SİBER GÜVENLİK POLİTİKASI: ABD, RUSYA VE ÇİN ÜZERİNE KARŞILAŞTIRMALI BİR ANALİZ[*]

Volkan GÖÇOĞLU[**], Mehmet Devrim AYDIN[***]

Öz

Ülke sınırlarının ulusal güvenlik politikası açısından taşıdığı önem, son yıllarda giderek hızlanan küreselleşme süreci ile birlikte azalmaya başlamıştır. Küreselleşme ile birlikte dünyada, ülkelerin güç dağılım kanalları yeniden şekillenmiş, asimetrik güç ilişkileri ortaya çıkmış ve ulusal güvenlik ihtiyaçları yeniden tanımlanmıştır. Son yıllarda yaşanan teknolojik gelişmeler siber güvenlik kavramını ortaya çıkarmış ve siber güvenlik, ulusal güvenliğin önemli bir unsuru haline gelmiştir. İnternetin, ülkelerin sınırlarını aşan yapısı, internet ağlarının bireysel hizmetlerin ve amaçların ötesinde devletin kritik altyapılarında ve kamu hizmetlerinin yürütülmesinde kullanılması, gün geçtikçe gelişen e-devlet uygulamaları, siber güvenliğin ulusal güvenlik içerisindeki önemini daha da pekiştirmiştir. Bu bağlamda, çalışmada ABD, Rusya ve Çin'in siber güvenlik politikaları, özellikle bu üç ülkede yayınlanan resmi politika belgeleri temelinde incelenmekte ve karşılaştırmalı bir analiz yapılmaktadır.

Anahtar Kelimeler: *Siber Güvenlik, Ulusal Güvenlik, Ülkelerin Siber Güvenlik Politikaları, Karşılaştırmalı Analiz.*

CYBER SECURITY POLICY: A COMPARATIVE ANALYSIS ON USA, RUSSIA AND CHINA

Abstract

The importance of country borders within the national security policy has begun to diminish continuously with the acceleration of the globalization process in recent years. With globalization, the power distribution channels of the countries have been reshaped; asymmetrical power relations have emerged and the needs for national security of countries have been redefined. Technological developments in recent years have disclosed the concept of cyber security and cyber security has become an important element of the national security of countries. The structure of the Internet that exceeds the borders of countries, the use of internet networks in the critical infrastructures of the state and in the execution of public services beyond the individual services and objectives, and the increasing e-government applications have further reinforced the importance of cyber security in national security. In this context, the study comparatively examined the cyber security policies of the USA, Russia and China particularly on the basis of official policy documents published in these three countries and such an analysis is presented.

Keywords: *Cyber Security, National Security, Cyber Security Policies of Countries, Comparative Analysis.*

[*] Bu çalışma, Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü bünyesinde, Prof. Dr. Mehmet Devrim AYDIN danışmanlığında, Dr. Öğr. Üyesi Volkan GÖÇOĞLU tarafından yazılan ve 28.12.2017'de jüri önünde savunularak kabul edilen "Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi" başlıklı doktora tezinden üretilmiştir.

[**] Dr. Öğr. Üyesi, Afyon Kocatepe Üniversitesi, Dinar Uygulamalı Bilimler Yüksekokulu, volkangocoglu@gmail.com, https://orcid.org/0000-0002-7036-2416.

[***] Prof. Dr., Hacettepe Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, mdaydin@hacettepe.edu.tr, https://orcid.org/0000-0001-8959-6194.

Makale Geliş Tarihi: 07.02.2019 Makale Kabul Tarihi: 15.08.2019

GİRİŞ

Son yıllarda giderek hız kazanan küreselleşme süreci, ülkelerin sınırlarının ulusal güvenlik politikası açısından taşıdığı önemi azaltmaya başlamıştır. Küreselleşme; ülkelerin güç dağılım kanallarını yeniden şekillendirmiş, asimetrik güç ilişkilerini ortaya çıkarmış ve ulusal güvenlik ihtiyaçlarının daha kapsamlı ve farklı şekillerde yeniden tanımlanmasına neden olmuştur (Kay, 2004). Savaşlar ve iç isyanlar bir kenarda tutulduğunda, küreselleşmenin sonucunda ülkeler arası güç dengelerini etkileyen unsurlar değişime uğramış, ülke çıkarlarının korunması küreselleşme öncesi döneme göre daha zor bir hale gelmiştir (Kirshner, 2006: 2). Bu denge değişiminde "siber güvenlik", ulusal güvenlik politikasının yeni ve oldukça kritik bir unsuru olarak ön plana çıkmıştır.

Bu çalışmada, "Etkili bir siber güvenlik politikasının temel boyutları neler olmalıdır?" araştırma sorusundan hareketle, ABD, Rusya ve Çin'in siber güvenlik politikaları, resmi politika belgeleri ve ilgili literatür üzerinden karşılaştırmalı olarak incelenmiştir. Söz konusu üç ülkenin seçilme nedeni, bu ülkelerin gerek ekonomik, gerekse askeri unsurlar bakımından dünyada "başat güç" ya da başka bir deyişle "süper güç" olarak kabul edilmeleridir. Dolayısıyla, bu ülkelerin siber güvenlik politikalarının, sahip oldukları siber güvenlik donanım ve tecrübelerinin incelenmesinin, araştırma sorusuna yanıt arama sürecinde son derece anlamlı olacağı düşünülmüştür. Araştırma yöntemi olarak nitel araştırma yöntemi, veri toplama tekniği olarak ise doküman analizi ve ikincil verilerden yararlanma tekniği kullanılmıştır. Bu çerçevede seçilmiş ülkelerin siber güvenlikle ilgili resmi dokümanları üzerinde bir doküman analizi yürütülmüştür. Çalışmanın ilk bölümünde, siber güvenlik ve ilgili kavramlar ele alınmıştır. Çalışmanın ikinci bölümünde siber güvenlik, ulusal güvenliğin kritik bir parçası olarak incelenmiştir. Çalışmanın üçüncü bölümünde ise Clarke ve Robert'ın (2010) çalışması ve Uluslararası Telekomünikasyon Birliği'nin raporları (ITU, 2015; 2017; 2018) ele alınmış ve Amerika Birleşik Devletleri (ABD), Rusya ve Çin'in siber güvenlik politikaları bunlarla ilişkilendirilerek analiz edilmiştir. Sonuç bölümünde ise araştırmadan elde edilen sonuçlar ortaya konmuştur.

1. SİBER GÜVENLİK VE İLGİLİ KAVRAMLAR

Siber güvenliğin genel olarak üzerinde uzlaşılmış belirli bir tanımı yoktur. Korff (t.y., 1-4), çalışmasında siber güvenliğin çeşitli kurumlarca yapılmış tanımlarına yer vermiştir. Buna göre NICE (The National Initiative for Cybersecurity Education) siber güvenliği; "bilgi ve iletişim sistemleri ile bu sistemlerin içerisinde yer alan bilgilerin herhangi bir zarara, saldırıya ya da yok edilmeye karşı korunduğu, savunulduğu bir faaliyet ya da süreç" olarak tanımlamaktadır.

Uluslararası Telekomünikasyon Birliği[1] (ITU, 2015) ise siber güvenliği "siber çevre, kurumlar ve bireylerin varlıklarını korumak adına kullanılabilecek araçların, politikaların, güvenlik kavramlarının, güvenlik talimatlarının, risk yönetim yaklaşımlarının, eylemlerin, en iyi örneklerin, güvence ve teknolojilerin toplamı" olarak tanımlamaktadır.

Siber güvenlik, siber uzayda (cyberspace) sağlanan güvenlik olarak düşünülebilir. Siber uzay, fizikî donanımların ortaya çıkardığı ve barındırdığı bir alan olmasına karşın, somut bir alan değildir. Siber uzay sadece internetle birlikte var olan bir alan da değildir. İnternete bağlı olmayan bilgisayarlar ya da farklı ağlar da siber alan oluşturabilir. Siber uzay birden fazla soyut olgunun bir araya gelmesinden de oluşabilmektedir. Yazılımlar, bilgiler ve ağlar buna örnek olarak verilebilecektir (Clark, vd., 2014). Bir diğer deyişle, siber uzay; "tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan bir ortam" olarak tanımlanabilir. Kavram ilk defa, bilim kurgu romanlarıyla tanınan William Gibson tarafından 1980'lerin başında kullanılmıştır (Kara, 2013: 4). Birleşik Krallığın siber güvenlik strateji belgesinde ise siber uzay "bilgileri saklamaya, düzenlemeye ve birbiri arasında alışveriş yapmaya imkân veren, bilgisayar, internet ve diğer sistemleri içeren altyapısal ve sektörel sistemleri destekleyen, dijital ve interaktif bir bağlantı ağı" (GCHQ, 2012: 3) olarak tanımlanmıştır. Günümüzde siber uzayla eş anlamlı olarak "siber ortam" terimi de kullanılmaktadır.

