Secure Cyberspace belgesine göre, ulusal güvenliğin sağlanmasında beş ulusal öncelik vardır. Bu öncelikler, bir ulusal siber uzay güvenlik müdahale sistemi, bir ulusal siber uzay güvenlik tehdidi ve savunmasızlık savunma programı, bir ulusal siber uzay güvenlik farkındalığı ve geliştirme programı, hükümetin siber uzay güvenliği, ulusal güvenlik ve uluslararası siber uzay güvenliği iş birliğidir (Aydın, 2021).

2011 yılında yayınlanan siber güvenlik strateji belgesi beş stratejik öncelikten oluşmaktadır. Bunlar, savunma bakanlığının teşkilat geliştirmesi, yeni savunma içeriklerinin edinilmesi, kamu-özel iş birliği, diğer ülkelerle güçlü ilişkiler kurulması ve yaratıcılığın artırılmasıdır. Bu iş birliği, internet yönetişimi, internet siber uzayda özgürlük ve insan haklarının korunmasıdır. İş birliğinde yer alan konular, uluslararası siber uzay gelişmeleri, çevrimiçi insan haklarının teşviki ve korunması, yürürlükteki uluslararası hukukun uygulanması, siber güvenlik kriterlerinin geliştirilmesi, siber ortamda davranış normları gibi uluslararası güvenlik konuları ve siber güvenlik kapasitesinin geliştirilmesidir (Aydın, 2021).

Beyaz Saray, Eylül 2018'de Amerika Birleşik Devletleri'nin siber stratejisini detaylandıran "Amerika Birleşik Devletleri Ulusal Siber Stratejisi" başlıklı bir rapor yayınladı. ABD'nin görevdeki Başkanı Donald J. Trump tarafından imzalanan rapor, "Bu Ulusal Siber Stratejinin yayınlanmasıyla,

ABD'nin artık 15 yıl sonra ilk kez tam olarak ifade edilmiş siber stratejisine sahip olduğunu" iddia etmiştir (Trump, 2018, s. 1).

Söz konusu Rapor, Rusya Federasyonu, İran İslam Cumhuriyeti, Kuzey Kore Halk Cumhuriyeti ve Çin Halk Cumhuriyeti'ni Amerikan uluslararası şirketlerine ve müttefiklerine karşı siber saldırılar düzenlemekle suçlamıştır. Ayrıca raporda, devlet dışı aktörlerin, ABD'nin "ifade özgürlüğü ve bireysel özgürlük" vizyonuyla oluşturulan siber alanı, "ABD'ye ve müttefiklerine kar sağlamak, asker toplamak, propaganda yapmak ve onlara saldırmak" amacıyla kullandığı ve ABD'ye düşman devletlerin korumasından yararlandığı belirtmiştir (Demircan, 2019, ss. 61-62).

2018 ABD Savunma Bakanlığı Siber Stratejisi, Bakanlığın bu tehdidi ele alma ve Ulusal Güvenlik Stratejisi ve siber uzay için Ulusal Savunma Stratejisi önceliklerini uygulama vizyonunu temsil etmektedir. Stratejiye göre, siber uzaydaki çıkarların silahlı çatışma seviyesinin altında iddialı bir şekilde savunmalı ve siber uzay operatörlerin kriz ve çatışmada Müşterek Kuvveti desteklemeye hazır olmasını sağlanması hedeflenmiştir. Ulusal Siber Güvenlik Departmanı'nın siber uzay hedefleri şu şekilde belirlenmiştir:

- Müşterek Kuvvetin çekişmeli bir siber uzay ortamında görevlerini yerine getirebilmesini sağlamak,
- ABD askeri avantajlarını artıran siber uzay operasyonları yürüterek Müşterek Kuvvetin güçlendirilmesi,
- ABD kritik altyapısını, tek başına veya bir kampanyanın parçası olarak önemli bir siber olaya neden olabilecek kötü niyetli siber faaliyetlerden korumak,
- Savunma Bakanlığı'na ait olmayan ağlardaki DoD bilgileri dâhil olmak üzere DoD bilgilerini ve sistemlerini kötü niyetli siber faaliyetlere karşı korumak,
- Kurumlar arası, endüstri ve uluslararası ortaklarla DoD siber iş birliğini genişletmek.

2018 yılında yayınlanan rapor, rakiplerinin ortaya çıkardığı yukarıda belirtilen zorluklarla mücadele etmek için, Amerika Birleşik Devletleri'nin ulusal siber stratejisinin üzerine kurulacağı dört sütunu detaylandırıyor ve açıklıyor. "I. Sütun: Amerikan Halkını, Anavatanı ve Amerikan Yaşam Tarzını Koruyun; Sütun II: Amerikan Refahını Destekleyin; Sütun III: Güç Yoluyla Barışı Koruyun; Sütun IV: Gelişmiş Amerikan Etkisi" Raporda, Trump yönetimi birinci sütunun hedefini "Ulusun bilgi ve bilgi sistemlerinin güvenliğini ve dayanıklılığını artırmak için siber güvenlik risklerini yönetmek" olarak tanımlamıştır. Trump yönetimi, federal güvenliği güvence altına almak için ana hatlarıyla belirtilen öncelikli eylemlere odaklanarak bu hedefe ulaşmayı hedeflemiştir (Demircan, 2019).

4.6.4. İngiltere

İngiltere'nin ilk ulusal siber güvenlik stratejisi, 2009'da yayınlandı ve ardından 2011 ve 2016'da yinelenmiştir. Kasım 2016'da yayınlanan mevcut ulusal siber güvenlik stratejisi, stratejik hedeflere yönelik ilerlemeyi ölçmek için iddialı bir denetim programıyla birlikte ulusal siber güvenlik amaçlarının olgun bir ifadesidir. 2011'deki selefinin ardından ikinci bir beş yıllık (2016-2021) Ulusal Siber Güvenlik Programı olarak çerçevelenmiştir; ancak, ortaya çıkan teknolojilerden ve rakip araçlardaki ve yeteneklerdeki uyarlamalardan kaynaklanan gelişen zorlukları tanımak için 2021 çerçevesinin ilerisini ilgilendirilmektedir. Ulusal siber güvenlik stratejisi, çok sektörlü davranış değişikliği yoluyla daha iyi ulusal siber güvenlik sağlamak için hükümet, endüstri ve toplum arasındaki ortaklıklara öncelik verir; ancak, hükümetin düşüncesindeki önemli bir değişiklik tarafından yönlendirilir (HM Government, 2016).

Hükümet, ulusal siber güvenlik inovasyonunu yönlendirmek için daha önce piyasaya güvenmenin yetersiz "hızlı hareket eden tehdidin önünde kalmak için gereken değişim ölçeği ve hızına" yol açtığını kabul etmiştir. Buna göre hükümet, beş yıl boyunca 1,9 milyar sterlinlik artırılmış mali yatırımla desteklenen birden fazla sektörde güvenli siber davranışları yönlendirmek için daha müdahaleci bir duruş benimsemiştir. Başarılı olursa, hükümet bu merkezi rolden geri çekilecek ve pazarın ve teknolojinin ikiz sürücülerinin Birleşik

Krallık toplumu ve ekonomisinin siber güvenliğini geliştirmeye devam etmesine izin verecektir (Stevens, 2021).

Ulusal Siber Güvenlik Programı, Birleşik Krallık'ın ulusal çıkarlarını ilerleten ve toplu güvenliği destekleyen iki taraflı ve çok taraflı siber girişimleri teşvik etmek için Uluslararası Eylem'e yönelik yenilenmiş bir taahhütle desteklenen Savunma, Caydırma ve Geliştirme olmak üzere birbirini destekleyen üç tema etrafında organize edilmiştir. "Savunma", gelişen siber tehditlere karşı koyar ve kamu eğitimi ve endüstri, özellikle de küçük-orta ölçekli işletmeler ile bilgi alışverişi yoluyla Birleşik Krallık varlıklarının ve toplumunun korunmasını ve dayanıklılığını destekler. Buna, kamu sektörü (gov.uk) alanındaki yaygın siber tehditlerin görülme sıklığını ve etkilerini otomatik araçlar yoluyla "nesnel olarak" azalttığını iddia eden bir Aktif Siber Savunma programı da dahildir (Stevens vd., 2019).

"Caydırıcı", siber uzayda düşman aktörleri belirlemeye ve takip etmeye yönelik eylemlere öncelik verir ve gerekirse onlara karşı saldırgan eylemlerde bulunma hakkını saklı tutar. Siber suç, siber terörizm ve hem devlet hem de devlet dışı yabancı siber aktörlerden kaynaklanan riskleri azaltmak için kriptografi de dâhil olmak üzere egemenlik yeteneklerinin geliştirilmesini vurgulamaktadır. Bu çabanın temel bir bileşeni, Savunma Bakanlığı ve Birleşik Krallık sinyal istihbarat teşkilatı GCHQ genelinde bir Ulusal Saldırı Siber Programının kurulmasıdır. Lonsdale (2016), "Geliştir" kolu, siber güvenlik becerileri açığını azaltmak ve özel sektör inovasyonunu ve büyümesini desteklemek için siber güvenlik eğitimini, araştırmasını ve eğitimini teşvik eder. Bir dizi eğitimsel erişim ve katılım programının yanı sıra, "geliştirmenin" son derece görünür bir bileşeni, Birleşik Krallık üniversitelerinde akredite Siber Güvenlik Araştırmalarında Akademik Mükemmeliyet Merkezleri'dir.

Bu bölümün sonunda şu değerlendirme ve yorumlarda bulunmak mümkündür. Uluslararası ilişkiler, gerek uluslararası toplumu oluşturan aktörlerin heves, hırs ve çıkarları, gerekse uluslararası toplumun hak, hukuk, adalet, demokrasi, özgürlük, eşitlik, terör, egemenlik, hakkaniyet, güç, iktidar vb. siyaset kuramının birçok soyut ve göreceli kavramını kendince yorumlaması nedeniyle, son 200 yıldır hayli karışık, karmaşık ve anarşiktir. Şimdiye kadar

önerilmiş uluslararası ilişkiler kuramları da kendi laf, anlam, anlayış ve önermelerini bu bağlamda bulduğundan, uluslararası ilişkilerin kavramsal çerçevesine de pek fazla mantıklı ve uygun soyutlama araçları sunabildiklerini söylemek pek mümkün değildir. Dolayısıyla, anarşik uluslararası ortam ve ilişkiler, özellikle SSCB'nin 1991'de çökmesi sonrasında, dengesi bozulmuş uluslararası sistemin –doğal olarak- uluslararası ilişkileri esir alacak şekilde hortlattığı terör gibi asimetrik tehditler nedeniyle daha da anarşik hale gelmiştir.

Ancak, özellikle liberal-demokratik Batı ile sözde ekonomik olarak entegrasyon ve işbirliğini yakalamış, ancak gerçekte katı Batı karşıtlığını ideolojik olarak sürdüren Rusya, Çin gibi süper güçler ile liberal-demokratik Batı uluslararası toplumuyla sorun ve uyumsuzluklar yaşayan İran, Kuzey Kore, Belarus gibi devletler, bir yandan artan konvansiyonel silahlanmalarının yanına, nükleer silahlanma imkan kabiliyetlerini de artırma ve/ya kazanmayı koymayı amaçlarken, özellikle 2000'li yıllarda Rusya kaynaklı bilgisayar korsancılığının uluslararası kriz, mücadele, çatışma ve savaşlarda konvansiyonel silahlardan çok daha etkili sonuçlar doğurabilecek, etkin bir asimetrik silah olduğunu keşfetmişlerdir. Zira siber evreni kullanan ve söz konusu ülkelerin vatandaşı birçok bilgisayar korsanı ve onların kullandıkları sanal bilgisayar virüsleri, siber uzayı siber savaş ortamına döndürmüş ve siber saldırıların uluslararası ilişkilerde milli hedef elde etme ve milli menfaatleri sağlama yolunda birer asimetrik savaş aracı, diğer deyişle sanal silah olarak kullanılmasına yol açtığı görülmüştür.

Böylece, son 20 yılda birçok devletin kendi milli siber altyapılarını, sistemlerini, ordularını, savunma mekanizmalarını ve karşı-taaruz konseptlerini oluşturduğu görülmüştür. Devletlerde gerek kamuda gerek ordularda siber savunma/taaruz kurum ve kuruluşları, siber komutanlıklar, askeri siber silah teşkilleri, siber güvenlik birimleri, siber güvenlik stratejileri, siber güvenlik doktrinlerinin ivedilikle oluşturulduğu gözlemlenmiştir. Uluslararası illegal yapılanmaların, kimi zaman serbest, kimi zaman devlet destekli olarak siber savaşlarda kullanılmaya başladığı ortam, doğru-yanlış herkese cazip gelmeye başlamıştır. Zira siber evren, bilinmezliklerle dolu, karanlık, zamansız, kuralsız, sınırsız ve çözümsüz bir âlemdir. Dolayısıyla, böylesi bir dünya da

dolandırıcılıktan korsanlığa, aldatmacadan istismara, saldırıdan onursuzluğa kadar her türlü illegalitenin olması, uluslararası topluma bugün artık pek de şaşırtıcı gelmemektedir.

Bu bağlamda, ulusal güvenlik de olduğu kadar, uluslararası ilişkilerde de siber güvenliğin günümüzün gelişmiş bilişim dünyasında en önemli konulardan birisi haline geldiğini savlamak mümkündür. Keza bunda esas faktör, siber savaşın çok ucuz, çok hızlı, çok gizli, çok hukuksuz, çok kuralsız ve çok sınırsız olmasındandır. Diğer deyişle, günümüzde herşeyin neredeyse bilgisayarlar, akıllı telefonlar vb. eçhizeler marifetiyle sanal evrende ve bilişim sistemleri üzerinden gerçekleştirildiği göz önüne alınacak olursa, uluslararası ilişkiler bakımından da siber güvenliğin bugün yurttaş, şirket, sivil toplum, devlet ve ulus-ötesi örgütlenmelerin olmazsa olmazı haline geldiğini iddia etmek pek de yanlış olmayacaktır. Bu yüzden de gelişmiş bilişim sistemi altyapılarını hemen her sektörde kullanan gerek ABD, İngiltere, Kanada, Avustralya, Hindistan, Türkiye vb. G-20 üyesi devletlerin, gerekse BM, NATO, AB, ASEAN, BRICS vb. uluslararası örgütlerin siber güvenlik politikaları benimseyip, kapsamlı siber güvenlik stratejileri ve doktrinleri geliştirdikleri görülmektedir. Ve de bu stratejilerin, yakın bir gelecekte çok daha fazla sıklıkla güncelleştirilmeye muhtaç dokümanlar haline geleceğini söylemek mümkündür.

