KÜRESEL GÜÇLERİN ULUSAL SİBER GÜVENLİK STRATEJİLERİ: ABD ÖRNEĞİ

Ayşegül GÜNEŞ*

Özet

Teknolojinin gelişmesiyle birlikte, değişen ve gelişen dünya düzeninde birçok yenilikler meydana gelmiş ve çok sayıda ülke, bu yeniliklere ayak uydurmada zorluklar yaşamıştır. Özellikle 21. yüzyıl bu gelişmenin belirleyici unsuru olmuştur. Peki, neden 21.yy belirleyici olmuştur? Çünkü hem internet ağının yaygınlık göstermiş olması hem de bu yüzyılın internet çağı olarak ilan edilmesi, bu belirleyici unsurun odak noktasını oluşturmuştur. İnternet ağının yaygınlık göstermiş olması, dünya çemberini daraltmış ve neredeyse küçük bir mahalle haline getirmiştir. Gelişen ve değişen dünya sisteminde üçüncü dünya devletleri geride kalmıştır. Bunun temel sebepleri arasında ekonomik eşitsizlikler, siyasal kısıtlamalar ve en önemlisinin de teknolojik yetersizliklerin olduğu görülmektedir. Bu tür ülkelerin küreselleşmeye ayak uyduramadıkları ve küresel birer güç olamadıklarının da bir göstergesidir. Teknolojik bakımdan gelişmiş ve gelişmekte olan ülkelerin küreselleşmeye yön verdikleri ve bu doğrultuda küresel birer güç olarak ortaya çıktıkları da görülmektedir. Çin Halk Cumhuriyeti, Rusya Federasyonu, Avrupa devletleri ve ABD gibi devletlerin teknolojik olarak önemli ilerlemeler kat etmeleri, beraberinde rekabet ortamını da getirmiştir. Bu rekabet, özellikle 21. yüzyıl dünyasında, tehditlere yol açmış ve güvenlik olgusunun tekrar gözden geçirilmesine sebebiyet vermiştir. Bu tehdit saldırılarına ve güvensiz ortamlara karşı devletler, ulusal siber güvenlik stratejileri geliştirmiştir. Bu devletlerden biri de, küresel bir güç olarak ortaya çıkmış olan ABD'dir. Bu bağlamda makale, ABD'nin ulusal güvenliğini korumak amacıyla nasıl bir strateji geliştirdiğini ve ne tür önlemler aldığını ele almakla birlikte, diğer devletlere karşı nasıl bir strateji geliştirdiğini de irdelemiştir.

Anahtar kelimeler: Siber Güvenlik, Küresel Güçler, Ulusal Güvenlik, ABD.

NATIONAL CYBER SECURITY STRATEGIES OF GLOBAL FORCES: US CASE

Abstract

With the development of technology, many innovations have taken place in the changing and evolving world order, and many countries have had difficulties in keeping up with these innovations. In particular, the 21st century has been the determining factor in this

* Department of International Relations, Selcuk University

development. So why was the 21st century decisive? Because the fact that the internet network is widespread and the announcement of this century as the age of internet has been the focus of this decisive factor. The fact that the Internet network is widespread has narrowed the world circle and made it almost a small neighborhood. In the developing and changing world system, the third world states remained behind. The main reasons for this are economic inequalities, political constraints, and the most important ones are technological deficiencies. It is also an indication that such countries cannot keep pace with globalization and cannot be a global force. It can be seen that technologically advanced and developing countries have led to globalization and emerged as a global power in this direction. The technological advancement of states such as the People's Republic of China, the Russian Federation, European states and the USA has brought about a competitive environment. This competition, especially in the 21st century, has led to threats and has led to the revision of the security phenomenon. Against these threat attacks and insecure environments, states have developed national cyber security strategies. One of these states is the United States, which has emerged as a global power. In this context, the article explores how the US has developed a strategy to protect its national security and what measures it has taken, and how it has developed a strategy against other states.

Key words: Cyber Security, Global Powers, National Security, USA.