Yue (2003: 566-568), siber güvenliğin araçlarını üç kategoriye ayırmaktadır. Birinci kategori "optimal tasarım" kategorisidir. Optimal tasarım; ağın kendini yenilemesi, onarması ve restore etmesini ifade etmektedir. Aynı zamanda bu ağın ne kadar bağlanılabilir ya da kapsayıcı (kapasite) olduğu ve bu kapasitenin arttıkça kapsadığı bağlantı sayısıyla birlikte tehditlere karşı ne kadar güvenli olduğu konusu da optimal tasarımla ilgilidir. İkinci kategori "sürekli ağ denetimi" kategorisidir. Burada ağın sürekli ve devamlı olarak gözlemlenmesi ve zayıf yönlerinin belirlenmesi söz konusudur. Ağda meydana gelecek problemler için teknik çözümler de kullanılabilecektir. Bu kategori aynı zamanda ağın güvenilirliği hakkında referans veren kategoridir. Son kategori ise "sonraki nesillerin güvenliği" kategorisidir. Söz konusu siber ortam ağlarında, birçok farklı güvenlik kriptoları kullanılabilmektedir. Ağlarda yer alan kriptolama sistemlerinin kalitesi ya da fazlalığı, ağ için katlanılacak olan maliyetin yanı sıra ağın gelecek siber saldırılara karşı dayanıklılığını da artıracaktır. Dolayısıyla ağı kullanacak olan gelecek neslin güvenliği de artmış olacaktır. Siber güvenlik, bu anlamda yukarıda da bahsedilen siber uzayın ya da ağların güvenliğinin sağlanması anlamına gelmektedir.

[1] International Telecommunication Union (ITU)

Siber güvenlik, bir takım yeni kavramları da beraberinde getirmiştir. Bunlardan ilki "siber saldırı"dır. Siber saldırılar, temelde insan kaynaklı eylemlerdir. Her ne kadar kullanılan araçlar ve hedef alınan noktalar sanal ortam ve verilerden oluşsa da saldırıların sonuçları insanları etkilemekte ve amaçları da insanların oluşturdukları amaçlara dayanmaktadır. Lu (2014: 11) siber saldırıların klasik hackerlar, paralı hackerlar, hacktivistler, iç mihraklar (kötü niyetli olmalarına gerek olmaksızın) ve ulus devletlerce yapılabileceğini belirtmektedir. Siber saldırıları gerçekleştiren bu unsurlar hedef olarak bireyleri, firmaları ve devlet kurumlarını hedef alarak onların ağlarına girmeyi deneyebileceklerdir. Siber saldırılar, bilgi barındıran sanal ağlara, bilgileri çalmak, değiştirmek ya da yok etmek amacıyla yapılabilmektedir. Söz konusu saldırılar bilgisayardan bilgisayara, cihazların ya da onların içerisindeki bilgilerin gizlilik, bütünlük ve ulaşılabilirliğini tahrip etmek için yapılmaktadır (O'Shea, 2003: 6).

Siber güvenlikle ilişkili bir başka kavram ise "siber sömürü"dür. Siber sömürü, bir siber ortamdaki siber güvenlik kusurlarından ortaya çıkan ve güvenlik açıklarının kullanılması sonucu ortamdaki bilgilerin çeşitli amaçlar doğrultusunda istismarına dayanan bir eylem ve aynı zamanda bilişsel bir suçtur. Erickson'a göre (2008, 115-118), siber sömürünün en etkili yöntemlerinden biri, bilgisayar programlarının güvenlik açıklarından yararlanarak onların içerisine sızarak onu kullanan kişi ya da kurumun bilgisi dışında, programı farklı amaçlar doğrultusunda kullanmaktır. Bu yöntemle programın güvenlik açıklarından faydalanılarak program ya farklı işlevlerde ya da kendi programlandığı işlevler doğrultusunda, ancak farklı amaçlarla kullanılabilecektir. Örneğin bir program, kendisinin bir işlevi gereği bilgisayardaki klavye hareketlerini (basılan tuşlar vb.) kayıt altında tutmaktadır, ancak bir hacker bunu siber sömürü olarak bilgisayarda diğer internet siteleri ya da banka hesabı şifrelerini öğrenmek ve ele geçirmek adına kullanabilecektir.

Siber güvenlik konusunda değinilmesi gereken önemli bir kavram da "kritik altyapı" kavramıdır. Bir ülkede kritik altyapı sayılabilecek her unsur siber güvenlik açıkları doğrultusunda birer hedef haline gelebilecektir. Bu anlamda hangi unsurların birer kritik altyapı sayılacağına değinmekte yarar vardır. AB Komisyonunun hazırlamış olduğu 2004 tarihli, 702 sayılı ve "Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunması" başlıklı tebliğde Kritik altyapı; "…insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güvenliklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları" şeklinde tanımlanmıştır. Bu bağlamda ülkeden ülkeye değişebilecek olsa da en genel hatlarıyla; bankacılık ve finans, enerji, gıda, iletişim, nükleer, su, turizm, ulaşım ve uzay sistemlerine yönelik altyapıları kritik altyapı sayılabilecektir.

Siber güvenlik konusunda öncelikli olarak değinilmesinin gerekli olduğu düşünülen kavramlar yukarıda ele alınmıştır. Bunlar dışında siber güvenlikte risk, tehdit, güvenlik açığı, zararlı yazılım vb. birçok kavram yer almakla birlikte bu kavramlar günlük hayatta da sıkça başka konular içerisinde kullanılan kavramlardır. Bu kavramlar, siber güvenlik konusunda da genel anlamlarına yakın olarak kullanıldığından dolayı ve çalışmanın uzunluğunu makul seviyede tutmak için ayrıca ele alınmayacaktır.

2. ULUSAL GÜVENLİK POLİTİKASININ KRİTİK BİR PARÇASI OLARAK SİBER GÜVENLİK

Ulusal güvenlik politikası; bir ulusun, askeri ve sivil tüm kaynaklarının ve araçlarının, topyekûn ve koordineli bir şekilde, "savunma görevlerini gerçekleştirmek" ve "milli çıkarları korumak" amacıyla kullanılmasına dayanan bir planı ifade etmektedir. Her ülke, örtülü ya da açık şekilde bir ulusal güvenlik politikasına sahiptir. Açık olan güvenlik politikaları belgelerden ve planlardan okunurken, örtülü politikalar ise ülkelerin güvenlikleri ile ilgili zaman içinde attıkları adımların ayak izlerinden okunarak, hamlelerin gideceği yönün öngörülmesi suretiyle tahmin edilebilmektedir (Doyle, 2007: 624). Devletlerin atacakları bu adımlar daha geri planda, toplumlarının sosyal karakteristiklerine ve onun ötesinde de stratejik kültürlerine göre şekil almakta (Lantis, 2002: 87-88) ve ulusal çıkarların itici kuvveti ile küresel sahadaki hareket alanlarının durumuna göre ilerlemektedir.

Ulusal güvenlik politikası süreçlerinin daha iyi anlaşılabilmesi için çeşitli yaklaşımlar geliştirilmiştir. Örneğin Gohlert (1974: 174), bu amaçla; "neyin güvenliği ve ne için?" sorusunun yanıtlanması gerektiğini belirtmiştir. Onun bu sorusuna Kamu Tercihi Kuramının penceresinden yaklaşan, Lehman ve Willett (1986), ABD'deki ulusal güvenlik politikalarını ele almışlardır. İncelemelerinin sonucunda, ulusal güvenliği sağlamak üzere yürütülen politikalarda dikkat çeken iki tip probleme rastlanmıştır; Birinci tip problemdeki konu, özel sektörün ulusal güvenlik politikası doğrultusunda üretime nasıl teşvik edileceği konusudur. Kamu tercihi kuramının ilkelerinden olan fayda maksimizasyonu (Buchanan, 1984), ulusal güvenlik konusunda devlet ve özel sektör arasında da kendini göstermekte ve özel sektörün üretim hedefleri buna göre şekil almaktadır. Lehman ve Willett'in (1986: 45-46) ortaya koydukları birinci tip probleme göre, devletler ulusal güvenliği sağlamak amacıyla farklı araştırma ve geliştirme (Ar-Ge) çalışmalarını (örneğin siber güvenlik) desteklemek isteyebilir. Bu çalışmalar özel sektör açısından bir kâr getirmeyecekse özel sektör bunun yerine daha çok para kazandığı spesifik bir silah üretimine yönelebilecektir. Söz konusu silah üretimi, devlet açısından ülkenin ulusal güvenliği için bir öncelik değilse, burada bir çatışma söz konusu olmaktadır. Bu problemin çözümü için Ar-Ge ve fizikî üretim için yapılacak kontratların ayrı şekillerde düzenlenmesi ve buna ek olarak Ar-Ge

faaliyetleri için hizmet satın alma teşviklerinin iyileştirilmesi politikası yararlı olabilecektir. İkinci ve diğerine nazaran daha temel olan problem tipi ise ulusal güvenlik politikasında yer alan aktörlerin daha iyi sonuçlar alınması amacıyla teşvik edilmesi problemidir. Söz konusu aktörler, devletin farklı kurumları, özel sektör, ilgili sivil toplum kuruluşları ve vatandaşlardan oluşmaktadır. Problemin çözümü ise, aktörlerin sağlıklı etkileşimine zemin hazırlayacak kapsamlı kurumsal reformların yapılmasında görülmüştür. ABD merkezli bu ve benzeri çalışmalarda, göze çarpan nokta, bir kamu politikası olarak ulusal güvenlik politikası oluşturma ve uygulama sürecinde farklı aktörleri dikkate alan liberal bir bakış açısının benimsenmiş olmasıdır.