5. RUSYA KAYNAKLI SİBER SALDIRILAR

5.1. Rusya Federasyonu'nun Siber Güvenlik Strateji Belgeleri

Günümüzde teknolojik gelişmelerin artan rolü göz önüne alındığında, siber alandaki gelişmeleri göz ardı eden devletlerin önemli güvenlik sorunlarıyla karşı karşıya kalabileceği söylenebilir. Bu anlamda devletler teknolojik gelişmeleri yakından takip etmeli; tüm kurum ve stratejilerini siber uzay ile uyumlu hale getirerek siber saldırılara karşı kapasitelerini yeniden düzenlemeleri gerekmektedir. Nitekim pek çok devlet gibi Rusya'nın da siber uzay alanında önemli bir gelişme kaydettiği biliniyor. RF'nin güvenlik temelli deneyimleri Afganistan Savaşı sırasında başlamıştır (Guliyeva, 2021).

Rusya'nın siber stratejisinin temelini oluşturan programın, 1980'li yıllarda Sovyetler Birliği Ordusu'nda görev yapan Mareşal Nikolai Ogarkov tarafından başlatılan "Askeri İşlerde Devrim" programı olduğu kabul edilmektedir. Anılan Programın, Sovyetler Birliğinin Silahlı Kuvvetlerini daha etkin kılmak için ağ teknolojilerine ve teknik operasyonlara önem verdiği bilinmektedir. Ayrıca Rusya'nın siber uzay politikasını etkileyen en önemli faktör, Rus siyasetinin tarih boyunca savaş temelli bir kültüre sahip olmasıdır. 1994-1996 yılları arasında yaşanan Çeçen Savaşı sırasında siber ortamın sağladığı imkânlar kullanılarak Rusya aleyhine olumsuz haberlerin yayılması, Rus güvenlik ve askeri bürokrasisinde ağ teknolojileri ve bilgi harbi alanındaki gelişmeleri teşvik etmiştir (Kari, 2019).

Rusya'nın savaşa bakışının ana hatlarını çizmek, Rusya'nın siber stratejisini kavramak için kritik öneme sahiptir; keza Rusya'nın siber güvenliğe bakış açısı, Rusya'nın savaşın doğasına ilişkin gelişen anlayışıyla iç içe geçmiş durumda ve bilgi savaşı kavramıyla şekillenmektedir. Siber güvenlik, Rus tartışmalarında Batılı bir kavram olarak algılanırken, anlamsal Rusça karşılığı bilgi güvenliğidir (Lilly & Cheravitch, 2020).

Askeri bilginler ve resmî belgeler, bilgi savaşı ve bilgi güvenliğinin biraz farklı tanımlarını sunar, ancak bilgi güvenliğinin, teknik olduğu kadar psikolojik veya bilişsel bir bileşeni de olan bir terim olan bilgi savaşının bir bileşeni olduğu genel olarak kabul görmüştür. Bilgi savaşı, devletlerarası çatışmanın ayrılmaz bir parçası olup amacı teknik ve psikolojik araçları kullanarak düşmana bilgi üstünlüğü sağlamak iken, siber operasyonlar ise devletin bir savaş alanı olarak kabul edilen bilgi ortamına hâkim olmak için kullandığı bir mekanizmadır (Thomas, 2019).

21 Ocak 2000'de yürürlüğe giren "Ulusal Güvenlik Konsepti" ve 9 Eylül 2000'de Rusya Devlet Başkanı Vladimir Putin tarafından kabul edilen "Bilgi Güvenliği Doktrini" resmî belgeler arasında yer almaktadır. 2011 yılında yayınlanan "Rus Silahlı Kuvvetlerinin Bilgi Alanındaki Faaliyetlerine İlişkin Kavramsal Görüşler" adlı belge, Rus Ordusunun bilgi çağındaki faaliyetlerini yasallık, iş birliği, yenilikçilik ve etkileşim gibi bazı ilkelere dayandırmıştır. 2013 yılında kabul edilen "Rusya'nın Dış Politika Konsepti" metni de ağ diplomasisi hakkında kritik bilgiler içermektedir (Guliyeva, 2021).

2000 Ulusal Güvenlik Konsepti, Rusya'nın ulusal güvenliğinin bilgi savaşları kavramını geliştirirken bilgi alanına hâkim olmaya çalışan ülkeler tarafından tehdit edildiğini vurgulamıştır. Güvenlik Konsepti, bilgi savaşının hem teknik hem de psikolojik yönleriyle ilgili tehditlere odaklanarak terimin bütüncül bir anlayışını sunmuştur. Rusya'nın 2010 Askeri Doktrini, bilgi savaşının statüsünü daha da yükseltti ve bilgi savaşının artan rolünü ilk kez çağdaş askeri çatışmaların bir özelliği ve Rusya ordusunun bilgi savaşı kuvvetleri ve araçları geliştirmektir (Lilly & Cheravitch, 2020).

2000 Doktrini; "bilgi, bilgi altyapısı, bilginin toplanması, üretilmesi, dağıtılması ve kullanılmasında yer alan varlıkların yanı sıra sonuçta ortaya çıkan halkla ilişkileri düzenleyen bir sistemin bir kombinasyonu" olan bilgi alanının geniş bir tanımını sağladı. Bu tanım, Rusya'nın bilgi alanının teknik ve bilişsel bir bileşen içerdiği anlayışıyla uyumludur. Bu geniş tanıma dayalı olarak, kavram bilgi güvenliğine yönelik çok çeşitli tehditleri içerir (Giles, 2016).

Bunlar, bilgi ve telekomünikasyon tesislerinin güvenliğine yönelik tehditler gibi daha teknik tehditlerden ve "bilgiyi işleme, depolama ve iletmeye yönelik teknik araçlarda bilgileri ele geçirmek için elektronik cihazların kullanılması"nı içeren sistemler ve toplumsal uyuma yönelik daha geniş tehditler arasında değişir. "Rus nüfusunun manevi, ahlaki ve yaratıcı potansiyelinde azalma" gibi 2013 Güvenlik Konseyi'nin Uluslararası Bilgi Güvenliğine İlişkin Temel İlkeleri, bu geniş anlayışı ve bilgi güvenliği ile ilgili tehdit yelpazesini doğruladı ve bilgi teknolojisini siyasi amaçlar için kullanılabilecek bir silah olarak görmüştür (Thomas, 2019).

Güncellenen 2016 Bilgi Güvenliği Doktrini, çeşitli düşmanlar tarafından bilgi alanında Rusya'ya yönelik artan tehdidi yeniden vurgulayarak kavramsal öncüllerinin ruhuna uygun olarak devam etti. Doktrin, öncelikle yabancı aktörler tarafından yönlendirilen bilgi bilişsel alanından kaynaklanan artan tehditleri ve bunların sosyal değerler ve istikrar üzerindeki etkilerini vurguladı. Bu belgeler, Rusya'nın bilgi alanındaki duruşunun, devleti kendisini savunmaya zorlayan Rusya'ya yönelik tehditlere yanıt olarak şekillendiği inancını göstermektedir. (Lilly & Cheravitch, 2020).

5.2. Rus Silahlı Kuvvetleri ile Rus İstihbarat Servislerinin Siber Kapasiteleri

Rusya, dünya çapında dezenformasyon, propaganda, casusluk ve yıkıcı siber saldırılar yürütmek için gelişmiş siber yetenekler kullanmaktadır. Bu operasyonları yürütmek için Rusya, çeşitli güvenlik ve istihbarat teşkilatları tarafından denetlenen çok sayıda birime sahiptir (Hakala & Melnychuk, 2021).

Rus Askerî İstihbarat Direktörlüğü (Glavnoye Razvedyvatel'noye Upravleniye/GRU), Rus İstihbarat Servisi (SluzhbaVneshney Razvedki/SVR), Rus Federal Güvenlik Servisi (Federalnaya Slujba Bezopasnosti/FSB)'nün gerek Rus kriminal örgütleri ile olan illegal bağlantıları gerekse de tek başlarına sahip oldukları siber kapasiteleri, RF'nin siber savunma ve saldırı kapasitesini belirleyen temel faktörlerdendir. Bu servislerden FSB ve SVR, RF Devlet Başkanı'na doğrudan bağlı durumda iken, GRU Savunma Bakanlığı'nın bir

parçası konumunda ve RF Silahlı Kuvvetleri emrinde görev yürütmektedir (Heickerö, 2015).

Sovyet sonrası Rusya'nın büyük bölümünde, FSB, harici siber operasyonların "komuta yüksekliklerini" sürdürmüştür. 1990'larda ve 2000'lerin başlarında Rus internetinin düzenlenmemiş alanında FSB, bağımsız Rus bilgisayar korsanlarını ve uzmanları siber operasyonlara dâhil etmesine veya zorlamasına yardımcı olan ilişkiler geliştirmiştir. Katmanlar halindeki gayri resmi bilgisayar korsanları, Rusya'nın siber yetenekli kadrolar geliştirmesine uzun süredir engel olan insan sermayesi sorunlarının aşılmasına yardımcı olmuştur (Turovsky, 2018).

Örneğin, FSB'nin önde gelen bilgisayar korsanlığı departmanlarından biri olan Bilgi Güvenliği Merkezi'ndeki (CIS) anonim bir kaynak, birimin personel eksikliklerini gidermek için yasa dışı bilgisayar korsanları çalıştırdığını iddia ederken, başka bir kaynak önde gelen CIS bilgisayar korsanlarından birinin, dış destek alırken genellikle "Rusya'nın yardıma ihtiyacı olduğu bir atmosfer" yaratmıştır (Darıcılı, 2019, ss. 136-138).

FSB'nin, 2003'te dağıtılan ABD Ulusal Güvenlik Teşkilatı'nın gevşek bir benzeri olan Federal Hükümet İletişim ve Bilgi Ajansı'nın (FAPSI) ve FSB'nin teknolojik araştırmalarına bir yılı aşkın süredir yardımcı olan Kvant Bilimsel Araştırma Enstitüsü'nün büyük bir kısmının mirası FSB'ye kaldı. Bu miras, FSB'ye saldırgan bir siber yeteneği geliştirmede önemli bir avantaj sağlamıştır (Darıcılı & Özdal, 2017).

FSB, büyük ölçüde KGB'nin halefi olarak görülen en güçlü özel servis olarak kabul edilir. Başlangıçta yurtiçi odaklı olmasına rağmen, faaliyetleri giderek artan bir şekilde yurtdışında yürütülmektedir. Hizmet, siber uzay da dâhil olmak üzere karşı istihbarat ve istihbarat toplamadan sorumludur. FSB ayrıca Rusya'nın iç bilgi alanının güvenliğini sağlamada önemli bir aktördür ve Roskomnadzor gibi federal kurumlarla iş birliği içinde çalışmaktadır (Lilly & Cheravitch, 2020).

İletişim, Bilgi Teknolojisi ve Kitle iletişim araçları), Minsifri (Rusya Federasyonu Dijital Kalkınma, İletişim ve Kitle İletişim Bakanlığı) ve

diğerlerini içerir. Örneğin, FSB'nin telefon dinleme yetkisi vardır. Rusya'daki tüm İnternet servis sağlayıcılarının yer almakla yükümlü olduğu bir izleme sistemi aracılığıyla Rusya veri trafiğini denetlemekle görevlidir (Lilly & Cheravitch, 2020).

Batılı istihbarat toplulukları, FSB'yi casusluk faaliyetleri olan Yılan, Uroburos ve Zehirli Ayı olarak da bilinen Turla APT (gelişmiş kalıcı tehdit) ile ilişkilendirmiştir. Programlama kalitesi, Rusya ile bağlantılı olduğu iddia edilen diğer saldırganlardan önemli ölçüde daha sofistike ve altyapısı daha karmaşıktır ve hedefleri daha dikkatli seçilir ve daha uzun ömürlüdür. ABD ordusu içinde keşfedilen "Agent.btz" solucanından Turla'nın bilinen en eski siber casusluk gruplarından biri olduğuna inanılmaktadır (Hakala & Melnychuk, 2021).

SVR (Foreign Intelligence Service), iki dış istihbarat teşkilatından biridir (diğeri GRU'dur) ve ana görevleri insani ve stratejik istihbarat faaliyetleridir. Siber uzayı yalnızca casusluk için değil aynı zamanda sabotaj ve bilgi operasyonları için de kullanan GRU'nun aksine, SVR, Kremlin'in politikacıların ve politika yapıcıların planlarını ve amaçlarını anlamasına yardımcı olabilecek sırları arayarak çoğunlukla geleneksel casusluk amaçları için bilgi çalmaktadırlar (Hakala & Melnychuk, 2021).

SVR, Rusya'nın birincil sivil dış istihbarat servisidir. Dış istihbaratın insan, sinyal, elektronik ve siber yöntemlerle toplanmasından sorumludur. Çoğu gözlemci, SVR'nin gizliliği korumaya ve tespit edilmekten kaçınmaya güçlü bir vurgu yaparak çalıştığını kabul etmektedir. SVR ile bağlantılı olduğu bildirilen çoğu siber operasyon, istihbarat toplamaktır. SVR'nin aynı zamanda yüksek düzeyde teknik uzmanlığa sahip olduğu ve genellikle güvenliği ihlal edilmiş ağlar içinde erişim kazanmaya ve bu erişimi sürdürmeye çalıştığı bilinmektedir (Lilly & Cheravitch, 2020).