Giriş

Bilgi ve iletişim teknolojileri, toplumun ve ekonominin ayrılmaz birer bileşenleri olmasının yanı sıra, siyaset odağının da ayrılmaz bir parçası olmuştur. Bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte, değişen ve dönüşen dünya sisteminde önemli ilerlemeler oluşsa da, bununla beraber, tehdit ve güvensizleşme ortamı da oluşmuştur. Güvenlik, insanoğlunun saldırı ve tehditlere karşılık sığınacağı en önemli kaynaktır. Güvenlik terimi insanlıkla beraber var olan ve insanlığın bulunduğu her ortam ve çağda önemini hissettiren bir terim olmuştur. Ayrıca insanoğlunun varlığından bu yana da, sürekli değişim geçirmiştir. Güvenlik teriminin ilgili olduğu alanların başında, bireysel, ulusal ve uluslararası boyutlar gelmektedir. Bu nedenle güvenlik her alanda insanoğlunun karşısına çıkmaktadır (Bayraktar, 2015: 23-25).

Gelişen ve günlük hayatın ayrılmaz bir parçası haline gelen bilişim teknolojileri sayesinde güvenlik terimi, bireysel, ulusal ve uluslararası boyutlara ek olarak siber uzay ve güvenlik boyutlarıyla da ilintili olmaktadır. Hatta bu karşılaşma o kadar etkili ve kapsamlı olmaktadır

ki, siber güvenlik alanı, çoğunlukla bireysel ve ulusal sınırları aşmakta ve uluslararası bir boyut kazanmaktadır. Bu nedenle siber güvenlik terimi, sadece bireysel ya da ulusal tedbirlerin tanımlanması, uygulanması ve önlenmesi ile sınırlı kalmamakta olup, küresel bir alanla iç içe olmaktadır (Daban, 2016: 80-81).

Dünya üzerinde devletlerarası meydana gelebilecek herhangi bir saldırı veya sorun karşısında başvurulacak temel örgüt, Birleşmiş Milletler kurumudur. BM Sözleşmesi'nin 51. Maddesinde; "Bu Antlaşma'nın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi, uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez. Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve Konsey'in işbu Antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez." Şeklinde olup, herhangi bir çatışma anında ilk yapılması gerekeni ifade etmektedir (Gündüz, 2015: 118).

BM'nin bu Antlaşma metni incelendiğinde, ifadede, siber saldırı ile ilgili herhangi bir bilgi verilmediği görülecektir. Siber güvenlik teriminin gelişmesi, siber tehditlerin etkileri ile kapsamlarının genişlemesi ve sınırlarüstü bir savunma zaafiyeti haline gelmesi sonucu, siber savaş hukuku üzerine çalışılmasını öngörmüştür. Bunların yanı sıra, gelişen bilim ve teknoloji, zamanla, siber saldırı, siber sömürü, siber tehdit, siber müdahale, siber çatışma ve siber şiddet gibi birçok alanlarda etkisini göstermiş ve devletler, bu alanlar üzerinde önlem ve tedbirler almaya çalışmıştır. Bu durum ise, hem rekabeti hem de olası bir güvenliği ortaya çıkartmıştır. 20. yüzyılın ortalarından itibaren, bilgisayarların ortaya çıkması, ardından internet denilen ağın gelişmesi ve 21. yüzyıl dünyasındaki yerlerini merkez olarak alması, tüm dünya devletlerini endişelendirmiştir. Çünkü doğrudan müdahale yönteminin yerini, internet ağıyla, devletlerin kurum ve kuruluşlarına siber sızma yönetimi almıştır (Ulaş, 2016: 174-175).

21. yüzyılın önemli küresel güçleri, başta ABD olmak üzere, Rusya ve Çin başı çekmektedir. Avrupa devletlerinin de bu güç dengelerinde yer aldıkları söylenebilir. Rusya'da bulunan ve dünyanın en büyük hacker okulundan sorumlu olan Özel İletişim ve Bilişim Servisi (FAPSI), siber alanında önemli gelişmelere imza atmıştır. Okulda siber savaşçılar yetiştirilmektedir.

FAPSI, aynı zamanda siber uzayda istihbarat toplamakla da görevlidir. ABD'deki Ulusal Güvenlik Ajansı (NSA) ile FAPSI'nin ortak yönleri burada ortaya çıkmaktadır. Kod kırma, telefon dinleme, zararlı yazılım yazma gibi çalışmaları da üstlenmektedir (O'Connel, 2002: 904-905).