Ulusal güvenliğin, kapsamlı bir kamu politikası olarak ele alınması, günümüzde oldukça değişen "ulusal güvenlik algısı"nın bir gereğidir. Devlet yönetimlerinin, özellikle Dünya Savaşları'ndan sonra ulusal güvenliği sadece ülkeye yönelik askeri saldırılar ve bu saldırılara karşı alınacak askeri-politik stratejiler olarak görmesi, bugün hatalı bir tutum olarak kabul görmektedir. Bello'nun (2011: 68) da belirttiği üzere artık ulusal güvenlik, sadece fizikî ve askeri saldırılara yönelik tedbir alınmasından ve bu saldırıların engellenmesinden oluşmamaktadır. Siber saldırılar, ekonomik büyümenin sekteye uğratılması, terör, salgın hastalıklar, iç ayaklanmalar, göçler ve küreselleşme ile gelen ve gelecek yeni tehditler de ulusal güvenliğin kapsamına girmiştir. Bu bağlamda ulusal güvenlik; sadece askeri stratejiler odaklı bir politika olarak değil, kamu düzeni ve kamu yararını, insan haklarını, ekonomik fayda-maliyet analizleri yanında milli, kültürel ve insani değerleri de göz önünde bulunduran" kapsamlı bir kamu politikası" olarak düşünülmelidir.

21. yüzyılda siber güvenlik, ulusal güvenliği yakından ilgilendiren ve ulusal güvenlik politikaları oluşturulurken hesaba katılması gereken konuların başında gelmektedir. Siber güvenliğin önemine ilişkin olarak PEW Araştırma Merkezi'nce (PEW Research Center) hazırlanan bir araştırmaya (2014) göre, araştırmaya katılan 1.600 teknoloji uzmanının 3'te 2'si 2025 yılına kadar büyük bir maddi hasar ve can kaybının yaşanacağı bir siber savaş beklemektedir (Rainie, vd., 2014'ten akt. Kshetri, 2016: 54). Siber güvenliğin ulusal güvenlik bağlamındaki bu yüksek risk potansiyeli, ona yönelik politikalar oluşturmayı da gerekli kılmaktadır.

Siber güvenlik konusuna ulusal bir perspektiften yaklaşan Cavelty (2014), siber güvenlik açıklarının gün geçtikçe fazlalaştığını, bunun doğrultusunda ise kişisel ve ulusal siber güvenliğin azaldığını savunmaktadır. Büyük ve uluslararası firmaların tüketici odaklı yaklaşımlarının ve vatandaşların bireysel özgürlük taleplerinin yanında devletlerin de geçmişten bu yana düstur edindikleri kritik altyapıları koruma politikaları, siber güvenliği ulusal bir güvenlik unsuru olarak ele alama tutumları ve siber güvenliğin sağlanması için radikal politika üretimi eğilimleri, siber güvenlik konusunda bir ikilem meydana getirmektedir. Bu ikilemde, birey

özgürlüğü ve ulus güveliği çatışmaktadır. Devletler kritik altyapıların korunmasına ve siber güvenliğin artırılarak güvenlik açıklarının azaltılmasına yönelik olarak daha merkezi ve katı kurallar koymak üzere adımlar atacak iken, bireyler ise kendi özgürlüklerine yönelik olarak siber uzaydaki hareket alanlarını en serbest şekilde muhafaza etmek istemektedir. İkilem bu çatışmadan doğmaktadır. Bu ikilemde, uluslararası şirketler de liberal görüşün etkisinde, bireylerin tutumundan yana taraf almaktadır. Devletler açısından, siber uzayda bireylere ve firmalara (özellikle yazılım firmalarına) sunulan serbesti, aynı zamanda ulusal siber güvenlik açısından genişleyen güvenlik açıklarını da beraberinde getirmektedir. Bu ikileme çözüm olarak, geniş kapsamlı tanımları ve birbirine bağımlı değişkenleri içeren, bireysel ve ulusal güvenlik önceliklerini belirleyerek bir uzlaşma temelinde oluşturulacak olan siber güvenlik politikası düşünülmektedir.

3. ABD, RUSYA VE ÇİN'DE SİBER GÜVENLİK POLİTİKASI

Clarke ve Robert (2010), siber güvenlik konusunda süper güç kabul edilen ülkelerin siber tehditlere karşı dayanıklılıklarını ölçebilmek için bir puanlama yöntemi geliştirmiştir. Söz konusu yöntem, tüm ülke bağlantısını bir anda kesebilmek, internet ağının yayılımı, siber bağımlılık, sunucuların (server) gücü gibi kriterleri kapsamaktadır. Bu doğrultuda Clarke ve Robert (2010)'ın yapmış olduğu puanlamada yer alan ve bu çalışmanın konusunu da oluşturan üç ülkenin siber güvenlik puanları ve ilgili değişkenler aşağıdaki tabloda sunulmuştur:

Tablo 1: Clarke ve Robert'a Göre Ülkelerin Siber Güvenlik Puanlamaları (Clarke ve Robert, 2010).

Unsurlar	ABD	Rusya	Çin
Siber Saldırı	8	7	5
Siber Bağımlılık[2]	2	5	4
Siber Savunma	1	4	6
Toplam	11	16	15

[2] Burada yer alan "siber bağımlılık" kavramı ilk bakışta olumsuzluk belirten bir kavram olarak algılanabilecek olsa da destek mekanizmaları, elektrik sistemleri, hat borularının da siber sisteme bağlı olma durumunu ve bunların tek bir merkezden kontrol altında tutulabilmesine yarayan bir sistemi belirtmektedir.

Ülkelerin siber güvenlik konusundaki mevcut durumlarını ve gelişimlerini sunan güncel ve küresel bir çalışma da belirli aralıklarla Uluslararası Telekomünikasyon Birliği tarafından hazırlanan rapordur (ITU, 2015, 2017, 2018). Rapor, ülkelerin siber güvenlik durumlarını değerlendirirken aşağıdaki göstergeleri temel almaktadır:

- Ülkede yürürlüğe konulan siber suç mevzuatı
- Ülkede bulunan Bilgisayar Acil Müdahale Ekibi (Computer Emergency Response Team/CERT), Siber Olaylar Müdahale Ekibi (Computer Incident Response Team/CIRT), Bilgisayar Güvenliği Müdahale Ekibi (Computer Security Incident Response Team/CSIRT)
- Belirlenen ulusal siber güvenlik stratejileri ve ölçütlerinin mevcudiyeti
- Siber güvenliğe dair farkındalık kampanyalarının mevcudiyeti
- Siber güvenliğe dair mesleki eğitim
- Siber güvenlik ile ilgili uluslararası forumlara katılım
- Siber güvenlik ile ilgili kamu-özel sektör işbirliği

Yukarıda sıralanan ölçütlerin belirlenmesi için birlik, ülkelerin ilgili birimlerine iletilmek üzere çeşitli anketler hazırlamakta ve bu anketleri ilgili birimlerde uygulatmaktadır. Verilerin doğrulanması için ise doküman analizi, ülkelerin resmi internet sitelerinden veri toplanması gibi ikincil veri toplama yoluna başvurmaktadır. Birliğin 2018 yılı raporuna göre, bu çalışmada odak alınan ülkeler olan ABD, Rusya ve Çin'in siber güvenlik skorları aşağıdaki tabloda sunulmuştur.

Tablo 2: Uluslararası Telekomünikasyon Birliğine Göre Ülkelerin Siber Güvenlik Puanlamaları (ITU, 2015, 2017, 2018).

Ülke	Skor 2015	Dünya Sıralaması 2015	Skor 2017	Dünya Sıralaması 2017	Skor 2018	Dünya Sıralaması 2018
ABD	0.824	1	0.925	2	0.926	2
Rusya	0.500	12	0.788	10	0.836	26
Çin	0.441	14	0.624	32	0.828	27

İki tablo arasındaki sıralamada ciddi farklılıklar göze çarpmaktadır. İki tablo arasındaki fark, siber güvenliğin hızla değişen dinamik bir alan olmasından kaynaklanabileceği gibi, tabloların oluşturulma ölçütlerinin farklılığından da

kaynaklanabilir. Birinci tablo, nicel verilerden ziyade dönem içerisindeki örnek olaylar temel alınarak yazarların yorumları sonucu oluşturulmuş, kriterleri net olarak belirlenmemiş ve temsili sayılabilecek bir tablo iken; ikinci tablo daha net belirlenmiş kriterler doğrultusunda hazırlanmıştır. Bunun ötesinde Uluslararası Telekomünikasyon Birliği tarafından sunulan ve Tablo 2'de alıntılanan raporun 2015 ve 2017 yıllarında ülkelerin o dönemki siber güvenlik durumlarını gösteren versiyonları da yayınlanmıştır. Bu yönüyle söz konusu sıralama daha sistematik bir nitelik taşımaktadır.