Analistler ve gözlemciler, SVR'nin son derece yetenekli ve profesyonel olduğunu kabul ettiler. GRU siber birimlerinin aksine, SVR istihbarat toplamaya ve hedeflenen ağlara erişim kazandığında tespit edilmeden kalmaya odaklanmış görünüyor. ABD hükümeti, SVR'yi 2016 ABD başkanlık seçimleri sırasında siyasi kampanyaları hacklemekten sorumlu iki Rus siber biriminden

biri olarak tanımladı. Gizlice çalışmaya odaklanılmasına rağmen, 2018'de bir Hollanda gazetesi, Hollanda istihbaratının SVR'nin altyapısını tehlikeye attığını ve ABD hükümetine çok önemli bilgiler sağladığını bildirdi. Özel siber güvenlik firmaları, SVR'nin daha sonra etkinliğini azalttığını kaydetmiştir (Darıcılı, 2019).

Ancak, daha yakın zamanlarda SVR etkinliğinin arttığı ve birimin çok sayıda siber casusluk operasyonuyla bağlantılı olduğu bildirildi. Örneğin, Nisan 2021'de ABD hükümeti, ABD hükümeti ve özel sektör ağlarına sızmak için tedarik zinciri güvenlik açıklarından yararlanan SolarWinds saldırısından APT 29'u sorumlu olarak tanımladı. Bir siber güvenlik danışma uyarısında, ABD hükümeti APT 29'un "sofistike olarak farklılık gösteren bir dizi ilk istismar teknikleri ve güvenliği ihlal edilmiş ağlarda gizli izinsiz giriş ticaret aracıyla birleştiğinde siber istismar yoluyla ABD ve yabancı kuruluşlardan istihbarat aramaya devam edeceğini" belirtti (Darıcılı & Özdal, 2017, ss. 127-128).

Genellikle GRU olarak anılan Genelkurmay Ana Müdürlüğü, Rusya'nın askeri istihbarat teşkilatıdır. Daha önceki siber operasyonlarda FSB'ye "arka koltukta oturan" olarak algılanmıştır. 2007'de Estonya'ya ve 2008'de Gürcistan'a karşı GRU, saldırgan siber operasyonlarda daha görünür hale gelmiştir. Batılı istihbarat teşkilatları, en son önemli saldırıları bu teşkilata atfetmektedir (Lilly & Cheravitch, 2020).

GRU'nun operasyonel riske yönelik görünüşte yüksek toleransı, büyük ölçekli saldırılardan çok daha sık sessiz casusluk çabalarından oluşan geleneksel olarak sinsi siber operasyonlar alanıyla birçok yönden uyumsuzdur. 2016'nın sonlarında tutuklanan eski bir FSB siber görevlisi, muhtemelen GRU bilgisayar korsanlarını onlar hakkında bilgi sızdırarak ifşa etme çabasıyla, GRU'nun "küstahça, kabaca ve acımasızca sunuculara girdiğini" iddia etti ve bu da her zaman onların atfedilmesine yol açmıştır (Turovsky, 2018, s. 198). GRU'nun bariz yanlış adımları ne olursa olsun, kuruluş en azından Başkan Putin'in güvenini alenen koruyor ve Rus siber ve bilgi operasyonlarının sürekli olarak ona atfedilmesi, GRU'nun bu kampanyaları yürütmeye devam edeceğini göstermektedir (Balforth, 2018). GRU, bilgi yüzleşmesinin hem bilgi-teknik hem de bilgi-psikolojik boyutları için etkin bir şekilde kullanılabilecek

yeteneklere sahiptir. Geleneksel olarak sinyal istihbaratı ve kriptografiden sorumlu olan 85. Özel Hizmet Merkezi (Birim 26165) ve Özel Teknolojiler Ana Merkezi (Birim 74455), bilgisayar tabanlı operasyonlardan sorumlu olmuştur (Lilly & Cheravitch, 2020).

5.3. RF'nin Siber Alanının Yapısal Özellikleri

Siber uzayı düşündüğümüzde, sınırları sanal olduğu ve yalnızca yapay olarak yeniden üretildiği için gerçek dünya ve coğrafyasının aksine, genellikle soyut bir bilgi alanı hayal ederiz. Bununla birlikte, egemen devletler için siber uzay yeni izleme ve düzenleme sorunları sunmaktadır. Örneğin, IP adreslerini (bir proxy aracılığıyla) atlamaya yönelik mevcut teknikler, sanal olarak "ülke değiştirebilen" kullanıcıların izlenmesini ve bu nedenle, özellikle sansür uygulayan eyaletler için yasa çıkarmayı zorlaştırır. İnternetin arkasındaki ilkeler, diğer deyişle merkezi olmayan bir organizasyon, makinelerin diğer makinelerle iletişim kurmasını sağlayan küresel olarak standartlaştırılmış dijital protokoller ve siyasi sınırları büyük ölçüde göz ardı eden bilgi aktarımları bu belirsizliği desteklemektedir. Rusya böyle bir temsile karşı çıkıyor. Aslında, liderlerinin internete ve hatta dijital ağların nasıl organize edildiğine ilişkin stratejik kavrayışları, egemenlik ve kimlik kavramlarının merkezi olduğu bir vizyonu yansıtıyor; Amerika Birleşik Devletleri ve Batı merkezidir (Limonier, 2014).

Rusya'nın hedeflerini ve yapısal siber asimetriyi anlamak için bazı temel kavramların tanıtılması gerekiyor. İlk olarak, kapalı bir ulusal ağ, küresel internetten bağlantısı kesilebilen ve hala devlet idaresi, ulusal ekonomi, sivil toplum ve ordu için iletişim sağlamada normal şekilde işlev gören bir ulusal ağı tanımlayan teorik bir kavramdır. Açık bir ulusal ağ, interneti yönetmenin mevcut Batı tarzına dayanan teorik bir devlet ağıdır. İkincisi, internetin Rus ulusal kesimi, kapalı bir ulusal ağın gerçek hayattaki bir örneğidir. İnternet altyapısı ve diğer bileşenlerden oluşur. Rusya'da ve onun egemen yasal yetkileri altında bulunan ağlar ve sistemler. Siber uzayın sınırlarını tanımlayan, politik, idari ve hukuki bir kavramdır (Ristolainen & Kukkola, 2019).

Üçüncüsü, birleşik bir bilgi alanı, Rusya rejiminin internetin Rus ulusal bölümünü geliştirmesini anlaşılır ve makul kılan stratejik-kültürel bir fikirdir. Fikir, siber uzayın bu bölümünün sibernetik ilkelere göre nasıl düzenlenmesi gerektiğini açıklar. Dördüncüsü, ulusal bir bilgi güvenliği ve savunma sistemleri sistemi, devletin ulusal kesimini belirlemek, korumak ve kontrol etmek için birbirine bağlı araç ve yöntemlerin bir toplamıdır. Sistemler sistemi, devleti ve egemenliğini korur ve bir ulusal güç kaynağı olarak işlev görür. Nihai durumunda, birleşik bilgi alanının bir tezahürü olarak, internetin tüm ulusal kesimini içerir. İlki dışındaki tüm bu kavramlar, Rus sivil ve askeri akademisinin düşüncesine dayanmaktadır (Ristolainen & Kukkola, 2019).

Rus stratejik düşüncesi, "siber uzay" terimini ve onun ima ettiği hayali dünyayı, 1990'ların sonunda ABD özel ve kamu kuruluşları tarafından biçimlendirilmiş ve büyük ölçüde dönemin çağdaş küreselleşme olasılıklarından ilham alan temsili bir dünya modeline dayanan bir şey olarak görmektedir. Sovyetler Birliği'nin düşüşü ile 11 Eylül 2001 arasında Ruslar "siber uzay" yerine "bilgi alanı"ndan bahsetmeyi tercih etmişlerdir. Bu terminolojik ayrım hiçbir şekilde retorik değildir. Bunun yerine, İnternet ve dijital dünya hakkında kökten farklı kavramlar önerir. Aslında bilgi alanı kavramı, yalnızca interneti değil, aynı zamanda destek çerçevesini ve bilgi dağıtım araçlarını (yazılı medya, televizyon, radyo vb.) içeren siber uzaydan çok daha geniş bir gerçekliği destekler. Aslında, mevcut Rus stratejik düşüncesi, siber uzayın varlığını münhasır ve benzersiz olarak tanımıyor ve bunun yerine kendi özel düzenlemesini gerektiriyor. Rusya, internet gibi dijital ağların, devletin olağan düzenleme hakkına sahip olduğu başka bir medya biçimi olduğuna inanmaktadır. Kısacası, Rus anlayışı büyük ölçüde yetkililerin egemenlik konusuna atfettiği önem tarafından şartlandırılmıştır ki, bu konu siber uzayı bir kavram olarak ortadan kaldırmaya, onun yerine siber uzayı bir egemenlik alanı olarak benimsemeye eğilimlidir (Darıcılı, 2019).

Rusya'da bilgi alanı kavramı esas olarak karar verme çevreleri ve doktriner metinlerle sınırlı olsa da hükümet ve kullanıcılar arasında İnternet'in nasıl temsil edileceği konusunda aşılmaz bir boşluk yoktur. Aksine, ötekilik ve enformasyonel alanın ima ettiği belirli bir egemenlik biçimini savunma

nosyonu, siber uzayın bir bölümünü bölgeselleştirmeye, diğer deyişle ağın bir parçası için bir anlatı yaratmaya yönelik büyük bir girişimde bulunabilmektedir. Ortak bir dil, uygulama ve değerlere, bir başka deyişle Runet'e (Rus İnterneti) dayanmaktadır (Kelly, 2014).

Runet aynı zamanda, Sovyet dönemine kadar uzanan tarihi, onu bugün harekete geçiren jeopolitik dinamikleri anlamamıza izin veren bir kablolama ve rekabet meselesidir. Uygulamada, mevcut Rus ağlarının fiziksel ve mantıksal organizasyonu, 30 yılı aşkın bir süre önce yapılan stratejik ve politik seçimlerin sonucudur. Bu miras, Runet'in belirli fiziksel ve mantıksal yönlerini açıklarken, aynı zamanda, egemen bir internet konusundaki söylemin öncelikle ağların kontrolü üzerindeki rekabetin sonucu olduğu Rusya'da siber uzayın nasıl önemli bir siyasi sorun haline geldiğini anlamamıza yardımcı oluyor. Bugün ve oldukça yakın zamanda, Runet'in ve hükümet kontrol mekanizmalarının resmi imajı sorgulanıyor ve bu da Rusya'da ağların oynadığı rol konusunda derin bir ayrışmayı ortaya koymaktadır. Rus siber uzayı, kökenleri Soğuk Savaş'a kadar uzanan belirli bir fiziksel ve insani örgütlenme tarafından şekillendirilen çok çeşitli hırslar ve jeopolitik temsiller için bir rezervuar olma özelliğine sahiptir (Limonier, 2014).

5.4. Rusya Federasyonu Kaynaklı Olduğu İddia Edilen ve Enformasyon Savaşı Enstrümanları Kullanılarak Yürütülen Siber Saldırılar

Siber alandaki düşmanların davranışlarını anlamak, siber savaşın teknik doğası nedeniyle genellikle zor olabilmektedir. Siber savaş ve bilgi savaşı söz konusu olduğunda Rusya en gelişmiş yeteneklerden birine sahiptir ve aynı anda stratejik avantaj ararlar ve beklenen sürprize sürprizle karşılık vermeye çalışırlar. Rus yetkililer, herhangi bir dış güç veya saldırıyla karşılaşmaları durumunda ve savaş dışındaki durumlarda kullanılmak üzere siber teknolojiler ve savaş kullanarak iyi bir saldırı sistemi oluşturmak için çalıştılar. Bu siber yöntemleri Estonya, Gürcistan ve Ukrayna örneklerinde birkaç kez test ettiler (Covington, 2016).

Moskova'ya atfedilen siber operasyonlar stratejik bir boşlukta yürütülmemektedir. Bunlar, daha geniş jeopolitik değerlendirmeler ve

Rusya'nın askeri, istihbarat ve siyasi liderliğinin kurumsal kültürünün yanı sıra, Moskova'nın topyekûn çatışmanın yetersiz kaldığı asimetrik devletler arası rekabete gelişen yaklaşımı tarafından etkinleştirilmekte ve şekillendirmektedir. Rusya'nın algılanan düşmanlara karşı siber ve bilgi operasyonlarını kullanmasının ardındaki motivasyonları ve kısıtlamaları anlamak için karar vericiler, mevcut politika ve doktrini, özellikle de Sovyet sonrası dönemden bugüne kadarki gelişimini kapsamlı bir şekilde incelemeli ve aynı zamanda siber saldırıları ve dijital etki kampanyalarını yürütmekten sorumlu aktörlerin daha sofistike bir şekilde anlaşılmasıdır. Bu, Rusya'daki yayınların ve resmi belgelerin araştırılmasını ve bu çabaların arkasındaki aktörlere yönelik daha incelikli ve güncellenmiş araştırmaları içermektedir (Lilly & Cheravitch, 2020).

Rusya, siber savaşı Batı'nın sahip olduğundan farklı görmekte; bu, taktiklerini savaş dışında ve bunun yerine siyaset söz konusu olduğunda nasıl kullandıklarından açıkça anlaşılmaktadır. Bot ağları, DoS (Hizmet Reddi) ve DDoS (Dağıtılmış Hizmet Reddi) saldırıları olan aynı araçların çoğunu siber savaş için kullanmaya devam ettiler. Rusya'nın bilgi güvenliğine ve bilgi tehditlerine yaklaşımının temel ilkeleri, Rusya'nın beyan politikasından tutarlı bir şekilde açıktır ve bunların uygulanmasının gelişimi, bilgi güvenliğine yaklaşımı ortaya koyan çok sayıda siyasi Rus belgesi aracılığıyla izlenebilmektedir. Araçların, lojistik ve yöntemlerin çoğu benzer olduğu için siber suçlar, siber terörizm ve siber savaş, Rusya'nın ağlarını büyütmesi ve geniş ölçekte kullanması kolaydır (Connell & Vogler, 2017).