Çin, ülkesinde üretilen korsan ABD markası olan Cisco'nun önünü kesti ve kendi markasını kurmuştur. Ayrıca 1990'lı yıllardan beri sistematik bir şekilde siber savaşla ilgili projeler geliştirmekte olan Çin, bu bağlamda, ülkenin internet alt yapısının korumalığını sağlamlaştırma stratejilerini de geliştirmektedir. Özellikle ABD menşeli yazılım ve donanımlardan uzak kalarak kendi yazılım ve donanımlarını geliştirmektedir. ABD'nin çalışmalarına bakıldığında, 1995 yılında, Ulusal Savunma Üniversitesi, ilk siber savaşçılarını mezun ettikleri görülmüştür. Birleşik Devletleri Siber Komutanlığı, resmi olarak 21 Mayıs 2010 tarihinde kurulmuştur. Faaliyetlerine ise, aynı yılda başlamıştır. Bu gelişmeler doğrultusunda ABD'nin özellikle Rusya ve Çin'e karşı siber politikalar geliştirdiği, bunların yanı sıra, üniversitelerde ve komutanlıklarda sibere önemli bir alan açarak geliştirmekle, dünyada siber alanında öncü olmayı hedeflediği söylenebilir. Bu gelişmelerle birlikte, diğer küresel güçlerden gelecek olası saldırı ve tehditlere karşı, tedbir ve önlemler alarak, ulusal siber güvenlik stratejilerine de önem verdiği görülmüştür. Tüm bu çabalar, değişen ve gelişen dünyada güvenlik kavramının kılıf değiştirmeye başlaması ve güvenliğin tehditle karşı karşıya kalınmasıyla oluştuğu da görülmektedir (Libicki, 1995: 7-8).

1. Değişen Güvenlik Kavramı ve Siber Algısı

Güvenlik kavramı, uluslararası sistemde yer alan tüm aktörler için önemli olan, bu aktörler arasında farklı anlamlarla tanımlanan fakat özünde her bir aktör için yaşamsal gereklilik olarak görülen bir kavramdır. Bu sebeple güvenlik kavramını, varlığı koruyan ve muhafaza etme amacı güden davranışlar olarak nitelemek mümkündür (Dedeoğlu, 2008, s.21).

İnsanlık tarihinin başlangıcından günümüze değin geçen sürede birçok aşamadan geçen güvenlik kavramı bugün sadece askeri güç kullanılarak engellenemeyecek kadar karmaşık, çok boyutlu bir hale bürünmüştür. Stabilizasyonun en önemli unsur olarak görülebileceği bu halde kişisel güvenliğe zarar verecek her şey güvenlik tehdidi oluşturabilmektedir (Bıçakcı, 2013, s.10).

Türk Dil Kurumu sözlüğünde *"toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet*" şeklinde açıklanan güvenlik, insanlık

tarihinin başlamasıyla ortaya çıkmış, günümüze kadar önemini korumuş ve yüzyıllar boyunca hayatın her alanında etkisini sürekli artırmış bir kavramdır (Güvenlik (t.y.), (http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c433e42013c60.29375572 10.01.2019 tarihinde erişildi).

Güvenliğin kavramsal çözümlemesi 1952 yılında Wolfers'in yaptığı çalışma ile başlaış ve ardından güvenlik çalışmaları uluslararası ilişkiler disiplininin önemli bir alt dalı olmuştur.(Baldwin, 2003) Wolfers çalışmasında güvenlik kavramını öznel açıdan *"kazanılmış değerlere yönelik tehdidin bulunması"* nesnel açıdan ise *"bu değerlere saldırılacağına dair korkunun bulunmaması"* şeklinde açıklamıştır (Baldwin, 2003).

Amerika Birleşik Devletleri ve Sovyet Sosyalist Cumhuriyetler Birliği arasında 1955-1965 yıllarında meydana gelen nükleer silahlanmayla birlikte sivil danışmanlara gereksinim duyulması ve bu bağlamda pek çok akademisyenin güvenlik konusuna yönelmesiyle bu dönem uluslararası güvenlik çalışmalarının "Altın Çağı" şeklinde nitelendiren Walt bu çalışmalarını, *"askeri kuvvetlerin kontrolü, kullanımı ve tehdit çalışmaları"* şeklinde nitelendirmiştir (Walt, 2003).