Tablo 1'de ABD, puanlar toplamında üç ülkeden en kötü durumda olan olarak belirlenmişken, Tablo 2'deki sıralamada 2015, 2017 ve 2018 yıllarında açık ara en iyi durumda olan ülke olarak belirlenmiştir. Bunun dışında her iki tabloda da Rusya ve Çin arasındaki puan farkının çok açık olmadığı gözlemlenirken, Rusya'nın Çin'den bir adım önde olduğu ortak sonucu ortaya çıkmıştır. Tablo 2'de göze çarpan başka bir sonuç ise ABD dışında, Rusya ve Çin'in önünde ismi belirtilmeyen birçok ülkenin bulunduğudur. Zira Rusya'nın sıralaması artan yıllar temelinde 12, 10 ve 26 iken Çin'in sıralaması ise 14, 32 ve 27'dir. Bu sonuç, araştırmada örneklem olarak alınan ve ülkeler arasında "süper güç" olarak nitelendirilen üç ülke olan ABD, Rusya ve Çin'in siber güvenlik konusunda aynı nitelemeyi hak etmediğini ortaya çıkarmaktadır. Ülkelerin kendi sıralamalarının yıllar bazında farklılaşmasının sebebi ise ülkelerin raporda belirlenen kriterlere, ilgili değerlendirme yılı içerisinde gerçekleştirdikleri uyum farklılıklarından kaynaklanmaktadır.

Ülkeler, özellikle ulusal güvenliklerinin sağlanması ve kritik altyapıların korunması noktasında geleneksel güvenlik yöntemlerinin yanı sıra gelişen teknolojiler ve bu teknolojiler beraberinde dönüşen kritik altyapılarla birlikte siber güvenlik konusunda farkındalık kazanmaktadırlar. Zira siber güvenlik, kritik altyapılar olan bilgisayar sistemleri, bilgi sistemleri, iletişim, enerji, su, finans sistemleri gibi sistemlerin yanında önceki dönemlerde fizikî olan ancak içinde bulunulan dönemde büyük oranda (özellikle yönetim mekanizmaları) siberleşmiş enerji ve endüstriyel kontrol sistemlerinin güvenliğini de içeren ve Tablo 2'de görüldüğü üzere ülkelerin fizikî ve ekonomik güçlerinin ötesinde bir güvenliği nitelemektedir. Bu bağlamda ülkeler, ulusal anlamda kritik altyapıları ve kamusal bilgi ve belgeleri, bireysel anlamda ise vatandaşların bilgi güvenliğini sağlamak üzere çeşitli siber güvenlik stratejileri oluşturmakta ve siber güvenlik politikaları uygulamaktadır. Başlığın ilerleyen kısımlarında söz konusu politikalar ABD, Rusya ve Çin temelinde ele alınacaktır.

3.1. Amerika Birleşik Devletleri'nin Siber Güvenlik Politikası

ABD'nin siber güvenlik politikasını anlamak için öncelikle bu politikanın hangi bileşenlerden ve aktörlerden ileri gelerek oluşturulduğunu belirlemekte yarar vardır. Bu bağlamda ABD'nin siber güvenlik politikası üzerine yönelimlerinin Ulusal Güvenlik Politikası ve Stratejisi, diğer stratejik belgeler, kanunlar, direktifler ve önerilen düzenlemeler, siber güvenlik ile ilgili kurumlar (9/11 komisyonu da dâhil olmak üzere) ve son olarak düşünce üretim kuruluşlarının (think-tank) etkisiyle (Tirrell, 2012: 7) gerçekleştiği söylenebilecektir. Çizilen bu çerçeve, ele alınacak olan diğer ülkeler için de ana çerçeve olarak kullanılabilecektir.

ABD'de siber güvenlik ile ilgili olarak yayınlanan ilk kapsamlı belge Beyaz Saray tarafından 2003 yılında yayınlanan "Secure Cyberspace" (Güvenli Siber Uzay) belgesidir (WH, 2003). Bu belge incelendiğinde, belgede "siber güvenlik" terimin yalnızca üç kez geçtiği görülmekte ve bunun yerine genel olarak güvenli siber uzay teriminin kullanıldığı görülmektedir. Belgede siber uzay, "kritik altyapıların işleyişini sağlayan ve birbirine bağlı yüzbinlerce bilgisayarın, sunucunun (server), modemlerin, anahtarların, fiber optik kabloların oluşturduğu alan" olarak nitelendirilmiştir (WH, 2003: vii). Siber uzayın korunması, ulusal güvenliğin sağlanmasında önemli bir bileşen olarak görülmüş ve belge, Ulusal Güvenliğin Sağlanmasına Yönelik Ulusal Strateji (National Strategy for Homeland Security) ile Kritik Altyapıların ve Değerli Varlıkların Fizikî Olarak Korunmasına Yönelik Ulusal Strateji (National Strategy for the Physical Protection of Critical Infrastructures and Key Assets) belgesinin uygulama bölümü olarak hazırlanmıştır. Belge, siber güvenlik konusuyla ilgili olan ulusal ve federal kurumların direktiflerini içermekte ve devlet ile yerel yönetim kurumlarının, özel sektör firmalarının, sivil toplum kuruluşlarının ve vatandaşların kolektif siber güvenliği geliştirmek üzere atacağı adımları belirlemektedir.

Secure Cyberspace belgesine göre, ulusal güvenliğin sağlanmasında beş adet ulusal öncelik bulunmaktadır. Bu öncelikler ulusal bir siber uzay güvenliği karşılık sistemi, ulusal bir siber uzay güvenliği tehdit ve güvenlik açığı savunma programı, ulusal bir siber uzay güvenliği farkındalık ve geliştirme programı, hükümetin siber uzayını güvenlik altında tutma, ulusal güvenlik ve uluslararası siber uzay güvenliği işbirliğidir.

Yukarıda adı geçen Secure Cyberspace belgesini, uygulama alanı olarak alt kategorisinde şekillendiren Siber Uzay Güvenliği Ulusal Stratejisi belgesi ise, ulusal siber güvenliğin sağlanması ardından karşı cevap verilmesine yönelik sekiz önemli eylem ve gelebilecek olan siber tehditlere karşı önlem niteliğinde sekiz önemli öncelik tanımlamaktadır (WH, 2003: x). Bunlar aşağıdaki tabloda gösterilmiştir:

Tablo 3: Siber Güvenlikte Sekiz Önemli Öncelik (WH, 2003: x.).

Tehditlere Karşı Eylem	Tehditlere Karşı Önlem
Kamu-özel işbirliği.	Gerekli hukuki düzenlemeler.
Taktiksel ve stratejik analizler.	Güvenlik açıkları ve sonuç analizi.
Sinoptik bir bakış açısı geliştirmek üzere özel sektör kapasite artırımı.	internet mekanizmalarının güvenliğini sağlanması.
Siber uyarı ve bilgilendirme ağının genişletilmesi.	Güvenilir dijital kontrol ve veri güvenliği sistemlerinin kullanımının yaygınlaştırılması.
Ulusal olaylar yönetiminin geliştirilmesi.	Yazılım açıklarının önlenmesi.
Ulusal boyuttaki kamu-özel işbirliğinde gönüllü katılımı.	Siber ağlar ve iletişim sistemlerinin fiziksel güvenliklerini sağlamak.
Federal siber güvenlik planlarının yürütülmesi.	Federal siber güvenlik ar-ge kurumlarının önceliklendirilmesi.
Kamu-özel sektör arasındaki bilgi akışı ve paylaşımının geliştirilmesi.	Aciliyet sistemlerini değerlendirilmesi ve güvenliklerinin sağlanması.

Belge genel olarak yukarıda ele alınan öncelik ve eylem maddelerinin açılımları ve detayları üzerinden şekillenmektedir. Ulusal boyutta öne çıkan vurgu, kamu-özel sektör ve vatandaşların bireysel siber alanlarına yönelik koordineli güvenliğin sağlanması, işbirliği ve katılım, kritik altyapıların korunması, ortak işbirliği ve farkındalık programlarının geliştirilmesidir. Uluslararası boyutta ise Kuzey Amerika Güvenli Siber Uzayını oluşturmak üzere Kanada ve Meksika ile yapılacak olan, siber tehdit ve risklere karşı ulaşım, enerji dağıtımı, iletişim, bankacılık gibi ortak kritik altyapıların korunmasına yönelik işbirliği örneği göze çarpmaktadır.

2003 yılında yayınlanan Secure Cyberspace belgesinin dışında ABD siber güvenlik politikası üzerine ulaşılabilir diğer belgeler 2011, 2013 ve 2015 yıllarında yayınlanmıştır. 2011 yılında yayınlanan siber güvenlik strateji belgesi beş adet stratejik öncelikten oluşmaktadır. Bunlar, savunma departmanının organizasyonel olarak geliştirilmesi, yeni savunma içeriklerinin edinilmesi, kamu- özel işbirliği, diğer ülkelerle bu konuda güçlü ilişkiler kurulması ve yaratıcılığın artırılmasıdır (DOD, 2011).

2013 yılında DOD, "Savunma Departmanının Ağları, Sistemleri ve Bilgiyi Savunma Stratejisi" (DoD Strategy for Defending Networks, Systems, and Data) isminde bir belge yayınlamıştır (DOD, 2013). Belgede stratejinin ana hedeflerine, 2011 yılındaki belgeye ek olarak savunmada esneklik, asimetrik güvenlik tehditlerine karşı savunma ve bu amaca yönelik yeni savunma mekanizmalarının kurulması gibi yeni vizyonlar eklenmiştir.