5.4.1. Estonya'ya yönelik siber saldırılar

Nisan 2007'de Estonya Hükümeti, ülkenin Sovyetlerin Nazilerden kurtuluşunu anma anıtını Tallinn'de daha az göze çarpan ve görünür bir yere taşımıştı. Bu karar, Rusça konuşan azınlıklar arasında isyanı ve Estonya'nın kritik ekonomik ve siyasi altyapısını hedef alan siber terörizmi tetiklemiştir. Rusya ve Estonya arasındaki sorunlu ilişki, modern devletlerden yüzlerce yıl öncesine dayanmaktadır. Estonya'daki Rus azınlık ile etnik Estonyalılar arasındaki gerilim, siber saldırı gerçekleştiğinde uzun süredir devam ettiği bilinmektedir. Estonya'daki Rus azınlıklar, heykelin kaldırılması ile

kimliklerinin hedef alındığını hissederek kendilerini dışlanmış hissettiler ve bu da ulusal tepkiye yol açmıştır (Herzog, 2011).

27 Nisan'dan 18 Mayıs 2007'ye kadar üç hafta boyunca, Estonya İnternet altyapısının bileşenleri, Dağıtılmış Hizmet Reddi (DDoS) saldırılarına, web sitesi tahrifatlarına, DNS sunucusu saldırılarına, toplu e-postaya ve yorum spam'ına boyun eğdirildi. Bu saldırılar, muhtemelen bir ulusa karşı siyasi bir çatışmada zorlayıcı bir araç olarak yönlendirilen ilk saldırılardır. Saldırılar sırasında Estonya, bir yanda yeni seçilen hükümet ve destekçileri ile diğer yanda Rus etnik azınlık grubu arasındaki bir iç çatışmanın içinde idi (Connell & Vogler, 2017).

Siyasi kurumlar saldırıların ilk hedefleri idi. Estonya Başbakanı Andrus Ansip ve diğer önde gelen politikacılara spam gönderildi. Estonya parlamentosunun e-posta hizmetleri, olağandışı veri yükünü artık kaldıramayacakları için geçici olarak kapatılmak zorunda kalmıştır. Estonyalı haber kuruluşu Postimees Online, sunucularına yönelik iki DDoS saldırısının kurbanı oldu ve ağlarına yabancı erişimi kapatmak zorunda kalmış, böylece Estonyalıların seslerini yurt dışında duyurma şansları sınırlanmış idi. Buna ek olarak, Postimees Online'daki tartışma forumları, botlar tarafından Başbakan'a kötü söz söyleyen ve hakaret eden yorumlarla spam edilmiş, Postimees Online'ın başkanı siber saldırıları "tarafsız ve bağımsız gazeteciliğe yönelik bir saldırı" olarak nitelendirmiştir (Herzog, 2011, ss. 42-44).

2007'de Estonya'ya yönelik saldırılara verilen çok uluslu yanıtlar, devletlerin veya devlet dışı aktörlerin interneti bir silah olarak kullanarak müttefiklerinin egemenliğini tehdit etmesi nedeniyle ülkelerin tarafsız ve kayıtsız kalmayacağına işaret etmiştir. Yine de Estonya'daki olaylara uluslararası tepkinin önceden var olan güvenlik topluluklarının sınırları içinde gerçekleştiğini not etmek önemlidir. Rusya siber saldırılara göz yumdu ve teşvik etti ve Kremlin, saldırılardan sorumlu bilgisayar korsanlarıyla bile iş birliği yaptığı iddia edildi (Herzog, 2011).

5.4.2. Gürcistan'a yönelik siber saldırılar

Ağustos 2008'de Rus Ordusu Gürcistan'ı işgal etiği süreçte sayısız, askeri kampanyaya koordineli siber saldırılar eşlik etmişti. Bu, büyük kara muharebe operasyonlarıyla birlikte yürütülen büyük ölçekli bir bilgisayar ağı saldırısının (CNA) ilk örneğini temsil etmiştir. Saldırının Rus hükümetiyle doğrudan bir bağlantısı yoktu, ancak Gürcistan üzerinde önemli bir bilgi ve psikolojik etkisi olmuş Gürcistan dış dünyadan etkili bir şekilde izole edilmiştir. Güvenlik uzmanları, Rusya'nın Gürcistan'a yönelik siber kampanyasının iki aşamasını belirlemiştir (Shakarian, 2011).

İlk aşama, 7 Ağustos akşamı Rus bilgisayar korsanlarının Gürcistan haberlerini ve hükümet web sitelerini hedef almasıyla başlamıştır. Rus Askeri Tahmin Merkezi yetkilisi Albay Anatoly Tsyganok, bu ilk eylemlerin, Gürcülerin hafta başlarında Güney Osetya medya sitelerini hacklemelerine bir yanıt olduğunu söylemiştir. İddia edilen karşı saldırıların kara harekâtından yalnızca bir gün önce gerçekleşmiş olması, birçok güvenlik uzmanının bilgisayar korsanlarının işgal tarihini önceden bildiklerini öne sürmesine yol açmıştır. Saldırının ilk aşamasında Rus bilgisayar korsanları öncelikle dağıtık hizmet reddi (DDoS) saldırıları gerçekleştirdi. DDoS saldırılarını kategorize etmenin bir yolu, semantik ve kaba kuvvet saldırıları arasında ayrım yapmaktır. Bu aşamadaki DDoS saldırıları öncelikle botnet'ler tarafından gerçekleştirildi. Bu ilk aşamada, saldırılar öncelikle Gürcistan hükümeti ve medya web sitelerini hedef aldı. Rus bot ağları, bu hedeflere saldırmak için kaba kuvvet DDoS'ye güvendi. Gürcü ağları, kırılgan yapıları nedeniyle, Rus bilgisayar korsanlarının bir yıl önce saldırdığı Estonya ağlarına göre sele karşı daha hassastı (Nazario, 2008).

İkinci aşamada, Gürcü medyası ve hükümet web siteleri saldırıları almaya devam etti, ancak Rus siber operasyonu, finans kurumları, işletmeler, eğitim kurumları, Batı medyası (BBC ve CNN) ve Gürcü bir hacker web sitesini içeren genişletilmiş bir hedef listesine zarar vermeye çalıştı. Bu sunuculara yapılan saldırılar yalnızca DDoS'u değil, aynı zamanda web sitelerinin tahrif edilmesini de (örneğin, Rus yanlısı duvar yazıları) içeriyordu. Gürcistan Devlet Başkanı Mikheil Saakashvili'yi Adolf Hitler'e benzeten bir resim gibi hükümet

sitelerinde). Ayrıca, birkaç Rus bilgisayar korsanı, spam e-posta kampanyası başlatmak için Gürcü politikacıların halka açık e-posta adreslerini kullanmıştır (Kozlowski, 2013).

Web sitesi tahrifatlarını gerçekleştirmek için Rus bilgisayar korsanları, arka uç veritabanıyla (normalde ortak bir SQL veritabanı-dolayısıyla adı) doğrudan iletişim kurmak için bir web sayfasındaki bir metin alanını kullanan SQL enjeksiyonu olarak bilinen başka bir saldırı türüne başvurdu. Operasyonun bu aşamasında, siber faaliyetlerin çoğu, genellikle "hacktivistler" olarak anılan "vatansever" Rus bilgisayar kullanıcılarının işe alınmasına kaydı. Bazı Rus hacker sitelerindeki ilanlara göre, birçok "haktivist"in Rus gençlik hareketlerinin üyesi olduğu düşünülmüştür. İşe alım öncelikle çeşitli web siteleri aracılığıyla yapıldı, bunlardan en ünlüsü 9 Ağustos 2008'de çevrimiçi olan "StopGeorgia.ru" idi. Bir bilgisayar korsanı, sağlanan talimatların acemi bir kullanıcı için bile çok erişilebilir olduğunu belirtmiştir. Örneğin, StopGeorgia.ru, özel makinelerden DDoS başlatmak için kullanımı kolay araçlar ve talimatlar sağladı. Hatta tıklandığında Gürcistan hedeflerine birden çok DDoS dağıtan "FLOOD" adlı kullanıcı dostu bir düğme bile içeriyordu (Shakarian, 2011).

Bilgisayar korsanlığı saldırılarının çoğu, botnet eylemlerinden farklı bir güvenlik açığına dayansa da yine de kaba kuvvetle Georgia sunucularına aşırı yüklenmeyi hedefliyorlardı. Sağlanan araçlar da çok yönlüydü. Örneğin, bazı aynı anda 17 Gürcü sunucusuna saldırabilmektedir. Bu bilgisayar korsanlığı web siteleri ayrıca, Rusya'dan mı yoksa Litvanya'dan mı erişilebildiğine dair spesifikasyonlar ve bilinen güvenlik açıkları dahil olmak üzere Gürcü sistemlerinin hedef listelerini de içeriyordu. Bunlar, SQL enjeksiyonuna duyarlılığı içeriyordu. Bazı güvenlik uzmanlarının StopGeorgia.ru'yu Rus organize suçuyla ilişkilendirmesi de dikkat çekicidir (Thomas, 2009, s. 38).

Ağustos 2008'de Gürcistan'a yönelik Rus siber harekâtı, büyük konvansiyonel askeri operasyonlarla eş zamanlı olarak gerçekleşen ilk büyük ölçekli CNA'yı temsil etmektedir. Bu CNA operasyonları, yalnızca medya ve hükümetin değil, aynı zamanda halkın dış dünya ile iletişim kurma kabiliyetini

de azalttığı için Gürcistan üzerinde önemli bir bilgi ve psikolojik etkiye sahipti (Shakarian, 2011).

5.4.3. Litvanya'ya yönelik siber saldırılar

2008 Haziran ayında Litvanya, üç günlük süre ile Rusya'nın yol açtığı ileri sürülen siber saldırılara uğramıştır. Bahsedilen siber saldırılar, Gürcistan ve Estonya örneklerinde olduğu şeklinde Litvanya'nın kritik altyapılarının "DDoS" saldırılarıyla çökertilmesi ve ülkede faaliyette bulunan popüler web sayfalarının "orak-çekiç" amblemleri ile hacklenmesi biçiminde olmuştur (Darıcılı, 2014).

Rusya ile Litvanya arasında yaşanan politik gerginliğin bu saldırıların arka planında da olduğu belirtilmektedir. Zira saldırılar Rusya'nın Sovyet döneminde çalışma kamplarında ölen Litvanyalı kurbanların yakınlarına tazminat ödemeyi reddetmesi, ilerleyen süreçte Rusya'nın Litvanya'ya enerji akışını kısıtlaması, buna cevap niteliğinde de Litvanya hükümetinin eski Sovyet sembollerini yasaklayan bir kanunu meclise sunması ve Rusya-AB ortaklık sürecini bloke etmesinin ardından başlamıştır (Darıcılı, 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 sürülmektedir. Keza 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).

5.4.4. Kırgızistan'a yönelik siber saldırılar

Siber saldırı, Ocak 2009'da Manas'taki Amerikan hava kuvvetleri üssünün geleceği hakkında ülke çapında hararetli tartışmaların yaşandığı sırada gerçekleşti. Üssün kapatılmasına karşı en güçlü protestolar muhalefetten geldi. Manas üssü, ABD'nin Afganistan'a saldırmaya hazırlandığı 11/09'dan sonra kuruldu. Kırgızistan, bu çabalarında George Walker Bush yönetimini destekledi

ve kendi topraklarında Amerikan Üssü kurulması konusunda anlaşmıştır (Kozlowski, 2013).

2005 yılında Kırgız Devlet Başkanı Kurmanbek Bakiyev, Dışişleri Bakanı Condoleezza Rice ile yaptığı görüşmede, Afganistan'daki durum istikrara kavuşana kadar Amerikan ve NATO kuvvetlerinin üssü kullanabileceğini kabul etti. 2009'un başında üssün kira süresinin uzatılması veya kapatılması tartışıldı. Bu ikinci seçenek, Kırgızistan hükümetini olumlu karar almaya ikna etmek için 300 milyon ABD doları kredi ve enerji sektöründe 1,7 milyon dolarlık yatırım öneren Rus hükümeti tarafından desteklendi. Şubat 2009'da Bakiyev, Amerikalılardan üssü terk etmelerini isteyeceğini duyurdu. Ancak Kırgızistan makamları ile ABD arasındaki uzun müzakerelerin ardından Haziran 2009'da anlaşma sağlandı. Yeni anlaşmaya göre kiralama bedeli 16 milyon dolardan 60 milyon dolara yükseldi ve ayrıca ABD ek yatırım sözü vermiştir (Bradbury, 2009).

18 Ocak 2009'da başlayan saldırılar 2 hafta sürdü. Saldırganlar, Kırgızistan'daki iki ana IPS (www.domain.kg, www.ns.kg) dâhil olmak üzere 4 internet sağlayıcı hizmetinden (IPS) 3'ü başarıyla bozdu. Devasa DDoS saldırıları kullandılar. Kırgızistan'da sadece 4 IPS olduğu için internet servislerinin çoğu çöktü. E-posta göndermek veya belirli web sitelerine girmek imkânsızdı ve ayrıca siber saldırı nedeniyle cep telefonlarının kullanılması engellendi. İnternet trafiğinin neredeyse %80'i çevrimdışı bırakılmıştır. Bununla birlikte, Kırgızistan'ın ortalama vatandaşları basit bir nedenden dolayı siber saldırıdan zarar görmedi. Sadece az sayıda Kırgız internet erişimine sahipti (Kozlowski, 2013).

Bununla birlikte, önde gelen başkana muhalefetin internette birbirine bağlı olduğunu vurgulamak önemlidir. IP trafiği, DDoS trafiğinin çoğunun üretildiği Rus sunucularına kadar izlendi. Bu sunucular, siber suçluların faaliyetleri ve Estonya ve Gürcistan'a saldırmak için yaygın olarak kullanılıyordu. IP adresi ve ağlar, 2007 ve 2008'deki önceki saldırılardan sorumlu gruplarla ilişkilendirildi. Ayrıca onları yöneten iki grup da 2008'dekilere benziyordu. Bu saldırıların arkasında RBN'nin olma olasılığı yüksekti. Muhtemel senaryo, Rus yetkililerin

devasa siber saldırıları gerçekleştirmek için RBN'den bilgisayar korsanları tuttuğu şeklindeydi (Ashmore, 2011).