Güvenlik kavramının açıklamalarında başvurulan en önemli kavram tehdit unsurudur. Bir güvenlik olgusundan söz edebilmek ancak varlığın devam ettirilebilmesi açısından bir tehdidin bulunmasıyla mümkündür. Bu tehdit birden fazla ve içsel ya da dışsal olabilir. Tehdit unsurunun varlığından emin olmanın yanı sıra tehdidin varlığına yönelik algılamaların olması da yeterlidir.(Dedeoğlu, 2008, s.22)

Güvenlik algısı uluslararası ilişkiler disiplini içerisinde yer alan aktörlerin hedefleri, yetenekleri, disiplin içerisindeki ağırlıkları gibi parametrelere göre farklılık göstermektedir. Aktörlerin uluslararası alanda tehdit algılaması farklı olmakta, bu alanda meydana gelen olayları karşılama ve olumsuz olgulardan etkilenme düzeyleri de birbirinden farklı güvenlik tanımlamalarını ortaya çıkarmaktadır.(Dedeoğlu, 2008, s.24)

Zaman içerisinde gelişen olaylar ve olgular güvenlik tanımını geliştirip zenginleştirdiği gibi yol ve yöntemlerini de değiştirmiştir. Güvenlik kavramına yönelik tanımlamaların daha iyi anlaşılabilmesi adına öncelikle kavramın tarihsel gelişimi incelendikten sonra Soğuk Savaş dönemi boyunca algılanan güvenlik tanımının bu dönem sonunda ulaştığı konum üzerine yoğunlışacaktır.(Bayraktar, 2015, s.28)

Bu bağlamda verilebilecek ilk örnek Sümerlerin M.Ö 3000'li yıllarda birbirlerini tehdit olarak görüp güç ve güvenlik arayışına girmeleri ve diğerlerini egemenlik altına alma girişimleri bahsi geçen dönem için güvenlik ve tehdit unsurları arasındaki yakın ilişkiyi açıklamaktadır.(Dedeoğlu, 2008, s.27)

Mısır, Hitit ve Asur medeniyetleri arasında yaşanan toprak paylaşım kavgaları güvenlik kaygısının ilk resmi şeklidir. Hititler, Mısır ve Asur'u egemenliklerini sürdürme konusunda engel olarak görmüşlerdir. Mısır'ın hızla güçlenmesi karşısında Suriye'de bulunan küçük krallıkları kendi tarafına çekmek isteyen Hititler, zorlayıcı tavırlar sergilemişlerdir. Bu zorlamalar sonucunda Suriye krallıklarının Mısır ile ittifak yapması üzerine Hititler ve Mısır arasında geçen mücadele olan Kadeş Savaşı yaşanmıştır.(Arıboğan, 2007, s.48-50)
Tehdit ve güvenlik arasındaki yakın ilişkiyi açıklayan bir diğer örnek ise Antik Yunan döneminde, Pers İmparatorluğu'nun profesyonel ve hemen harekete hazır olabilecek ordusunun Yunan şehir devletlerince tehdit olarak algılanması ve Attik-Delos Deniz Birliği'ni kurmalarıdır.(Dedeoğlu, 2008, s.28)

Bahsi geçen dönemde kurulan ilişkilerdeki güvenlik algısının değerlendirilmesi yine o döneme göre yapılmalıdır. Bu konuda verilebilecek örneklerden birisi Thucydides'in "Peloponez Savaşları" isimli kitabında Spartalılar ve Atinalılar arasında meydana gelen savaşın Atina'nın güçlenmesi karşısında Spartalılarda oluşan korkudan yola çıkarak tehdit ve güvenlik arasındaki yakın ilişkiden bahsetmiştir.(Eralp,1996,s.34)

14. ve 15. yy'da Avrupa'da yaşanan Yüzyıl Savaşları, Haçlı Seferleri gibi olaylar ile 16. yy'da ortaya çıkan reformlar ve 17. yy'da bulunan bazı önemli buluşlar güvenlik algısında birtakım değişiklikler meydana getirmiştir. İdealist yaklaşımın baş gösterdiği 18.yy'da ise bu yaklaşımın gereği olarak savaş reddedilip barış savunulmuştur. Bu bağlamda savunulan düşünce; dünya üzerinde yer alan bütün devletler barış ortamını oluşturup, bünyelerinde tehdit unsurlarını barındırmazlarsa güvenlik ihtiyacına gereksinim kalmayacağı yönündedir.(Duygu,2015,http://www.tuicakademi.org/uluslararasi-sistem-acisindan-guvenlik-ve-guvenlik-algisinda-yasanan-degismeler/ 20.12.2018 tarihinde erişildi.)