2014 yılında ise Beyaz Saray Basın Ofisi ABD ile AB arasında yapılan siber güvenlik işbirliğine dair bir yazılı açıklama yapmıştır (WHOPS, 2014). Söz konusu işbirliği internet yönetişimi, internet özgürlüğü, siber uzayda insan haklarının korunması gibi konular üzerinedir. İşbirliğinde yer alan konu başlıkları ise uluslararası siber uzay gelişmeleri, online insan hakları tanıtımı ve korunması, yürürlükteki uluslararası hukukun uygulanışı, siber güvenlik ölçütleri geliştirme, siber ortamdaki davranış normları gibi uluslararası güvenlik konuları, üçüncü taraf ülkelerde siber güvenlik kapasitesi geliştirmedir.

DOD'un son olarak 2015 yılında yayınladığı diğer bir belge ise "Siber Strateji" (Cyber Strategy) ismini taşımaktadır. Belgeye verilen isim daha önceki isimlendirmeler olan "siber uzay güvenliği" ya da "siber güvenlik" isimlendirmelerine bakarak daha genel bir stratejiyi ifade eder niteliktedir. Belgenin içeriği incelendiğinde ise (DOD, 2015) belgenin, yeni bir siber stratejiyi ön görmekle birlikte stratejiye yönelik atılan somut adımların da altını çizdiği görülmektedir. Belge yeni bir siber stratejinin gerekliliği olarak üç durumdan bahsetmektedir. Birincisi ABD çıkarlarına, DOD ağlarına ve bilgi sistemlerine karşı artarak devam eden kapsamlı saldırılar; ikincisi, dönemin başkanı Obama'nın DOD'a diğer Birleşmiş Milletler (BM) ülkeleriyle birlikte hareket ederek bir savunma planı oluşturma direktifi ve son olarak da 2012 yılından itibaren DOD'un oluşturmaya başladığı ve kurumun görevlerini yerine getirmek üzere operasyonları yürütecek olan, sivil, askeri yaklaşık 6.200 personelden oluşan Siber Görev Güçleri (Cyber Mission Force/CMF) yeni stratejinin nedenleridir. Bu gelişmeler ve oluşan yeni bileşenler yeni bir stratejiyi gerekli hale getirmiştir. Bu yönleriyle 2015 yılında yayınlanan strateji belgesi, önceden de altı çizildiği üzere, somut adımlara önem vermiş gözükmektedir. Bu doğrultuda diğer belgelerde belirtilen stratejik hedeflerin dışında bu belgede, stratejik hedeflere ulaşılması için gerçekleştirilen uygulamalara da yer verilmektedir.

Tüm bu incelenen hususların doğrultusunda ABD'nin siber güvenlik politikası geliştirmede öncü bir ülke olduğu gözlemlenmektedir. Oluşturduğu siber altyapıların milli olması ülkenin siber bağımlılığını asgari düzeyde tutarken, kritik altyapıların büyük çoğunlukla siber altyapılara bağlı olması, ülkenin siber savunma fonksiyonunu zayıflatmaktadır. Bu durum Clarke ve Robert (2010)'ın ABD için yaptığı siber güvenlik güç puanlamasını doğrulamaktadır.

3.2. Rusya'nın Siber Güvenlik Politikası

Ulusal Güvenlik Strateji Belgesinde yeterince yer almamasına karşın, Rusya'nın siber güvenlik ile ilgili spesifik stratejiler oluşturarak belgeler yayınladığı ve dahi bu konuda ABD'den daha erken işe başladığı söylenebilecektir. Uluslararası İletişim Birliği Rusya'nın siber güvenlikle ilgili politikalarını belirleyen belgelerin 2000 yılından bu yana geliştirildiğini belirtmektedir. Bu belgeler (ITU, 2015), Rusya Federasyonu Bilgi Güvenliği Doktrini (RFBGD, 2000), Uluslararası Bilgi Güvenliğinde Rusya Federasyonu Devlet Politikası Temel Prensipler Belgesi (2013 ve 2020 yılları için çıkarılan iki adet) (Basic Principles for State Policy of the Russian Federation in the field of International Information Security) ve henüz taslak halinde bulunan Rusya Siber Güvenlik Stratejisi (RSG, t.y.) belgeleridir.

2000 yılında yayınlanan ilk belge (RFBGD, 2000); bilginin toplanması, tesis edilmesi, bilgi sistemleri ile bilgi ve iletişim teknolojileri, web siteleri, iletişim ağları, bilgi işlem süreçleri, bu teknolojilerin geliştirilmesi ve güvenliklerinin sağlanmasını konu almaktadır. Temel amaç ülke çıkarlarını iç ve dış bilgi konulu tehditlere karşı korumak ve sürekli gelişimi muhafaza etmektir. Bilgi güvenliğinin; istihbarat, karşı istihbarat, bilim ve teknoloji, bilgi analizi gibi fonksiyonlarla insani ve ekonomik kaynakların bilgiye karşı olan tehdidin öngörülmesi, belirlenmesi, önlenmesi ve zararlı sonuçlarının yok esilmesi amacıyla kullanılması esastır. Söz konusu bilgi güvenliği konusu, devlet kurumları, araştırma kurumları ve askeri-endüstriyel kurumların koordineli ve planı bir şekilde uygulayacakları aktiviteler ile sağlanacaktır (RFBGD, 2000: md.8-11). Bu aktivitelere ek olarak, siber uzaydaki artan karmaşıklık ve kritik altyapılara yönelik büyüyen tehdit, yabancı devletlerin Rusya Federasyonuna karşı gerçekleştirecekleri saldırılara yönelik oluşturulacak istihbarat ağının güçlendirilmesini gerekli kılmıştır. 2000 yılında yayınlanan belgede dikkat çeken önemli bir nokta da o dönemki yerli bilgi sistem ve teknolojileri ile bilgi güvenliği konusunda yapılan akademik çalışmalar ve oluşturulan insan kaynağının yeterli düzeyde görülmemesidir (RFBGD, 2000: md.18). Ülkelerin bilgi teknolojileri alanında kaydettikleri gelişmelerle siber uzaydaki hâkimiyetlerini artırarak, bu alanda domine olma hedefleri göz önüne alınarak Rusya'da çalışmalar hız kazanmalı ve yerli üretim sistem ve ağlara yönelinmesi gerekmektedir. Ülkelerarası bilgi güvenliğinin sağlanması ve ülkelerin stratejik istikrarlarının, eşitsizliklerin korunmasına yönelik uluslararası düzenlemelerin eksikliğinin altı çizilmektedir (RFBGD, 2000: md.19).

Ulaşılabilen kaynaklardan Uluslararası Bilgi Güvenliğinde Rusya Federasyonu Devlet Politikası Temel Prensipler Belgesi, 2020 (ISS, 2017) ele alındığında, belgenin başlığının spesifik olarak "bilgi güvenliği" kavramını içeriyor olması, siber güvenlik konusunun kapsamına daha yakın bir belge olduğunu göstermekle birlikte bu belgede de "siber güvenlik" terimi geçmemektedir. Belge, ulusal stratejik hedeflerden ziyade, uluslararası hedefleri belirtmeye yöneliktir. Buna

rağmen bu strateji belgesinin hukuki altyapısını, yapılan uluslararası anlaşmaların yanında, federal kanunlar ve ulusal anlamda gerçekleştirilen diğer hukuki düzenlemeler oluşturmaktadır (ISS, 2017: md.3). Belgedeki temel prensiplere bakıldığında; federe hükümetler ile Rusya'nın uluslararası bilgi güvenliğini sağlamak üzere, hükümetler arası hedef planlarını, konuyla ilgili hukuki ve örgütsel fonksiyonları da dahil ederek daha iyi bir uluslararası bilgi güvenliği sistemi oluşturmaya yönelik hazırladığı göze çarpmaktadır. Bununla birlikte, stratejik belgelerin etkili uygulanabilmesi amacıyla kurumlar arası iş birliğinin sağlanması ve reel ekonomide, bilgi iletişim teknolojilerini ileri düzeyde kullanan diğer güçlü devletlerle Rusya'nın gelişmişlik eşitliğinin sağlanması ve korunması temel hedefler arasında yer almaktadır.