5.4.5. Ukrayna'ya yönelik siber saldırılar

2013'ün sonunda Ukrayna Devlet Başkanı, Avrupa Birliği ile taraflar arasındaki bağları önemli ölçüde güçlendirecek ve kitlesel halk gösterilerini tetikleyecek bir Ortaklık Anlaşmasını terk etmişti. Birkaç ay sonra, gözden düşmüş Başkan Yanukoviç Rusya'ya kaçtı ve Rusya, Kırım Yarımadası'nı işgal etti. Euromaidan protestoları ve bunun sonucunda ortaya çıkan çatışma boyunca hem Ukrayna hem de Rusya'daki kurumlar ve medya kuruluşları hedef odaklı kimlik avı e-postaları tarafından gönderilen DDoS saldırılarına, web sitesi tahrifatlarına ve Uzaktan Yönetim Araçları'na (RAT) maruz kalmıştır (Baezner, 2018).

13 Mart 2014'te, Kırım'ın statüsüne ilişkin referandumdan üç gün önce, Rusya, halkın dikkatini Kırım'daki Rus birliklerinin varlığından başka yöne çekmenin bir yolu olarak, Ukrayna bilgisayar ağlarını ve iletişimini istikrarsızlaştırmayı amaçlayan sekiz dakikalık bir DDoS siber saldırısı başlatmıştır. Mayıs 2014'te, Ukrayna cumhurbaşkanlığı seçimlerinden önce, Rus yanlısı bir bilgisayar korsanlığı grubu, oylamayı manipüle etmek için bir dizi siber saldırı gerçekleştirmiştir (Baezner, 2018).

CyberBerkut bilgisayar korsanları, Merkezi Seçim Komisyonu'nu hedef alarak seçim sonuçlarını değiştirmek amacıyla ağı işgal etti ve dosyaları sildi. Kötü amaçlı yazılım seçimden 40 dakika önce kaldırıldığı için saldırı başarısız oldu. Ancak bilgisayar korsanları seçim sayımını geciktirmeyi başarmıştır. Sonraki birkaç yıl içinde, Ukraynalı yetkililer elektrik şebekelerine yönelik iki siber saldırıyı Rusya'ya bağlamışlardır. 23 Aralık 2015'te başka bir DDoS saldırısı, çağrı merkezlerini ve üç enerji dağıtım şirketinin ağını etkilemiştir. Sonuç olarak, batı Ukrayna'daki 230.000'den fazla tüketici, bir ila altı saat arasında değişen elektrik kesintilerine maruz kalmıştır. Ayrıca, Rusya devlet destekli olduğu iddia edilen Kum Solucanı Timi, 16 trafo merkezinin sistemlerini engellemeyi başarmıştır. Benzer bir siber saldırı da 2016 yılında meydana gelmiştir. Kiev'deki bir trafo merkezindeki kesintiler, bir saatlik elektrik kesintisine neden olmuş; ancak bu girişim, ilgili ekipmanı tamamen

devre dışı bırakma girişiminde başarısız olmuştur (europarl, 2022). Bu siber saldırılar, düşmanı bozmak, gözetlemek veya ona zarar vermek için kullanılmıştır. Bu saldırıları gerçekleştirmek için devlet dışı aktörleri vekil güçler olarak kullanarak, savaşan taraflara siber uzaydaki eylemleri için makul inkâr edilebilirlik de sağlanmıştır. Ukrayna ihtilafı bağlamında yürütülen siber faaliyetlerin Ukrayna'yı yalnızca yerel düzeyde etkilemediğini, aynı zamanda uluslararası düzeyde de yansımaları olduğunu ortaya koymuştur. Ukrayna'daki siber çatışmanın sosyal ve politik etkileri, Kırım haber ve bilgi kaynaklarının hâkimiyetini içeriyordu. Rusya tarafından, Ukrayna hükümetinin Ukraynalılar nezdindeki güvenilirliğinin erozyona uğraması ve bunun sonucunda Ukrayna halkının hükümete olan güveninin kaybolmasına yol açmıştı. Ekonomik etkiler, çeşitli DDoS saldırılarının ve web sitesi tahrifatlarının neden olduğu gelir kaybı ve itibar kaybının maliyetlerini ve Ukrayna elektrik şebekesine yapılan siber saldırıların ardından ekipmanı değiştirme ihtiyacından kaynaklanan masrafları içeriyordu (Lewis, 2022).

Rusya'nın 2014 yılında egemen Ukrayna toprağı olan Kırım'ı ilhakı sonrasında, gerek Ukrayna'nın iç siyasi meselelerinin cevaz vermemesi, gerekse uluslararası toplumun bu işgale karşı gereken tepkiyi gösterememesi, Rusya'yı milli hedef, amaç ve menfaatleri bağlamında hedef coğrafya olarak gördüğü Ukrayna'ya karşı, özellikle siber evren kapsamında daha da saldırgan hale getirmiştir. Nitekim 2016 ile 2021 arasında Ukrayna'ya yönelik Rusya kaynaklı siber saldırılar artarak yoğunlaşmıştır. Bunlardan en dikkate değer olanı, tarihin en yıkıcı siber saldırısı olarak kabul edilen NotPetyamalware'in Haziran 2017'de muhasebe yazılımı aracılığıyla başlatılmasıdır. NotPetya, Chornobyl nükleer santralini ve kamu kurumları, bankalar, posta hizmetleri, gazeteler, ulaşım altyapısı ve işletmeler tarafından kullanılan 13.000'e yakın cihazı vurmuştur. Bilgisayar sürücüleri yok edilmiş ve virüs şifrelemesinden sonra veri geri yükleme devre dışı bırakılmıştır (europarl, 2022).

Kötü amaçlı yazılımın küresel bir etkisi oldu, 65 ülkeyi ve yaklaşık Avrupa ve ABD şirketleri FedEx, Maersk ve Merck dâhil olmak üzere 50.000 sistem ve 10 milyar ABD dolarının üzerinde zarara neden oldu. 2018 ve 2021'de iki büyük siber saldırı girişimi gerçekleşti. İlki, Ukrayna'nın 23

eyaletinde faaliyet gösteren Auly klor damıtma istasyonunu hedeflerken, ikincisi Ukrayna güvenlik servisi web sitelerini hedef aldı. Devlet yürütme organları tarafından kullanılan elektronik etkileşim sistemine yönelik bir saldırı başarısız oldu; ancak, sisteme zarar vermeyi başardı (Lewis, 2022).

2022'nin başında siber saldırılar daha da artmıştır. Örneğin, 13 Ocak 2022'de Microsoft, Ukrayna hükümetini ve birkaç kâr amacı gütmeyen kuruluşu ve BT kuruluşunu hedef alan kötü amaçlı yazılım tespit edildiğini bildirmiştir. Ertesi gün, aralarında Bakanlar Kurulu ve Savunma, Dışişleri, Eğitim ve Bilim Bakanlıklarının da bulunduğu 70 hükümet web sitesi geçici olarak bilgisayar korsanları tarafından kontrol edilmiştir. Ukrayna Dijital Dönüşüm Bakanlığı Rusya'yı sorumlu tuttu. Şubat ortasında, bir DDoS saldırısı birkaç devlet dairesinin, bankanın ve radyo istasyonunun web sitelerini birkaç saatliğine devre dışı bıraktı. Birçok ülke Rusya'yı saldırıyı başlatmakla suçladı. Ukraynalılar arasında panik ve kafa karışıklığına yol açtı. Bakanlar Kurulu ve birkaç bakanlık da dâhil olmak üzere aynı web siteleri 23 Şubat'ta yeniden hedef alındı. Ek olarak, HermeticWiper veri silme kötü amaçlı yazılımı finans, BT ve havacılık sektörlerinden 100 kuruluşa karşı başlatıldı (Lewis, 2022).

Siber saldırılar mart ayında devam etti ve kötü amaçlı yazılımlar hükümet ve finans web sitelerinin yanı sıra hükümet dışı, yardım ve yardım kuruluşlarına karşı başlatıldı ve bu durumda ilaç, gıda ve yardım malzemelerinin dağıtımını engellemiştir. Diğer vakalar arasında vatandaşlara ve devlet hizmetlerine yönelik kimlik avı saldırıları ve telekomünikasyona yönelik saldırılar yer almıştır. 14 Mart'ta CaddyWiper kötü amaçlı yazılımı, bildirildiğine göre hem devlet hem de finans sektörlerindeki birkaç Ukraynalı kuruluşun sistemlerine sızmıştır. İki gün sonra, bir Ukrayna televizyon kanalında, Ukrayna Devlet Başkanı Volodymyr Zelenskyy'nin halkı teslim olmaya çağırdığını iddia eden yanlış bir mesaj yayınlanmıştır (europarl, 2022).

Mart ayının sonundan itibaren Ukrayna'ya yönelik siber saldırılar, hükümeti, orduyu ve çeşitli kuruluşları hedef alan kimlik avı e-postalarının yanı sıra gözetim yazılımı yüklemek için bir LoadEdge arka kapısının kullanılmasını içeriyor. Ukrtelecom ve WordPress sitelerini hedef alan siber saldırılar, bir bağlantının çökmesine ve finans ve devlet web sitelerine erişimin kısıtlanmasına

neden oldu. 30 Mart'ta MarsStealer bilgi hırsızı, Ukrayna vatandaşlarının ve kuruluşlarının kullanıcı kimlik bilgilerine erişti (Lewis, 2022).

Benzer şekilde, Nisan ayında bilgisayar korsanları, Ukrayna hükümetinden ve medya kuruluşlarından hassas bilgileri ve kullanıcı kimlik bilgilerini ele geçirdi. Ayrıca kötü amaçlı bir Truva atı ve sahte bir sosyal medya sayfası anketi yardımıyla vatandaşların bankacılık ve ödeme verilerine el koydular. Diğer siber saldırılar toplumsal zarar vermeye çalıştı. Bu tür bir örnek, elektrik santrallerinin faaliyetini engelleme ve milyonlarca insana elektrik akışını engelleme girişimini içeriyordu. En son saldırı, savaşla ilgili bir dizi pulu piyasaya sürerken Ukrayna posta servisinin çalışmalarını durdurmayı başardı (europarl, 2022).

Bu bölümün sonunda şu değerlendirme ve yorumlarda bulunmak mümkündür. Özellikle 2001 yılındaki 11 Eylül terörist saldırıları sonrasında asimetrik tehditlerin gerek devletleri gerekse uluslararası toplumu ne denli tehdit edebileceği iyice görülmüştür. Hatta bahse konu saldırılar neticesinde NATO tarihinde ilk defa kolektif İttifak savunmasının devreye alınmasını hükmeden 5. Madde işletilmiş ve tüm üye devletlerce uluslararası terör risk ve tehditleri sebebiyle aktif edilmesine karar verilmiştir. 1990'lı yıllarda liberal-demokratik Batı dünyası ile neoliberal ideolojinin ekonomik bacağı bağlamında, aynen Çin Halk Cumhuriyeti gibi, ikitisadi bütünleşme ve entegrasyonunu sağlama çabaları gösteren Rusya Federasyonu, 2000'li yıllarda bunda hayli başarılı olarak tekrar ekonomik-politik ve askeri-politik bağlamda toparlanmış, eski SSCB dönemindeki siyasi, ekonomik ve askeri gücüne kavuşmuştur. NATO ile hayli ortaklık içine girmiş ve NATO ile Rusya arasında çeşitli iş birliği ve koordinasyon amaçlı etkin ve doğrudan ikili mekanizmalar NATO çatısı altında oluşturulmuş olsa da Rusya hem NATO'yu her zaman kendisine en büyük tehdit görmüş hem de Avrupa'da birinci kuşak sınırdaş coğrafyalarında (diğer deyişle, Ukrayna, Finlandiya ve İsveç'te) NATO'nun bulunmasına izin vermeme siyasasını bir ulusal güvenlik meselesi olarak benimsemiştir.

Bu bağlamda, zaten 1990'lı yıllardan itibaren yüzünü Batı'ya ve AB'ye dönen Ukrayna ile bozulan ilişkileri, Karadeniz'de Ukrayna üzerinden sahip olduğu ayrıcalık ve imkân-kabiliyetleri kaybetme gelişme ve olasılıkları,

Rusya'yı Ukrayna'ya karşı daha da saldırgan hale getirmiştir. Önce 2014 yılında Kırım bölgesini ilhak ederek, egemen ve bağımsız bir devlet olan Ukrayna'dan koparmış, müteakiben de 24 Şubat 2022 tarihinde egemen ve bağımsız bir devlet Ukrayna'nın topraklarına saldırılar düzenleyerek topyekün savaş açmıştır. Rus saldırganlığı, 2000'li yıllarda Baltık'da Estonya ve Litvanya'da, Kafkaslar'da Gürcistan'da, Orta Asya'da Kırgızistan'da Ukrayna'ya yaptığı gibi konvansiyonel saldırılar ile gerçekleşmemiş, bilakis Rusya'nın gelişmiş bilgisayar korsancılığı ve bunu adeta bir resmi devlet uygulamasına dönüştürmesi ile gerçekleştirdiği görülmüştür.