19. ve 20. yy'da ise sanayileşmenin ortaya çıkardığı pazar arayışı ve güçlü olan devletlerin kapasitelerini daha da artırmaya yönelik çalışmaları iki kere dünya savaşının yaşanmasına sebebiyet vermiştir. Söz konusu savaşların tekrar yaşanmaması adına güvenlik önlemleri

alınmaya çalışılmıştır. Bu önlemlerden biri olan Milletler Cemiyeti yeni bir savaşın meydana gelmesine engel olamamıştır. Önlemlerden bir diğeri ise Birleşmiş Milletler'in kurulmasıdır. Birleşmiş Milletler Güvenlik Konseyi uluslararası sistemde barış ve güvenliğin sürdürülmesine engel olan olaylarla ilgilenmektedir (Duygu, 2015, http://www.tuicakademi.org/uluslararasi-sistem-acisindan-guvenlik-ve-guvenlik-algisinda-yasanan-degismeler/ 20.12.2018 tarihinde erişildi.).

Soğuk Savaş döneminde ise güvenlik kavramının temel unsurları siyasi, ekonomik ve askeridir. İki büyük güç arasında yaşanan bu dönemde güvenliğin temelinde çevreleme ve caydırıcılık anlayışları yer almıştır. Soğuk Savaş dönemi güvenlik kavramının tarihsel gelişimi açısından bir dönüm noktasını ifade eder. Bu dönemde, devletlerin güvenliğinden daha çok bireyin güvenliğine vurgu yapılmıştır (Duygu,2015, http://www.tuicakademi.org/uluslararasi-sistem-acisindan-guvenlik-ve-guvenlik-algisinda-yasanan-degismeler/ 20.12. 2018 tarihinde erişildi.)

Soğuk Savaş'ın bitmesiyle beraber ülkelerin tehdit anlayışında değişimler meydana gelmiştir. Söz konusu değişimler, uluslararası siyasi alanda değişik boyutlarda yeni oyuncuların ve yeni dengelerin oluşması şeklinde yaşanırken, bu değişimin en kritik ve önemlisi tehdit unsurunda gerçekleşen genişleme ile güvenlik algısında meydana gelmiştir. Söz konusu dönem sonrasında ortaya çıkan yeni alanda milli güvenliğe yönelik tehditler değişmiş; etnik ve dini çatışmalar, terörizm, Kitle İmha Silahları'nın kullanımının artması, siber terörizm gibi yeni tehdit değişkenleri meydana gelmiştir.(Turgut, 2003).

2. Siber Güvenlik ve Ulusal Güvenlik Kavramları

Siber uzay içerisinde yer alan bilişim sistemlerini tehdit ve saldırılardan korumak, bu alan içerisinde bulunan bilgilerin gizliliğini sürdürmek, söz konusu saldırı ve tehditlerin niteliklerini belirlemek, bunlara karşı yaptırımlar oluşturmak hedefiyle geliştirilen ulusal ve uluslararası hukuk ile insan haklarına mutabık her çeşit tedbir ve oluşumları siber güvenlik olarak tanımlamak mümkündür. (Kara, 2013, s.5-6)

Siber Güvenlik, siber ortam ve bu ortamda bulunan kullanıcıların variyetlerini koruma altına almak hedefiyle kullanılabilecek; araç ve yöntemler ile güvenlik anlayış ve tedbirleri, risk yönetimi, ilkeleri ve teknolojilerin toplanmasıyla meydana gelir.(Şentürk, 2012, s.112)

Milli güvenliğin bir kolu olarak görülen siber güvenlik uygulamalarının kaynağı erişilebilirlik, gizlilik ve bütünlük üzerinedir. Erişilebilirlik; kişilerin istedikleri zaman bilgiyi elde edebilmesini, gizlilik; bilgiye yalnız yetkili kişiler tarafından erişilebilmesini, bütünlük ise söz konusu bilginin herhangi bir değişime uğramamış, bozulmamış olması anlamına gelmektedir. Sayılan bu öğelerden erişilebilirlik düzeyinin yükselmesiyle gizlilik ve bütünlük düzeyleri kısmen düşecektir. Gizlilik ve bütünlük düzeyindeki yükselme ise erişilebilirliği kesintiye uğratabilmektedir.(Hekim &Başıbüyük, 2013, s.137)