Belgede, 2000 yılında yayınlanan belgeye göre bilgi güvenliği açısından daha kapsamlı tanımlara yer verilmiştir. Buna göre uluslararası bilgi güvenliği kavramı (ISS, 2017: md.6), "bireysel hakların gaspı olasılığını, bireysel, toplumsal ve ülkesel bilgi alanına karşı tehditleri, kritik bilgi altyapıları üzerindeki yıkıcı ve kanuni olmayan etkileri önlemek adına küresel bilgi alanında sağlanan durum" olarak tanımlanmaktadır. Uluslararası bilgi güvenliği sistemi ise "bilgi alanında farklı aktörlerin aktivitelerini düzenleyen ulusal ve uluslararası kurumlar seti" şeklinde tanımlanmış olup bilgi güvenliği sistemi bu kurumların özneleştirilmiş hali olarak ele alınmıştır (ISS, 2017: 2). Belgede, hedeflere ulaşmak üzere araç olarak kullanılacak olan kurumlarda başat aktör federal yönetim organları gösterilirken, bu organların yapacakları kamu-özel sektör işbirliğinin de altı çizilmiştir. Federasyonun güvenlik konseyi ise yönetim organları arasındaki koordinasyonu sağlayacak yönlendirici birim olarak görülmüştür. Rusya'nın siber güç anlayışını yukarıda olduğu gibi resmî belgelerin dışında, aynı zamanda Rusça literatürde inceleyen ve Rusya'nın siber güvenlik politikasını Jervis'in saldırı-savunma kuramı üzerinden değerlendiren Medvedev (2015: 3), ülkenin siber görevler üstlenen kurumlarını; Federal Güvenlik Servisi (Federal Security Service/FSB), Dış İstihbarat Servisi (Foreign Intelligence Service/SVR) ve ordunun Ana İstihbarat Direktörlüğü (Main Intelligence Directorate/GRU) olarak sıralamıştır. Diğer yandan araştırmanın önemli bir sonucu da, Rusya'nın siber güvenlik anlayışının savunmadan daha ziyade saldırıya dayandığı saptamasıdır. Savunma anlayışı sadece yapılacak yatırımların daha dikkatli bir şekilde şekillendirilmesine yön verirken, literatürde devletin siber güvenlik anlayışının, rakipleri düşman olarak görmek ve saldırılara saldırı ile karşılık vermek üzere strateji geliştirmek olduğu görüşü ağır basmıştır.

Giles (2013)'in çalışmasında ise yukarıda incelenen strateji belgelerini destekler biçimde Rusya'nın vatandaşların internet ve sosyal medya kullanımında aktivist hareketlerin önüne geçmek adına bir takım sansür ve sınırlamalara gittiği vurgulanmaktadır. Bu sınırlamaların federal hukuki altyapıları da bulunmaktadır. Diğer ülkelerde olduğu gibi internet ve siber uzay, Rusya'da da politik olmaktan

çok ekonomik ve sosyal bir oluşum olarak görülse de 2011-2012 yıllarında yapılan seçimlere yönelik protestoların sosyal medya ve internette geniş bir eyleme dönüşmesi bu görüşü maskelemiştir (Giles, 2013: 2). Söz konusu farkındalık artırıcı olayın sonrasında Rusya'da strateji belgelerinde de yer aldığı gibi ülke içi huzur ve istikrarı bozacak olan her türlü siber olaya karşı önlem alınması görevine karşılık, internet üzerinde devlet kontrolü de artmıştır. Yazar, internet ve dolayısıyla ifade özgürlüğü temelinde Rusya siber güvenlik politikasının böyle bir ortamda aldığı karışık halin, taslak aşamasında olan Siber Güvenlik Politikası belgesiyle açığa kavuşacağını beklemektedir. Bu anlayışa paralel olarak başka bir çalışmasında Giles (2012: 65), Londra Siber Konferansında Birleşik Krallık Dışişleri sekreteri ve arkadaşlarının sunumlarında siber uzayı "gelişim, yenilik, yeni fikir ve açıklamalara açık bir alan" olarak nitelerken, Rusya Bakanı Shchegolev'in bunu "ulusal hukuki düzenlemelere uygunluk ve özgürlüğün ülkenin güvenlik önceliklerini sağlamak kaydıyla" ifadeleriyle tamamladığının altını çizmektedir. Aslında bu bakış açısı, Rusya'nın siber güvenlik ve siber uzaya bakış açısını batı konsensüsünden en temel şekilde ayıran farklılığı da temsil etmektedir. Bu noktada Rusya'nın siber güvenliğe karşı tutumunu özetleyen iki anahtar kavram; "ulusal internet" ve "ülke egemenliğine karşı siber uzaydan gelecek herhangi bir tehdit potansiyeline karşı katı koruma" olarak nitelendirilebilecektir.

3.3. Çin'in Siber Güvenlik Politikası

Çin Halk Cumhuriyeti'nin kuruluşundan sonraki ilk 30 yıllık dönemdeki (1949-1978) dış politikası genel olarak ülkenin egemenliğini sürdürmek ve ülkeye karşı gelmesi muhtemel işgal niteliğindeki tehditlerin önlemek üzerinde gelişmiştir. Bilgi toplumuna geçişle birlikte gelişen yeni teknolojiler ve kaynak bağımlılıkları Çin açısından yeni sorunları da beraberinde getirmiştir. Her yıl önemli oranda artan bir ivmeyle 2010 yılında internet kullanıcı sayısı 457 milyona, 2017 yılında 731 milyona ulaşmış (Techinasia, 2017), ülkede internet olmadan iş yapmak olanaksız hale gelmiştir (Fei, 2011: 185). Artan internet, bilgi ve iletişim teknolojilerinin doğrultusunda ülkede, siber suçlar ve internet ağına yapılan siber saldırılar sonucunda ülkede 350.000'in üzerinde insan etkilenmiş (Symantec, 2018) ve siber güvenlik konusu Çin'in de öncelik verdiği bir konu haline gelmiştir.

Siber güvenliğin önemine, Çin'in algısı da diğer ülkelere benzer şekilde gelişmiştir. Devlet açısından siber güvenliği önemli kılan konular; siber eylemlerle ülkedeki kritik altyapı fonksiyonlarının zarara uğratılması, internetin, bilginin ve her türlü sanal dosyanın toplum düzenine, ekonomik gelişim sürecine, bireysel mülkiyet hakkına, askeri kapasitenin gelişimine zarar vermek amacıyla kullanılması gibi etmenlerdir (Swaine, 2013: 3). Bu tehditlere karşı Çin'in uyguladığı siber güvenlik politikası daha ulusal ve uluslararası platforma kısmen kapalı olması suretiyle batı ülkelerinden ayrılmaktadır. Gierow (2015) yaptığı çalışmada, Çin'in bir takım yönleriyle batı ülkelerinden ayrılan siber güvenlik

politikasının ana hatlarını belirtmiştir. Buna göre, Çin kendi bilişim teknolojisini üreterek sektördeki lider ülkelerin hegemonyasından uzak durmakta ve ulusal egemenliğini bu alanda da sürdürmek hedefindedir. Politikanın ana yaklaşımı bağımsız internet teknolojisi olmadan siber güvenliğin sağlanamayacağı yönündedir. Devlet yönetimi, uluslararası alanda ihracat yapan yerli teknoloji firmalarına kayda değer desteklerde bulunmaktadır. Söz konusu firmalar, küresel olarak kabul görmüş internet yazılımlarına ve teknoloji donanımlarına alternatif üretimlerde bulunmaktadır. Çin'in ürettiği akıllı telefonlar ve en önemlisi alternatif akıllı telefonlar için uygulama indirme mağazaları buna somut birer örnektir. Ülkede bu örneklerin küresel boyutta dış ülkeler tarafından üretilenleri için kullanım yasakları ve sansürler uygulanmaktadır. Bu engellemelerin nedeni ise ülke içi ve dışı bilgi sızdırılması ve espiyonajdır. Diğer yandan Çin'de korsan yazılımların kullanılma oranın yüksekliği ve bu nedenle yazılımların düzenli güncellemelerle daha güvenlikli hale getirilmemesinden dolayı hackerlik ve siber suç girişimleri artmakta, oluşan durum siber güvenliğe zarar vermektedir.

Çin'in siber güvenlikle bilgi ve iletişim teknolojilerine verdiği önemin geçmişi 20. yüzyılın sonlarına yani bu teknolojilerin ilk ortaya çıktığı zamanlara kadar dayanmaktadır. İlk olarak 1986 yılında ekonomik bilgilerin yönetimine dair küçük bir grup kurulmuştur. 2003 yılında ise siber güvenliğe dair ilk sivil belge olan Belge 27 yayınlanmıştır. Belge, kritik altyapıların korunmasına yönelik aktif bir savunma politikası oluşturmayı amaçlarken dinamik gözlemleme, gelişimi destekleme, devlet organları ve kurulan ekonomik bilgilerin yönetimi grubuyla iş birliği yaparak siber güvenlik politikalarını yönlendirmeyi amaçlamıştır (Raud, 2016: 11). Çin'in siber güvenlik alanında yaptığı kurumsal ve hukuki düzenlemelerin geçmişi 2014 yılının biraz öncesine dayanmaktadır. Çokuluslu bir denetim şirketi olan ve dünyada bu alanda en büyük dört şirketten (Big Four) biri olan KMPG'nin yayınladığı raporda (KMPG, 2016: 5) bu düzenleme ve gelişmeler kronolojik olarak sıralanmıştır. 2014 yılından önce yapılan düzenlemeler siber güvenliğe ve sistemsel altyapıların önemine odaklanılmış, devlet tarafından oluşturulan konsey bilgisayar bilgi güvenliği prosedürleri oluşturulmuş, Kamu Güvenliği Bakanlığı (Ministry of Public Security) bilgisayar virüslerine karşı savunma ve internet için birtakım standartlar geliştirmiştir. 2014 yılında, Çin devlet başkanı Xi Jinping başkanlığında siber güvenlik grubu kurulmuş ve yapılan çalışmalar o yılki hükümet raporunda yer almıştır. 2015 yılında Çin'in ulusal kongresi olan NPC'de (Standing Committee of the National People's Congress) kamuoyu yoklaması yapmak suretiyle halkın da görüşlerini göz önüne alarak Siber Güvenlik Kanunu tasarısını oluşturmuştur. Tasarı, Haziran 2016'da kongre tarafından ikinci kez tartışmaya açılırken, aynı yılın temmuz ayında tasarının son halini kuruluş resmi internet sitesinde yayınlanmış ve kamuoyunun ilgisine sunuluştur.