Nitekim Rusya, siber savaşla bu coğraflarda elde ettiği başarıyı iyi analiz etmiş ve özellikle Batı ile yaşadığı uluslararası ihtilaf ve uyuşmazlıklarda milli amaç ve hedeflerini gerçekleştirmek için siber evren gibi sanal bir ortamı, siber silahlar gibi de asimetrik vasıta ve mekanizmaları gayet uygun biçimde kullanabileceğini görmüştür. Zira siber savaş, harbin alanı, vasıta ve silahları ile sanal, zamansız, bilinmez, limitsiz ve kuralsız bir genel özelliğe sahiptir ve siber dünyada günümüz reel dünyasındaki evrensel savaş hukuku hükümleri geçerli değildir. Bu durumun da Rusya'yı Şubat 2022'den beri konvansiyonel silahlarla savaşıp bir türlü başarılı olamadığı Ukrayna coğrafyasında ulusal hedefleri yönünde daha etkin ve çabuk sonuçlar almak üzere siber evreni, bir siber savaş alanı ve asimetrik bir terör silahı gibi kullanmaya ittiği görülmektedir. Dolayısıyla, 2022'den bu yana Ukrayna'ya yönelik Rusya kaynaklı gerçekleştirilen siber saldırıları bu bağlamda değerlendirmek uygun olacak ve bu nevi siber risk ve tehdit içerikli saldırıların, Batı'nın Ukrayna'ya yüklü ve kıymetli konvansiyonel silah yardımı yaptıkça daha da artarak devam edeceğini söylemek pek de yanlış olmayacaktır.

6. SONUÇ VE DEĞERLENDİRME

Bilişim sistemleri ve internet, 1970'lerden itibaren insanlığın genel bir fenomeni haline gelmiş, bu alandaki teknolojik gelişmeler akıl almaz bir hızla ilerleyerek gelişmiş ve geliştirilmiş; özellikle her türlü otomasyon, sanal dünya, bilişim ve iletişim, internet, sosyal medya ve daha birçok ağ tabanlı ve ağ merkezli bilişsel aktivite ve evren, modern insan yaşamının ayrılmaz bir parçası haline gelmiştir. Günümüzde akıllı telefon, tablet ve taşınabilir bilgisayar gibi bilişim emtiyaları, insanın doğal bir ihtiyacı ve olmazsa olmazı haline gelmiş, hatta bunlara sahip olmayanlar sanki modern öncesi bir çağda yaşıyormuşçasına tepkiler görür hale gelmiştir. Zira sosyal medya ve ağ tabanlı bilişim uygulamaları, yeni medyadan eğitime, reklamcılıktan bankacılığa ve daha birçok toplumsal sektörün işlevsel temeli haline dönüşmüştür.

Siber evrende, "tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam" olarak, bu adeta zamansız, sınırsız ve kuralsız sanal faaliyetlerin içerisinde yaşadığı bir dünya olup, bilişim sistemlerinde hızlı ve inanılmaz gelişmelerin sonucunda kötü amaçlı faaliyet ve eylemlerin de evreni haline gelmeye başlamıştır (Sağıroğlu, 2018, s. 25). Nitekim gerek bireysel gerekse ulusal amaç, hedef ve çıkarlarını gerçekleştirmeye çalışan kimi çevreler sanal âlemi, diğer deyişle siber uzayı bir mücadele alanı, bir savaş alanı olarak kullanmaya teşebbüs etmişler ve bunda da büyük ölçüde başarılı olmuşlardır.

Bundan ötürü, özellikle Batılı demokrasiler gibi devletin meşru kanun, nizam, Anayasa ve hukuk ilkeleri çerçevesinde şeffaf ve demokratik yönetim ve hukuk devleti temelli ilişkiler ile işlediği ülkelerde, Rusya Federasyonu, İran, Çin Halk Cumhuriyeti, Kuzey Kore Halk Cumhuriyeti vb. gibi özelde Batılı demokratik toplumlar ve devletlerle, ve de genel anlamda liberal-demokratik uluslararası toplumla başarılı bir ilişki, koordinasyon ve işbirliği ortaklığı kuramayan kimi devletler, Batı ile aralarındaki türlü siyasi sorun, ihtilaf ve

uyuşmazlıkları kendi ulusal menfaatleri çerçevesinde çözebilmek için sanal âlemi ve buradaki eylemleri adeta asimetrik bir savaş aracı olarak kullanmaya başlamışlardır. Batılı liberal-demokratik dünyaya karşı bir siber savaş olarak nitelendirilebilecek bu zamansız, kuralsız ve limitsiz asimetrik mücadele, söz konusu devletlerce çeşitli terörist faaliyetlerin yanında ilave asimetrik savaş metot ve araçları olarak yararlanılmıştır. Ancak, bu siber eylem ve saldırıların çoğu zaman gizli kalabilmesi ve zamansız, kuralsız ve sınırsız, diğer deyişle asimetrik bir tehdit yaratması yanında, hedef tarafta yarattığı olumsuz etkinin de oldukça büyük ve yıkıcı olması sebepleriyle, uluslararası ilişkilerde uyumsuz ve başarısız söz konusu otokratik ve liberal-demokratik rejimli olmayan Rusya, Çin, İran, Kuzey Kore gibi devletlerce gerçekleştirilen siber saldırılar, uluslararası ilişkilerin araçsallaştırılması bağlamında –gerektiğinde- başvurulan bir asimetrik tehdit unsuru ve hatta savaş uygulaması haline gelmiştir.

Nitekim siber uzayın ortaya çıkışı, devletlerin hem kullanıcıları hem de güvenlik kurumları için birçok güvenlik sorununu beraberinde getirmiştir. Siber saldırganlar, finansal kurumları hedef alarak, ulusal sırlara erişerek ve sızdırarak ve İran nükleer tesislerine karşı Stuxnet solucanı da dâhil olmak üzere birçok örneğin gösterdiği gibi, ulusal altyapıya kinetik bir saldırıya benzer gerçek fiziksel hasara neden olarak hasara yol açma potansiyeline sahiptir. Saldırganlar nadiren iz bıraktıklarından ve aslında kökenlerini gizlemeye çalıştıkları için siber saldırıların atfedilmesi daha zordur. “Siber güvenlik” terimi, konuya büyük ölçüde belirli bir perspektiften bakan akademik ve popüler alanyazının konusu olmuştur.

Hemen herkes siber uzayın günlük hayatın bir gerçeği olduğunun farkındadır. İnternet, bağlandığı milyarlarca bilgisayar, yönetimi ve sağladığı deneyimler de dâhil olmak üzere siber uzay, her yerde bulunması, ölçeği ve kapsamı göz önüne alındığında, içinde yaşadığımız dünyanın merkezi bir özelliği haline geldi ve temel olarak yeni bir gerçeklik yaratmıştır.

Yeni dijital çağda uluslararası ilişkilerin bilim insanları da siber uzayı keşfetmeye başlamıştır. Geleneksel uluslararası ilişkiler teorisi, fiziksel mekânlardaki etkileşimlere dayanır ve bunlara atıfta bulunmaktadır. Uluslararası ilişkilerde her türlü alan, dünya siyasetinde güç ve etkiyi

genişletmek için fırsatlar sunmaktadır. Siber uzay, casusluktan savunmaya ve bilgisayar korsanlığına kadar her devlet için önemli bir dış politika aracı haline gelmiştir.

Rusya'nın savaşa bakışının ana hatlarını çizmek, Rusya'nın siber stratejisini kavramak için kritik öneme sahiptir; keza Rusya'nın siber güvenliğe bakış açısı, Rusya'nın savaşın doğasına ilişkin gelişen anlayışıyla iç içe geçmiş durumda ve bilgi savaşı kavramıyla şekillenmektedir. Siber güvenlik, Rus tartışmalarında Batılı bir kavram olarak algılanırken, anlamsal Rusça karşılığı bilgi güvenliğidir. Nitekim Rusya, dünya çapında dezenformasyon, propaganda, casusluk ve yıkıcı siber saldırılar yürütmek için gelişmiş siber yetenekler kullanmaktadır. Bu operasyonları yürütmek için Rusya, çeşitli güvenlik ve istihbarat teşkilatları tarafından denetlenen çok sayıda birime sahiptir. Rus Askerî İstihbarat Direktörlüğü, Rus İstihbarat Servisi, Rus Federal Güvenlik Servisi'nin gerek Rus kriminal örgütleri ile olan illegal bağlantıları gerekse de tek başlarına sahip oldukları siber kapasiteleri, RF'nin siber savunma ve saldırı kapasitesini belirleyen temel faktörlerdendir.

Geçtiğimiz 15-20 yıl boyunca, Rusya'nın savaş kavramsallaştırması, silahlı şiddetin yanı sıra askeri olmayan araçları da içerecek şekilde değişmiştir. Bu dönüşüm, Rus doktrininde bilgi savaşının artan önemi ile örneklendirilmektedir. Bu doktrine göre, bilgi savaşı siber ve bilgi operasyonlarından oluşur ve modern çatışmanın ayrılmaz bir parçasıdır. Resmi doktrin, bilgi savaşını tartışırken, Rusya'yı saldırgan hasımların karakterize ettiği bir ortamda savunma duruşuna asil bir şekilde bağlı kalan bir devlet olarak tasvir etmektedir.

Bununla birlikte, Rus askeri bilim insanlarının çalışmaları, etkililikleri, çağdaş çatışmalar çerçevesindeki uygunlukları ve karşılanabilirlikleri nedeniyle siber silah geliştirmeye yönelik artan bir ilgiyi göstermektedir. Saldırı siber araçlarına ilişkin bu analizler, Rusya'nın çağdaş çatışma düşüncesine paralel olarak gelişen gerçek Rus siber ve bilgi operasyonları uygulamasıyla daha doğru bir şekilde uyumlu görünmektedir. Nitekim Rusya Federasyonu'nun ulusal hedef ve menfaatlerini gerçekleştirmek üzere 2000'li yıllarda Estonya, Gürcistan, Litvanya ve Kırgızistan devletlerinde giriştiği siber saldırı eylem ve

faaliyetleri ve bu vakalardan çıkarılabilecek bazı operasyonel ve istihbarati ders ve tespitlerin şu şekilde olabileceği değerlendirilmektedir.

Birincisi, Rusya'nın kendi halklarının vatansever "hacker milislerini" bir ağ yürütmek üzere çalıştırdıkları, hedef bir bağımsız ve egemen devlete saldırmak için, önce onları motive edip, devreye soktukları görülmektedir. Rusya'nın temel konseptinin, vatansever "hacker milislerini" uygun hedeflere yönlendirerek, bu siber uzay operasyonlarını konvansiyonel savaşla senkronize ettiği müşahade edilmekte; böylece, fiziksel evrendeki eylem ve aktivitelere ilave olarak, en etkili siber uzay taktik, teknik ve prosedürleri kullanılmaktadır. Dolayısıyla, potansiyel saldırgan devletlerin bu nevi siber saldırı faaliyetlerini anlamak, fark etmek ve engellemek için, hedef ulusların saldırgan devletlerin hacker sohbet odalarını ve iletişimlerini izlemeleri gerekmektedir.

İkincisi, herhangi bir gerçek askeri operasyondan önce siber uzaydaki hedeflerin tanımlanması ve erişimlerin geliştirilmesi gerekir. Gerçek planlanan saldırılar ve faaliyetler, etkinliklerini değerlendirmek için düşük seviyede uygulanmalıdır. Gelecekteki siber savaşta, ulusların bu hazırlık operasyonlarını, keşif faaliyetlerini ve araştırma saldırılarını, geleneksel askeri operasyonları desteklemek için gerçekleştirilen herhangi bir ağ saldırısından çok önce gerçekleştirmeleri gerekecektir.[3]

Siber savaş ve bilgi savaşı söz konusu olduğunda Rusya en gelişmiş yeteneklerden birine sahiptir ve aynı anda stratejik avantaj ararlar ve beklenen sürprize sürprizle karşılık vermeye çalışırlar. Rus yetkililer, herhangi bir dış güç veya saldırıyla karşılaşmaları durumunda ve savaş dışındaki durumlarda kullanılmak üzere siber teknolojiler ve savaş kullanarak iyi bir saldırı sistemi oluşturmak için çalışmışlardır ve bu siber savaş yöntemlerini Estonya, Gürcistan ve Ukrayna örneklerinde birkaç kez test etmişlerdir. Bu bağlamda, RF'nin önümüzdeki yıllarda da siber savaş ve terör yöntem ve tekniklerine başvurarak gerek küresel güç mücadelelerinde gerekse günümüzde Ukrayna savaşında olduğu şekilde bölgesel gerginlik ve kriz ve çatışmalarda üçüncü taraflara karşı siber saldırı girişimlerinde bulunabileceği yüksek ihtimal olarak görülmektedir.

[3] Ayrıntı için bkz. (Hollis, 2018)

Günümüzde siber evrende uluslararası toplum ve hukukla uyumsuzluk ve başarısızlık gösteren Rusya Federasyonu ve benzeri devletlerin ulusal hedef, amaç, varlık ve çıkarlarını realize etmeye yönelik hedef ülke ağ tabanlı bilişim sistemlerine gerçekleştirdikleri siber terör temelli siber saldırı eylemleri nedeniyle, ilgili hedef ülkenin birçok ağ tabanlı bilişim işletim sisteminde yıkıcı ve büyük çaplı hasar ve zararlar meydana gelmektedir. Üstüne üstelik bu siber saldırılar gerçekleştiren devlet tarafından ulusal hedeflerini gerçekleştirme ve uluslararası ilişkilerde güç, üstünlük ve kazanç sağlamaya yönelik olunca, hedef ülkelere yönelik siber saldırı eylemlerinin uluslararası ilişkilerde bir asimetrik silah aracı haline getirildiğini söylemek mümkündür.

Nitekim Rusya'nın 2000'li yıllarda ulusal hedef ve amaçlarını realize etmeye destek sağlaması maksadıyla Estonya, Gürcistan, Litvanya ve Kırgızistan'a yönelik siber saldırı eylemlerini bu bağlamda değerlendirmek mümkündür. Milenyum çağının hızla gelişen bilişim teknolojileri dünyası destekli post-modern ve gerçek-ötesi çağında, artık bireysel ve kamusal düzeylerde devletlerin milli çıkarlarının olduğu kadar, uluslararası hukuka ve liberal-demokratik değerlere sahip ve saygılı uluslararası toplumun menfaatlerinin de siber terörizm içerikli saldırılardan korunması hayat önem arz etmektedir. Zira bu siber saldırı eylemlerini, adeta uluslararası toplumun gözlerinin içerisine sokarcasına, hiç çekinmeden ve defalarca gerçekleştiren Rusya Federasyonu ve benzeri devletler ile kimliği belirsiz devlet-dışı aktörlerin siber uzayda gerçekleştirdikleri her nevi siber saldırı eyleminden, bu eylemlerle ilgili çeşitli iz, şüphe ve/ya kanıtlar ortaya çıktığında bunları icra ettiklerini inkâr ederek, sonunda gerek ulusal hadefler, gerekse uluslararası ilişkiler çıkar ve kazançları bakımlarından hayli kazançlı çıktıkları görülmektedir.