Erişilebilirlik, bütünlük ve gizlik unsurlarını her daim koruma durumunda olan bilgi güvenliğinin belli ölçülerde yapılabilmesi için birtakım çalışmalar yapılmıştır. Çalışmalardan biri olan ISO 27001; Bilgi Güvenliği Yönetim Sistemi, kurum ve kuruluşların kurulum, sistem ve gözetim iyileştirme evrelerini kapsamaktadır. Bir diğer çalışma olan ISO 27002 ise; Bilgi Güvenliği Yönetim Sistemi sürecinde uygulanacak önlemleri içeren bir tehdit standardıdır. (Çifci, 2013, s.220-227)

Hiçbir ayrım olmaksızın tüm kurum ve kuruluşların hizmetlerini ve aralarındaki iletişimi sorunsuz bir şekilde gerçekleştirebilmeleri için kullanmaları gereken ağlar bulunmaktadır. Çalışanların ve hissedarların internet ve iç ağ sistemleri aracılığıyla tüm web uygulamaları ve alıcılarına ya da yurttaşlara sunduğu hizmetleri gerçekleştirdiği ağlar bunlardan birkaçıdır. İletişim yolları ve bilgi aktarımının bir bütün halini aldığı bu ortamlarda kullanılan sistemlerin güvenlik derecesi ile kullanıcıların duyarlılıkları siber güvenlik seviyesini belirleyecektir.(Tan & Aktaş, 2011, s.34)

Siber güvenliğin üç ana ilkesine ek olarak bilgi güvenliği açısından da önemli olan, kimlik doğrulama, güvenirlik, hesap verilebilirlik, inkar edilemezlik, esneklik ve emniyet gibi güvenlik ilkeleri de mevcuttur. Hesap verilebilirlik; gerçekleştirilen hareketlerin kullanıcıya yanı hareketleri gerçekleştiren şahsa kadar izlenebilmesidir.(Yeşilyurt, 2015, s.170-172)İnkar edilemezlik; herhangi bir iş ya da işlemin yapılmış olduğunun kanıtlanması ve geri çevrilememesidir (Yılmaz &Salcan, 2008, s.86).

Siber güvenlik, kurum içi ya da kurum dışından gerçekleştirilebilecek her çeşit siber saldırılar ile savaşın yanı sıra, bilgi aktarımı ve iletişim teknolojileri içerisinde bulunan, kullanıcı, sistem aktarımı ya da üretici kusurlarından oluşan açıklıklar ile zayıflıkları yani güvenlik

risklerini minimum seviyeye indirmeyi hedeflemektedir. (Bilgi Teknolojileri ve İletişim Kurumu, 2009, s.3).

Siber güvenlik, siber uzayın tamamını kapsamaktadır. Siber güvenlik kavramı bu kavramı kullanan kişilerin bakış açılarına göre birbirlerinden farklı anlamlara gelebilmekte ve tanımlanabilmektedir.(Akyeşilmen, 2018,s.110) Bilinçli veya bilinçsiz tüm tehditleri önleme hedeflenir. Tanımda yer alan süreçlerle ilgili gerçekleşen hareketler, sadece öngörülebilir tehditleri değil, öngörülemeyen tehditleri de içerisinde barındırır (Alp, 2018). Güvenlik kavramı fertlerden toplumlara, toplumlardan devletlere dek bütün varlıklar için önemli bir kavramdır. Uluslararası alanda bulunan bütün aktörler, kapsamları ve hedeflerine göre birbirinden farklı güvenlik düşüncelerine ve arayışlarına sahiplerdir (Dedeoğlu, 2008, s.24).

Devletlerin varlıklarını devam ettirebilmeleri, yer aldıkları sistemde ne kadar güvende olduklarına bağlıdır. Bu sebeple her devletin nihai amacı varlığını korumak ve devam ettirmek olduğundan, yaşamsal gereklilik olarak görülen güvenlik arayışının devletler açısından da geçerli olması olağandır.(Çeçen, 2005). Her bir devletin birey olarak kabul edilebileceği uluslararası arenada uluslararası güvenlik kavramı, devletlerin varlıklarını devam ettirebilmeleri açısından tehdit veya tehdit algısının olmaması şeklinde ifade edilir.