NPC'nin oluşturduğu kanun taslağı 1 Ocak 2017'de uygulanmak üzere yürürlüğe girmiş ve uygulanmaya başlamıştır. Kanun (COV, 2017) 7 bölüm ve 79 maddeden oluşmaktadır. 1. ve 2. bölümde genel prensipler ve hükümetin genel siber güvenlik stratejisi hakkında bilgi verilmektedir. 3. bölümde servis sağlayıcı ve ilgili kuruluşlarının sağlaması gereken siber güvenlik standartları Çok Boyutlu Ağ Güvenliği Koruması Şematiği altında verilmiştir. 4. bölümde bilgi güvenliği konuları; özel hayatın gizliliği, siber suçlar, zararlı yazılımlar, kanunsuz bilgi yayılımı gibi odak noktalar üzerinden ele alınmıştır. 5. bölümde ağların izlenmesi ve acil durumlarda tehlikelere karşı yapılacak hamleler açıklanmıştır. 6. bölümde ağ güvenliği kurallarının ihlal edilmesi durumunda uygulanacak yaptırımlar belirtilirken, son bölümde tanımlar ve diğer ek bilgiler yer almıştır.

Çin Halk Cumhuriyeti'nin siber güvenlik konusunda geliştirdiği politikalar güçlü ulusal güvenlik standartlarının oluşturulması dışında, diğer ülkelerin siber güvenliklerine risk ve tehdit oluşturan bir çizgi de izlemektedir. Bu saldırılardan muzdarip olan ülkeler ABD, Tayvan ve Almanya olarak örnek gösterilebilecek olsa da bu saldırılardan dolaylı olarak etkilenen ülke sayısı 2009 yılında 103'ü bulmuştur (Spade, 2012: 3-4). Özellikle ABD kongresinde dile getirilen konulardan birisi olarak Çin'in siber devlet güçlerinin kendi milli firmalarına rekabet üstünlüğü sağlamak üzere ABD firmalarının teknoloji bilgilerini çalmaya yönelik bir çok saldırıda bulunduğu vurgulanırken, Çin tarafı bunu "hırsızlığın durdurulması için ağlayan bir hırsız" olarak nitelemektedir (Lindsay, 2015: 7-8). ABD ve Çin arasındaki söz konusu atışma ve suçlamaların yanında, literatürde iki ülke arasında yapılan siber güvenlik anlaşması önemli bir yer tutmaktadır.

Çin ile ABD arasındaki dış ilişkiler Çin Halk Cumhuriyeti'nin kurulmasından bu yana çeşitli alanlarda fikir ayrılığı, çatışma ve stratejik güvensizlik çizgisinde ilerlemiştir. Son yıllarda bu iki ülkenin en fazla çatışma yaşadığı alanlardan biri de siber uzay konusu olmuştur. Çatışma ve fikir ayrılıklarını yumuşatmak üzere iki ülke arasında görüşmeler 2013 yılında başlamış olsa da 2014 yılında ABD'nin Çinli bazı askeri görevlilerin casusluk faaliyetlerinde bulunduğunu iddia etmesiyle aniden kesilmiştir (Harold, vd., 2016, iii). 2015 yılında ise Çin devlet başkanı Xi Jinping'in Beyaz Saray'a yaptığı ziyarette, ABD başkanı Obama ve Jinping arasında bir siber mutabakat gerçekleştirilmiştir. Buna göre iki ülke; zararlı siber eylemlere karşı bilgi ve yardım ihtiyacında işbirliğinde bulunma, siber hırsızlık ve entelektüel sermayeye zarar verecek siber kaçakçılıklardan kaçınma, ülkelerin siber politikalarında uluslararası standartlara uyum gösterme, siber suçlarla mücadelede iki ülke arasında çok gelişmiş bir diyalog mekanizması kurulması konularında fikir birliğine varmıştır (Rollins, 2015).

Lieberthal ve Singer (2012: vi-x) çalışmalarında, ABD ve Çin arasında siber politikalardaki uyuşmazlıkları çeşitli konu başlıkları halinde sıralamışlardır. Yazarlara göre uyuşmazlıklar şu başlıklar altında toplanabilir: Farklılaşan siber

terminolojiye bağlı olarak iki ülkenin kullandığı kavramların içlerinin farklı doldurulması (siber saldırı, bilgi saldırı gibi), siber eylemlerin asıl amaçlarının belirsizliği, savunma odaklı bekleyiştense önce saldıran olmanın avantajlı olması algısı, siber olaylardaki zaman planlaması karmaşıklığı (saldırı ya da savunma için harcanan ve beklenen doğru zaman), eylemlerin yerelleşmesi (tek bir merkezden yönetilmemesi).

Sonuç olarak, ABD ve diğer ülkelerin Çin'i siber güvenlik konusunda güçlü bir tehdit olarak gördüğü söylenebilir. Öte yandan Çin de dünya genelindeki internet ve bilgisayar teknolojisi pazarında en büyük payın ABD'de olması nedeniyle, siber güvenlik konusunda ABD lehine büyük bir eşitsizliğin söz konusu olduğunu savunmaktadır.

SONUÇ

ABD, Rusya ve Çin'in siber güvenlik politikalarına ilişkin resmi politika belgelerinin incelenmesiyle ulaşılan sonuçlar şu şekilde özetlenebilir:

ABD'nin siber güvenliğe yönelik farkındalığı ağırlıklı olarak 2000'li yılların başlarında oluşmuştur. Somut adımların daha çok son yıllarda atıldığı ve bu adımların ağırlıklı olarak siber güvenliği sağlamak üzere devlet kurumlarının kapasitelerinin geliştirilmesine ve olası siber tehditlere karşı ülkenin savunma mekanizmalarının güçlendirilmesine odaklandığı belirlenmiştir. Belgelerdeki politika önerilerinin, karşı saldırı ve siber bağımsızlık üzerine odaklandığı görülmüştür.

Rusya'da ise incelenen belgeler ışığında; ülkenin siber güvenlik politikası oluşturma sürecinin savunmacı anlayışla oluşturulduğu sonucuna ulaşılmıştır. Rusya, savunma mekanizmalarının kurulmasında, müttefik ülkelerle yapılacak işbirliklerine önem vermektedir. Yönetimin siber güvenlik politikası öncelikli olarak savunma boyutuna odaklanmaktadır. Diğer yandan konu ile ilgili literatürde altı çizilen bir nokta da ülkenin "saldırıya karşı saldırı" politikasını ön plana çıkarmış olmasıdır. Savunma ve saldırı kriterleri kadar ağırlıklı olmamakla birlikte ülkenin "kapasite"ye yönelik olarak eldeki bilgi ve iletişim altyapılarının güçlendirilmesine ve milli mekanizmaların önemine atıf yapan politikaları önemsediği kanaatine varılmıştır.

Çin'in siber güvenlik politikasına bakıldığında ise, diğer ülkelerden farklı olarak, kendi milli siber ağlarını kullanarak ve uluslararası platformlarda yaygın şekilde yer edinmiş birçok ağı kullanmayı yasaklayarak ya da sınırlandırarak oldukça güçlü bir savunma mekanizması geliştirdiği görülmektedir. Bu yönde izlenen bir politika, somut savunma mekanizmaları kurmasa da ülkeyi siber güvenlik konusunda batı ülkelerine nazaran daha güvenlikli bir hale getirmektedir. Bu durum diğer ülkelerden farklı olarak Çin'in "bağımsızlık" kriteri ve politikası

üzerinde yoğunlaştığını göstermektedir. Dünya çapında yaygın olarak kullanılan siber yazılım ve donanımların Çin tarafından engellenmesi, yerlerine milli alternatiflerin üretilmesi ve kullanılması oldukça önemli adımdır. Buna ek olarak, hukuki düzenlemelerle servis sağlayıcı ve operatörlere yüklenen güvenlik önlemi alma zorunluluğu ve kritik altyapılara yönelik olarak oluşturulan ilave güvenlik stratejileri, bu politikanın temelini oluşturmaktadır. Bunun yanında, literatürde, Çin'in güçlü bir saldırı politikası izleyerek ABD'den teknoloji istihbaratı almaya yönelik siber saldırılarda bulunduğu da iddia edilmektedir. Çin'in, savunma, saldırı ve bağımsızlık kriterlerine yönelik politikalar üzerine odaklandığı görülmektedir. İncelenen belge ve çalışmalara göre, Çin'in siber güvenlik kapasitesinin geliştirilmesine yönelik politika önermelerinin, genel olarak güvenlik standartlarının geliştirilmesi odaklı olduğu söylenebilir. İncelenen belgelerde, siber güvenlikle ilgili kurum kapasitelerinin geliştirilmesine odaklı politika önerilerine direkt olarak rastlanmamakla birlikte, kapasite boyutunun, Çin'in "milli siber güvenlik altyapısı" politikası içerisinde ve yüksek önemde olduğu gözden kaçırılmamalıdır.