Bu yüzden de siber savaş ile ilgili bir başka esaslı ve tehlikeli gelişme de söz konusu siber saldırgan devletlerin bu siber saldırı eylemleri sonrasında kazançlı çıktıkları ve uluslararası toplum tarafından suçlanmadan kurtuldukları oranda, bu eylemlerinin dozaj, sıklık ve genişliğini artırmaları istekleridir. Bunda ana motivasyon, siber saldırı eylemlerinin, mermi, bomba, füze, güdümlü mermi ve benzeri her türlü konvansiyonel mühümmata nazaran hedef ülkenin esas olarak siyasi, askeri, enerji, iktisadi, mali, finansal üstyapı, altyapı ve

bilişim sistemlerine çok büyük zararlar vermeleri, bunlar üzerinde hayli etkin ve yıkıcı sonuçlar doğurmalarıdır. Ayrıca, bu siber saldırı eylemlerinin kullanılmasındaki bir başka önemli motivasyonda, siber saldırı silahı olan bir bilgisayar virüsünün hedef ülke konvansiyonel sistemlerine, kamu ve özel kurum/kuruluşlarına ve kamu/özel bilişim ağı altyapısına her türlü konvansiyonel mühimmattan çok daha hızlı ve fazla zayiat verebilmesidir. Zira bu siber saldırı silahı olan sanal bir bilgisayar virüsü, zamansız, kuralsız ve sınırsız bir savaş enstrümanıdır. Bu yüzden, bir hedef ülkenin bankacılık-finans altyapısı, enerji santrallerinin veya hükümet kurumlarının ağ tabanlı bilişim işletim sistemleri bu bilgisayar virüsleri tarafından hedef alındığında, tümü anında çökmekte ve işlevsiz kalmakta; o sistemler üzerine binlerce ton konvansiyonel mühümmatın atılmasından daha büyük bir zarara uğramaktadırlar. Bu bağlamda, geleceğin savaşlarının siber uzayda gerçekleşecek siber savaşlar olacağını savlamak mümkündür.

Bundan ötürü, son sözde vurgulanabilecek bir husu da şudur; Rusya Federasyonu gibi ulusal hedef, amaç ve menfaatlerini siber uzayın içerisinde gerçekleştirdiği siber saldırı eylemleri ile meşrulaştırıp elde etmeye çalışan, bu bağlamda siber uzayı kullanarak siber saldırı eylemleri düzenleyip uluslararası ilişkilerde bu saldırıları araçsallaştıran, bu saldırıları siber savaş mücadelesi kapsamında birer asimetrik siber terör silahı olarak kullanan, kullandıkları da ciddi ve açık kanıtlarla gerçeklenen, uluslararası hukuk, liberal-demokratik toplumsal düzen ile sorunlu, uyumsuz ve başarısız devletlere karşı uluslararası toplum ve örgütlerce etkin hukuki yaptırımlar uygulanmadığı sürece, bu siber saldırı faaliyet ve eylemlerinin önümüzdeki yakın ve orta vade küresel/bölgesel güç mücadele, kriz, çatışma ve savaşlarında sayıları gittikçe artar şekilde ciddi birer asimetrik siber-savaş silahı ve siber-terör enstrümanı olarak kullanılacağını savlamak pek de yanlış olmayacaktır.

KAYNAKÇA

Abdoh, M., Musa, M. & Salman, N. (2009). Detecting Spam by Weighting Message Words. *Çankaya Üniversitesi Fen-Edebiyat Fakültesi Dergisi*, 11, 1-7.

Akarçay, P. & Ak, G. (2018). Rethinking Cyber Warfare: Timeless, Normless And Unconstrained. *Journal of Institute of Economic Development And Social Researches*, *4*(9), 195-214.

Akarslan, H. (2015). *Bilişim Suçları*. Seçkin Yayınları.

Aktaş, O. (2020). *Siber Güvenli -Hacking Atölyesi*. Gazi Kitabevi.

Alford, L. D. (2001). Cyber Warfare: A New Doctrine and Taxonomy. *Crosstalk: Journal of Defense Software Engineering*, *14*(4), 27-30.

Alioğlu, S. D. (2019). Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları. [Yayımlanmamış Yüksek Lisans Tezi]. İstanbul Bilgi Üniversitesi.

Amoroso, E. (2006). *Cyber Security*. Silicon Press.

Aschmann, M., Van Vuuren, J. J., & Leenen, L. (2015). Cyber armies: the unseen military in the grid. In J. Zaaiman & L. Leenan (Eds.). ICCWS 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security (pp. 20-29). UK: Academic Conferences Limited.

Ashmore, W. C. (2011). Impact of Alleged Russian Cyber Attacks. *Baltic Security & Defence Review*, 11, 9-19.

Ataman, N. (2003). The Impact of Non-State Actors on World Politics: A Challenge to Nation-States. *Alternatives: Turkish Journal of International Relations*, *2*(1), 42-52.

Aycock, J. (2011). *Spyware and Adware*. Springer US.

Aydın, E. (2021). Study of the Cyber Security Measures: Comparative Work of the United States and Turkey. [Yayımlanmamış Yüksek Lisans Tezi]. Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü

Baezner, M. (2018). *Hotspot Analysis: Ukrayna İhtilafında Siber ve Bilgi Savaşı*. Güvenlik Çalışmaları Merkezi. https://css.ethz.ch/content/dam/ethz/special- Interest/gess/cis/center-for-securities-Studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf

Balforth, T. (2018, Ocak 12). Putin Praises Skills of GRU Spy Agency Accused of UK Poison Attack. *Reuters*. https://www.reuters.com/article/us-britain-russia-putin/putin-praises-skills-of-gru-spyagency-accused-of-uk-poison-attack-idUSKCN1N71YV

Barkham, J. (2001). Information Warfare and International Law on the Use of Force. *New York University Journal of International Law and Policy*, 34, 57-114.

Bashir, M., Wee, C., Memon, N. & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, 65, 153-165.

Bayraktar, G. (2015). *Siber Savaş ve Ulusal Güvenlik Stratejisi*. Yeni Yüzyıl Yayınları.

Baezner, M. (2018). *Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict*, Version 2, Center for Security Studies (CSS) Pubs.

Ben-Israel, I. (2001). Security, Technology, and the Future Battlefield, Haggai Golan (Ed.). *The Texture of Security*, Maarachot, (ss. 269-327), Tel Aviv.

Ben-Israel, I. (2010). From the Sword's Blade to Computer Memory. *Odyssey*, 9, 4-13.

Benzer, D. R. (2014). *Güncel Tehdit: Siber Suçlar*. Seçkin Yayınları.

Berkowitz, B. D. (2003). *The New Face of War: How War Will Be Fought in the 21st Century*. Free Press.

Bıçakcı, S. (2019). Siber Güvenlik ve Savunma, *Güvenlik Yazıları Serisi*, 42, 1-8

Bıçakcı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler Dergisi, 9*(34), 204-226.

Bradbury, D. (2009, Mart 22). The Fog of Cyberwar. *The Guardian*. http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattackinternet-acess

Broadhurst, R. G., Grabosky, P., Alazab, M. & Chon, S. (2014). Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime. *International Journal of Cyber Criminology, 8*(1), 1-20.

Bülbül, İ. & Poyraz, E. (2017). *Etik Hackerlığa Giriş*. Hayygrup Yayıncılık.

Canongia, C. & Mandarino, R. (2014). Cybersecurity: The New Challenge of the Information Society. *Tools and Applications, 2*(1), 60-80.

Carr, J. (2010). *Inside Cyber Warfare*. O'Reilly Media.

Cavelty, M. D. (2014). Breaking the Cyber-security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics, 20*(3), 701-715.

Cavelty, M. D. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge.

Choucri, N. (2012). *Cyberpolitics in International Relations*. The MIT Press.

Cybersecurity and Infrastructure Security Agency (CISA). (2022). *Russia Cyber Threat Overview and Advisories.* https://www.cisa.gov/uscert/russia.

Cilluffo, F. J. & Clark, J. R. (2016). Building a Conceptual Framework for Cyber's Effect on National Security. *Journal of Information Warfare*, *15*(2), 1-16.

Clarke, R. A. & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. Harper Collins.

Cohen, F. E. (2007). Cyberspace and Space. *Colombia Law Review, 107*(1), 201-256.

Collier, J. (2018). Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision. *Politics and Governance*, 6, 13-21.

Connell, M. & Vogler, S. (2017). Russia's Approach to Cyber Warfare. CNA Analysis and Solutions, March.

Covington, S. R. (2016). *The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare. Defense and Intelligence Projects.* Belfer Center for Science and International Affairs Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/legacy/files/Culture%20of%20Strategic%20Thought%203.pdf.

Cranor, L., Egelman, S, Hong, J. & Zhang, Y. (2007). Phinding Phish: An Evaluation of AntiPhishing Toolbars. İçinde *Proceedings of the Network and Distributed System Security Symposium.*

Cyberwarfare by Russia (2022). İçinde *Wikipedia. https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia*

Çıtak, Ö. (2018). *Ethical Hacking*. Abaküs Yayınları.

Darıcılı, A. B. (2014). Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi. *International Journal of Social Inquiry (IJSI), 7*(2), 4-15.

Darıcılı, A. B. (2015). NATO'nun Siber Güvenlik Stratejisi'nin Analizi. İçinde *Uluslararası İlişkiler Konferansı Uluslararası Sistemde Yeni Düzen Arayışları Bildiri Kitabı* (ss. 407-417). Uludağ Üniversitesi

Darıcılı, A. B. (2019). Analysis of Manipulation of the Russian Federation in the 2016 Presidential Elections of the United States of America within the Scope of Intelligence Techniques. *Güvenlik Bilimleri Dergisi, 8*(1), 133-150.

Darıcılı, A. B. & Özdal, B. (2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi. *Bilig*, 83, 121-146.

Darıcılı, A. B. & Çelik, S. (2021). National Security 2.0: The Cyber Security of Critical Infrastructure. *PERCEPTIONS*, *26*(2), 259-276.

Davis, J. (2007). Hackers Take Down the Most Wired Country in Europe, *Wired Magazine, 2*(1), 12-19.

Davis, S. (2019). NATO in the Cyber Age: Strengthening Security & Defence, stabilising Deterrence. (NATO Parliamentary Assembly Meeting Final Report). *NATO.* https://www.nato-pa.int/download-file?filename=sites/default/files/2019-09/148%20STC%20Davis%20-%20NATO%20IN%20THE%20CYBER%20AGE%20-%20fall%20revision%20-%20clean%2011.9.19.pdf

De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A. & Mazzara, M. (2019). Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era. *Future Internet, 11*(127), 44-76.

Demircan, C. (2019). Implications of Cyber Weapons in Cyber Security: A Case Study of Stuxnet and Duqu. [YayımlanmamışYüksek Lisans Tezi]. Anadolu Üniversitesi Sosyal Bilimler Enstitüsü

Duić, I., Cvrtila, V. & Ivanjko, T. (2017). International Cyber Security Challenges. *MIPRO*, 2, 1525-1232.

Dunn Cavelty, M. & Kristensen, K. S. (2008). *Securing the Homeland: Critical Infrastructure, Risk, and Security*. Routledge.

European Commission (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* European Data Protection Supervisor. https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en

European Commission (2017). *State of the Union 2017-Cybersecurity: Commission Scales up EU's Response to Cyber-attacks* [Press Release]. European Commission. http://europa.eu/rapid/press-release_IP-17-3193_en.html.

European Comission (2020). *The EU's Cybersecurity Strategy for the Digital Decade*. High Representative of the Union For Foreign Affairs and Security Policy. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Europarl (2022). *Russia's War on Ukraine: Timeline of Cyber-attacks (Briefing 21-06-2022).* Think Tank European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Farhat, V., Mccarthy, B. & Raysman, R. (2017). Cyber Attacks: Prevention and Proactive Responses. Security Law: Overview (Resource ID: 3-511-5848). *Thomson Reuters.* https://www.hklaw.com/files/Uploads/Documents/Articles/2017CyberAttacksPreventionandProactiveResponses.pdf

Geers, K. (2011). *Strategic Cyber Security*. CCDCOE Publication.

Ghernaouti-Hélie, S. (2013). *Cyberpower: Crime, Conflict and Security in Cyberspace*. EPFL Press.

Giles, K. (2016). *Handbook of Russian Warfare*. NATO Defense College Research Division, NATO Defense College.

Guirguis, M., Bestavros, A., Matta, I., & Zhang, A. (2005). Reduction of quality (RoQ) attacks on Internet end-systems. İçinde *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies* (ss. 1362-1372) vol. 2. doi: 10.1109/INFCOM.2005.1498361.

Guliyeva, N. (2021, Eylül 10). Cyber Security Strategy of the Russian Federation. *Ankara Kriz ve Siyaset Araştırmaları Merkezi.* https://www.ankasam.org/cyber-security-strategy-of-the-russian-federation/?lang=en

Güntay, V. (2016). Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi (Micro-CAT). [Yayımlanmış Doktora Tezi]. Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü.

Habersetzer, N. (2020). *Interview with Andrei Soldatov on Digital Rights in Russia.* Human Rights Watch. https://www.hrw.org/news/2020/06/19/interview-andrei-soldatov-digital-rights-russia

Hakala, J. & Melnychuk, J. (2021). *Russia's Strategy in Cyberspace*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf

Halfond, W. & Orso, A. A. (2006). Analysis and Monitoring for Neutralizing SQL-Injection Attacks. *ASE, 4*(1), 174-183.

Halfond, W., Viegas, J. & Orso, A. (2006). *Classification of SQLInjection Attacks and Countermeasures.* SSSE https://faculty.cc.gatech.edu/~orso/papers/halfond.viegas.orso.ISSSE06.pdf

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review, 100*(4), 817–885. http://www.jstor.org/stable/23249823

Hearn, K. (2009). Circumnavigating the Great Firewall. İçinde A. Chong & F. Bin Yahya (Eds.), *Alterity between Online and Offline Politics Forth Coming*. International Convention of Asia Scholars 6 (ICAS6).

Heickerö, R. (2015). *Emerging Cyber Threats and Russian Views on Information.* [Press Release]. Swedish Defense Research Agency.

Henkoğlu, T. (2014). *Adli Bilişim*. Pusula Yayınları.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49-60.

HM Government (2010). *A Strong Britain in an Age of Uncertainty.* http://www.official-documents.gov.uk/

HM Government (2016). *National Cyber Security Strategy 2016-2021.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Hollis, D. (2018). Cyberwar Case Study: Georgia 2008. *Small Wars Journal, 6*, 1-10.

International Telecommunication Union (2009). *Overview of Cybersecurity. Recommendation* [Report No: ITU-T X.1205]. Geneva International Telecommunication Union. http://www.itu.int/rec/T-REC-X.1205-200804-I/en

Johnson S. E. & Libicki, M. C. (1995). *Dominant Battlespace Knowledge: The Winning Edge*. National Defense University Press.

Jordan, T. (2003). *Cyberpower*. Taylor & Francis Group Pubs.

Kara, M. (2013). Siber Saldırılar-Siber Savaşlar ve Etkileri. [Yayımlanmamış Yüksek Lisans Tezi]. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü.

Kari, M. J. (2019). Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – A Tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threats. [Yayımlanmamış Doktora Tezi]. University of Jyvaskyla Faculty of Information Technology.

Kasper, A. & Vernygora, V. (2021). The EU's Cybersecurity: A Strategic Narrative of a Cyber Power or a Confusing Policy for a Local Common Market?. *Deusto Journal of European Studies*, (65), 29-71.

Kaspersky Lab. (2015). *Kaspersky Security Bulletin 2015 Final Report.* [Report No: 34]. Kaspersky. https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin2015_FINAL_EN.pdf

Kaspersky, Lab. (2020). *What is Cyber Security?* https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kantchev, G. & Strobel, W. P. (2021, Ocak 2). *How Russia'a 'Info Warrior' Hackers Let Kremlin Play Geopolitics on the Cheap.* Wall Street Journal. https://www.wsj.com/articles/how-russias-info-warrior-hackers-let-kremlin-play-geopolitics-on-the-cheap-11609592401

Kelly, S. (2014). *Freedom on the Net 2014: Russia. Freedom House Report* [Report No: 12]. Russia Freedom House. https:// freedom house.org/sites/default/files/resources/Russia.pdf

Klimburg, A. (2011). Mobilising Cyber Power. *Survival, 53*(1), 41-60.

Klimburg, A. & Healey, J. (2012). Strategic Goals & Stakeholders. A. Klimburg (Ed.). *National Cyber Security: Framework Manual* içinde (ss. 66-107). NATO CCDCOE Publication.

Kneale, J. (1999). The Virtual Realities of Technology and Fiction: Reading WilliamGibson's Cyberspace. M. Crang (Ed.). *Virtual Geographies: Bodies, Spaceand Relations* içinde (ss. 205-221). Routledge.

Koret, J. & Bachaalany, E. (2015). *The Antivirus Hacker's Handbook.* John Wiley & Sons Inc.

Korkmazer, S. (2013). Siber Güvenlikte USOM'un Rolü. İçinde *Siber Güvenlik ve Siber Terörizm Çalıştayı Bildiri Kitabı.* UTSAM Polis Akademisi Başkanlığı.

Kovac, L. (2018). Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review, 23*(89), 15-28.

Kozlowski, A. (2013). Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan. İçinde *1st International Scientific Forum Bildiriler Book* (ss. 236-245). European Scientific Institute.

Kshetri, N. (2014). Cybersecurity and International Relations: The U.S. Engagement with China and Russia. http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf

Kuzmanovic, A. & Knightly, E. W. (2003). Low-rate TCP-targeted Denial of Service Attacks. İçinde *Proceedings of ACM SIGCOMM* (ss.75-86). ACM Press.

Lewis, A. J. (2022). *Cyber War and Ukraine.* https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79InugnYWlcZL4r3Ljuq.ash

Libicki, M. (1995). What is Information Warfare? *Strategic Forum* 28. Washington D.C. National Defense University.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. Rand Corporation.

Lilly, B., & Cheravitch, J. (2020). The Past, Present, and Future of Russia's Cyber Strategy and Forces. İçinde *12th International Conference on Cyber Conflict (CYCON) Bildiriler Kitabı* (ss.129-155). doi: 10.23919/CyCon49761.2020.9131723.

Limonier, K. (2014). Russia in Cyberspace: Issues and Representations. *Hérodote, 152-153*(1-2), 33-50.

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy*, *7*, 63-86.

Lonsdale, D. J. (2016). Britain's Emerging Cyber-strategy. *The RUSI Journal, 161*(4), 52-62.

Medeiros, B. P. & Goldoni, R. F. G. (2020). The Fundamental Conceptual Trinity of Cyberspace. *Contexto International, 42*(1), 31-52.

Merriam-Webster (2020). *Cyberattack.* https://www.merriam-webster.com/dictionary/cyberattack

Ministry of Defence Brazil (2016). *Defense White Paper.* https://www.defesa.gov.br/arquivos/2017/mes03/livro-branco-de-defesa-nacional-consulta-publica-12122017.pdf

Nakashima, E. (2013, Şubat 10). US said to be the target of massive cyber-espionage campaign. *The Washington Post.* https://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html

Namanya, A. P., Awan, U. & Disso, J. P. (2018). The World of Malware: An Overview. İçinde *IEEE 6th International Conference on Future Internet of Things and Cloud Bildiriler Kitabı.*

Nath, S. (2012). What Military Deterrence Can not Do, Cyber Deterrence Can Do to Iran: Exploring The Implications of Manipulative Incessant Usage of The Term 'Pre- Emptive'. *International Journal of Social Sciences and Humanity Studies, 4*(1), 313-323.

Nazario, J. (2008). *Georgia DDoS Attacks-A Quick Summary of Observations.* Security Engineering and Response Team. http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-ofobservations

Nyang, D., Mohaisen, A. & J. Kang, (2015). Keyloggingresistant Visual Authentication Protocols. *IEEE Transactions on Mobile Computing*, *13*(11), 2566-2579.

Nye, J. S. (2010). *Cyber Power*. Harvard Kennedy School Pub.

O'Hanlon, M. E. (2000). *Technological Change and the Future of Warfare*. Brookings Institution Press.

Quadri, L. A. & Rasgaq, M. O. (2020). Cyber Theatre a Fifth Domain of International Politics: Africa and the rest of the world in the Cyberspace. *AHBV Akdeniz Havzası ve Afrika Medeniyetleri Dergisi, 2*(2), 98-111.

Rattray, G. J. (2009). An Environmental Approach to Understanding Cyberpower. F. D. Kramer & S. H. Starr (Eds.). *Cyberpower and National Security* içinde (ss. 253-274). National Defense University Press.

Ristolainen, M. & Kukkola, J. (2019). Closed, Safe and Secure-The Russian Sense of Information Security. V. Benson & J. McAlaney (Eds.). *Emerging Cyber Threats and Cognitive Vulnerabilities* içinde (ss. 53-71). Academic Press.

Roskin, M. G. & Berry, N. O. (2014). *Uluslararası İlişkiler: Uİ'nin Yeni Dünyası*. Çev.: Özlem Şimşek. Adres Yayınları.

Rubenstein, R. (2014). Nation State Cyber Espionage and its Impacts. https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage.pdf

Russakovsky, O., Deng, J., Su, H., Krause, J. & Satheesh, K. (2015). ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision 115*(3), 211-252.

Russinovich, M. E. (2014). *Rogue Code: A Novel*. Thomas Dunne /St. Martin's.

Sağıroğlu, Ş. (2018). Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler. Ş. Sağıroğlu & M. Alkan (Eds.) *Siber Güvenlik ve Savunma-Farkındalık ve Caydırıcılık* içinde (ss. 21-45). Grafiker Yayınları.

Saha, A., Subramanya, A. & Pirsiavash, H. (2020). Hidden Trigger Backdoor Attacks. Association for the Advancement of Artificial Intelligence Research Food [Düşünce Yazısı]. University of Maryland. https://arxiv.org/pdf/1910.00033.pdf.

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* The International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.

Shackelford, S. J. (2010). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, İçinde *Conference on Cyber Conflict Bildiriler Kitabı.*

Shakarian, C. P. (2011). The 2008 Russian Cyber-Campaign Against Georgia. *Military Review*, *11*, 61-68.

Sharma, A. (2010). Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis*, *34*(1), 62-73.

Sheldon, J. B. (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*, *5*(2), 95-112.

Sigholm, J. (2013). Non State Actors in Cyberspace Operations. *Journal of Military Studies, 4*(1), 1-37.

Sikorski, M. & Honig, A. (2012). Practical Malware Analysis. *Network Security,* 12, 1-20.

Singer, P. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Skoudis, E. & Zeltser, L. (2004). *Malware: Fighting Malicious Code*. Prentice Hall Professional.

SORM. (2022). İçinde *Wikipedia.* https://en.wikipedia.org/wiki/SORM

Stadnik, I. (2017). What is an International Cybersecurity Regime and How We Can Achieve It?. *Masaryk University Journal of Law and Technology, 11*(1), 135-148.

Stevens, T. (2021). United Kingdom: Pragmatism and Adaptability in the Cyber Realm. N. Romaniuk & M. Manjikian (Eds.). *Routledge Companion to Global Cyber-Security Strategy* içinde (ss. 191-200). Routledge.

Stevens, T., O'Brien, K., Overill, R., Wilkinson, B., Pildegovičs, T. & Hill, S. (2019). *UK Active Cyber Defence: A Public Good for the Private Sector* [Research Analysis Report]. The Policy Institute King's College London for the Public Security. https://www.kcl.ac.uk/policy-institute/research-analysis/active-cyber-defence

Syiemlieh, P., Khongsi, G. M. & Sharma, U. M. (2015). Phishing: An Analysis on the Types, Causes, Preventive Measuresand Case Studies in the Current Situation. *IOSR Journal of Computer Engineering*, 15, 1-8.

Şahinaslan, Ö. (2013). Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma. [Yayımlanmamış Doktora Tezi]. Trakya Üniversitesi Sosyal Bilimler Enstitüsü

Tabansky, L. (2011). Basic Concepts in Cyber Warfare. *Military and Strategic Affairs, 3*(1), 75-92.

The White House (2021, Nisan 15). *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government*. The White House Briefing Room. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

Thomas, F. (2015). *Adware: The Only Book You'll Ever Need*. Lulu Press, Inc.

Thomas, T. (2019). *Russian Military Thought: Concepts and Elements*. The MITRE Corporation.

Thomas, T. L. (2009). The Bear Went Through the Mountain: Russia Appraises its Five Day War in South Ossetia. *Journal of Slavic Military Studies, 22*, 31-67.

Trump, D. J. (2018). *National Cyber Strategy of the United States of America*. The White House Pub.

Turovsky, D. (2018). *Invasion: A Brief History of Russian Hackers*. Inviduum.

Umarani, C. & Sengupta, R. (2020). Keyloggers: A Malicious Attack. *International Journal of Trend in Scientific Research and Development, 5*(1), 34-39.

U.S. Defence Intelligence Agency (2017). Military Power Publications. https://www.dia.mil/Military-Power-Publications/

U.S. Office of the Director of National Intelligence (2021). Annual Threat Assessment, https://www.dni.gov/files/ODNI/documents/ assessments/ATA-2021-Unclassified-Report.pdf

Ülgen, S. (der.) (2015). *Türkiye'de Nükleer Enerji ve Emniyeti*. EDAM.

Vida, M. A. (2005). Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?. *51 NAVAL L.REV,* 132, 140-148.

Vlajic, N., Chowdhury, M. & Litoiu, M. (2019). IP Spoofing In and Out of the Public Cloud From Policy to Practice, *Computers, 8*(81), 1-17.

Watney, M. (2015). Challenges Pertaining to Cyber War Under International Law. *Third International Conference on Cyber Security, Cyber Warfare, and Digital Forensics Bildiriler Kitabı*. IEEE Explore 2014, (ss. 1-5). Lebanese University. https://ieeexplore.ieee.org/xpl/conhome/6908325/proceeding.

William, C. A. (2014). *Impact of Alleged Russian CyberAttacks*. [Research Paper]. School of Advanced Military Studies United States Army Command and General Staff College. https://apps.dtic.mil/sti/citations/ADA504991.

Wilson, C. (2007). *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*. [CRS Congress Report No: Code RL31787]. Congressional Research Service. https://sgp.fas.org/crs/natsec/RL31787.pdf

Yeniakit (2023, Ocak 27). *Leopard Tanklarının İntikamı mı? Rus Hackerlardan Almanya'ya Siber Saldırı.* https://www.yeniakit.com.tr/haber/leopard-tanklarinin-intikami-mi-rus-hackerlardan-almanyaya-siber-saldiri-1727968.html

Yılmaz, O. (2017). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik. *Siber Politikalar Dergisi*, *2*(4), 22-43.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Canfidan KABAKCI

EĞİTİM BİLGİLERİ

İlk Öğretim : Ankara Keçiören İsmail Enderuni İlkokulu

Rize Fındıklı Ahmet Şahinler İlkokulu

Çankırı Merkez Ortaokulu

Çankırı Lisesi (Kredili Sistem – Fen Bilimleri)

Balıkesir Polis Okulu : 1997-1998

Lisans Öğrenimi : Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi

Kamu Yönetimi

İŞ DENEYİMİ

Çalıştığı Kurumlar : 1998 - 2022 Emniyet Genel Müdürlüğü (Emekli Polis)

2022 – TİM/İTKİB Başkanlık Özel Kalemi (halen devam ediyor)