Ulaşılan bu sonuçlardan hareketle; ABD, Rusya ve Çin'in siber güvenlik politikaları; "savunma", "saldırı", "bağımsızlık" ve "kapasite" boyutları açısından aşağıdaki tabloda özetlenmeye çalışılmıştır. Tabloda ele alınan her bir boyut, ülkeler bazında Güçlü (G), Orta (O) ve Zayıf (Z) şeklinde derecelendirilmiştir.

Tablo 4: Siber Güvenlik Politikası Öncelikleri Açısından Karşılaştırmalı Analiz

Ülke	Savunma			Saldırı			Bağımsızlık			Kapasite		
	G	O	Z	G	O	Z	G	O	Z	G	O	Z
ABD	X				X			X		X		
Rusya	X			X				X			X	
Çin	X			X			X			X		

Tablo 4'te sunulan üç ülkenin siber güvenlik politikalarının öncelikleri ve bunların dereceleri, incelenen resmi belgelerde yer alan politika önerilerinden yola çıkılarak belirlenmiştir. Dolayısıyla karşılaştırma tablosu, söz konusu ülkelerin belirlenen boyutlarda "somut olarak sahip oldukları gücü" göstermemektedir. Bunun yerine, bu ülkelerin ulusal siber güvenlik stratejileri, ilgili politika belgeleri ve literatür bazında "hangi siber güvenlik boyutlarına daha çok odaklandıklarını" göstermektedir.

Sonuç olarak bu çalışmadan elde edilen bulgular genel olarak değerlendirildiğinde, Türkiye'de, siber güvenlik alanında yapılacak geliştirici ve yenilikçi çalışmalar için henüz çok geç kalınmadığı düşünülmektedir. Hızlı yapısal reformlar ve yerinde politikalarla, siber güvenlik alanında önemli bir atılım gerçekleştirilmesi mümkün olabilecektir. Yukarıdaki karşılaştırma tablosunda sunulan ve "siber güvenlik politikasının öncelikleri"ni oluşturduğu düşünülen dört boyutun tamamında (savunma, saldırı, bağımsızlık ve kapasite) Türkiye'nin kısa sürede ciddi adımlar atması mümkündür. Zira süper güç olarak nitelendirilen ABD, Rusya ve Çin'deki siber güvenlik politikası adımlarının da ağırlıklı olarak son 20 yılda atıldığı göz ardı edilmemelidir. Ulusal Güvenlik Politikasının artık ayrılmaz ve kritik bir parçası haline gelen Siber Güvenlik Politikasının Türkiye'de dört boyutu itibariyle gözden geçirilerek ele alınması ve ileriye dönük kapsamlı bir siber güvenlik stratejisinin vakit geçirilmeden oluşturulması son derece önemlidir.

KAYNAKÇA

Bello, F. (2011). Public Policy Implication on National Security. Erişim tarihi: 08.04.2017, http://nials-nigeria.org/pub/lFATIMABELLO.pdfn

Breene, K. (2016). There Are Now Five Countries Considered to be Cyberwar Superpowers. Erişim tarihi: 27.03.2017, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

Buchanan, J. M., (1984). Politics without Romance: A Sketch of Positive Public Choice Theory and Its Normative Implications. Ed: J.M. Bunchanan ve R. D. Tollison. The Theory of PublicChoice II. USA: The University of Michigan Press.

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

Clark, D., Berson, T., and Lin, H. S., (2014). At the Nexus of Cybersecurity and Public Policy. Computer Science and Telecommunications Board. National Research Council, Washington DC: The National Academies Press.

Clarke, R. A. ve Robert, K. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins.

COV (2017). China Passes New Cybersecurity Law. Erişim tarihi: 27.07.2017, https://www.cov.com/-/media/files/corporate/publications/2016/11/china_passes_new_cybersecurity_law.pdf

DOD (2011). Department of Defense Strategy for Operating in Cyberspace. Department of Defense. Erişim tarihi: 17.04.2017, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

DOD (2012). Military and Security Developments Involving the Democratic People's Republic of Korea. USA: Department of Defense.

DOD (2013). DoD Strategy for Defending Networks, Systems, and Data. Department of Defense, Erişim tarihi: 18.04.2017, http://iac.dtic.mil/csiac/download/DDNSD_Public_Releasable_11132014.pdf

DOD (2015). The DOD Cyber Strategy. Washington: The Department of Defense. Erişim tarihi: 19.07.2017, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Doyle, R. B. (2007). The U.S. National Security Strategy: Policy, Process, Problems, Public Administration Review, 67(4), 624-629.

Erickson, J. (2008). Hacking: The Art of Exploitation. San Francisco: No Starch Press.

Fei, G. (2011). China's Cybersecurity Challenges and Foreign Policy. Georgetown Journal of International Affairs, 2011, 185-190.

GCHQ (2012). 10 Steps to Cyber Security. UK: Crown.

Gierow, H. J. (2015). Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses. Mercator Institute for China Studies, (22), 1-10.

Giles, K. (2012). Russia's Public Stance on Cyberspace Issues. 4th International Conference on Cyber Conflict, Tailinn: NATO CCD COE Publications.

Giles, K. (2013). Internet Use and Cyber Security in Russia. Russian Analytical Digest No: 134, Erişim tarihi: 24.04.2017, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RAD-134-2-4.pdf

Gohlert, E. W. (1974). National Security Policy Formation in Comparative Perspective. Policy Studies Journal, 3(2), 174-177.

Harold, S. W., Libicki, M. C. ve Cevallos, A. S. (2016). Getting to Yes with China in Cyberspace. CA: RAND Corporation.

ISS (2017). Basic Principles for Sate Policy of the Russian Federation in the Field of International Information Security to 2020. Erişim tarihi: 23.04.2017, https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf

ITU (2015). Global Cybersecurity Index (GCI) 2015. Erişim tarihi: 25.06.2019, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

ITU (2017). Global Cybersecurity Index (GCI) 2017. Erişim tarihi: 25.06.2019, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

ITU (2018). Global Cybersecurity Index (GCI) 2018. Erişim tarihi: 25.06.2019, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

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

Kay, S. (2004). Globalization, Power, and Security. Security Dialogue, 35(1), 9–25.

Kirshner, J. (2006). Globalization and National Security. NY: Routledge.

KMPG (2016). Cyber Security in China. Management Consulting. China: KMPG.

Korff, D. (t.y.). Cyber Security Definitions. UK: Associate of the Oxford Martin School of the University of Oxford's Global Cybersecurity Capacity Centre.

Kshetri, N. (2016). The Quest to Cyber Superiority. Switzerland: Springer.

Lantis, S. J. (2002). Strategic Culture and National Security Policy. International Studies Review, 4(3), 87-113.

Lehman, J. ve Willett, T. D. (1986). National Security and Industrial Policy: The Need For a Public Choice Perspective. Contemporary Policy Issues, (7), 36-47.

Lieberthal, K. ve Singer, P. W. (2012). Cybersecurity and U.S. - China Relations. Brookings.

Lindsay, J. R. (2015). The Impact of China on Cybersecurity. International Security, 39(3), 7-47.

Lu, M. (2014). Types of Cyber Attacks. Trustworthy Cyber Infrastructure For The Power Grid. Erişim tarihi: 18.03.2017, https://tcipg.org/sites/default/files/ rgroup/tcipg-reading-group-fall_2014_09-

12.pdf

Medvedev, S. A. (2015). Offense-Defense Theory Analysis of Russian Cyber Capability. Masters' Thesis, California: Naval Postgraduate School.

O'Shea, K. (2003). Cyber Attack Investigative Tools and Technologies. İç. HTCIA, Institute for Security Technology Studies, Hanover, NH: Dartmouth College.

Raud, M. (2016). China and Cyber: Attitudes, Strategies, Organisation. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

RNS (2015). Russian National Security Strategy. December 2015 – Full-text Translation. Erişim tarihi: 21.04.2017, http://www.ieee.es/Galerias/fichero/ OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

Rollins, J. W. (2015). U.S.–China Cyber Agreement. Erişim tarihi: 28.04.2017, https://fas.org/sgp/crs/row/IN10376.pdf

RSG (t.y.). Концепция стратегии кибербезопасности Российской федерации (Rusya Federasyonu Siber Güvenlik Stratejisi Kavramı) Erişim tarihi: 21.04.2017, http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

Spade, C. J. M. (2012). Information As Power: China's Cyber Power and American's National Security. U.S. Army War College.

Swaine, M. D. (2013). Chinese Views on Cybersecurity in Foreign Relations. China Leadership Monitor, 1-27.

Symantec (2018). 2017 Norton Cyber Security Insights Report Global Results. Erişim tarihi: 02.07.2019, https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

Techinasia. (2017). China Now Has 731 Million Internet Users, 95% Access From Their Phones. Erişim tarihi: 27.04.2017, https://www.techinasia.com/china-731-million-internet-users-end-2016

WH (2003). The National Strategy to Secure Cyberspace. Washington: The White House. Erişim tarihi: 17.04.2017, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Yue, O. (2003). Cyber Security. Technology in Society, (25): 565–569.