Ulus devletlerin ortaya çıkması ile birlikte gündeme gelen ulusal güvenlik kavramı, Birinci Dünya Savaşı'nın yaşanmasıyla evrensel bir boyuta ulaşmış ve akabinde İkinci Dünya Savaşı'nın ardından yeni ulus devletlerin oluşmasıyla önemini sürdürmüştür. Ulusal güvenlik tanımı ilk gündeme geldiği dönemde, yalnızca ülkenin bütünlüğü ve bağımsızlığını ifade edecek şekilde kullanılmış ve askeri güvenlik olarak tanımlanmıştır. Fakat ilerleyen zamanlarda uluslararası sistemde yaşanan değişiklikler sistem içerisine yeni aktörlerin dâhil olması ve tehdit algılamalarında meydana gelen farklılıklar ulusal güvenlik tanımının içeriğinde de değişim yaşanmasına sebep olmuştur. Meydana gelen değişimlerle birlikte ulusal güvenlik kavramı, devletin askeri, siyasi, ekonomik ve sosyal menfaatlerinin muhafaza edilmesi amacıyla gerçekleştirilen önemli çalışmalar bütünü olarak idrak edilerek makro güvenlik yaklaşımı haline gelmiştir.(Alkin & Gürlesel, 2004). Ulusal güvenlik kavramı mevcut dönem itibariyle ulusal çıkarların bir bütünü olarak değerlendirilmesi gereken bir kavram olmuştur. Siber güvenlik ve Ulusal güvenlik tanımları düşünüldüğünde aslında birbirlerine karşılık gelen hatta birbirlerini tamamlayan iki kavram olduğunu söylemek mümkündür (Arkun, 2003).

3. Küresel Güçlerin Ulusal Siber Güvenlik Stratejileri

Siber güç, etkili olduğu bütün çalışma sahaları ve güç öğeleri üzerinde gelişen olayları etkileyerek kazanım elde etmek için siber uzayı kullanma yeteneğidir. Mevcut tanıma göre siber uzay, günümüzde birçok ülkede kara, deniz, hava ve uzay gibi bir askeri operasyon olarak görülmektedir. Siber uzay, milli güç öğelerinin üzerinde etkinlik kurmasından ötürü öteki alanlardan ayrılır. Siber uzayın kapsamı, sadece kendisini oluşturan en temel öğelerden biri olan internetten ibaret değildir. Mevcut tanımdan yola çıkarak,"internet, iletişim ağları, dış dünyaya kapalı askeri ağlar, enerji hatları ağları, cep telefonları yazılım altyapılı telsizler, elektronik komuta sistemleri, cep teflonları, uydu sistemleri, insansız hava araçları sistemleri gibi birçok yazılım ve donanım elemanları toplamı" siber uzayın kapsamına girdiğini söylemek mümkündür (Akyazı, 2013).

Uluslararası İlişkiler disiplini yönünden bakıldığında ise siber uzayı Amerika Birleşik Devletleri ve Rusya Federasyonu'nun hem yıllardır ortaya koydukları ağ teknolojileri ve bunlar aracılığıyla askeri güçlerini ve casusluk olanaklarını azami derecede gerçekleştirmek için uygulamaya çalıştıkları planlamaları hem de kendi siber güvenliklerini temin etmek adına oluşturdukları strateji ve doktrinler ışığında domine ettikleri anlaşılmaktadır (Darıcılı, 2017: 19-20).

4. Küresel Bir Güç Olarak ABD'nin Ulusal Siber Güvenlik Politikaları

Uluslararası ilişkilerde tüm diplomatik yollar tükendikten sonra savaş başlar. Böyle bir durumda savaş, nihai sorun çözme yöntemi olarak görülmektedir. Savaş olgusunun geçirdiği değişim sürecinin anlaşılabilmesi açısından 11 Eylül saldırıları, uluslararası sistem üzerinde derin etkilere sahip olmuştur. ABD'nin böyle bir saldırıyla karşılaşması, ABD'yi de büyük bir endişeye sürüklemiştir. 11 Eylül saldırısından hemen sonra ABD Savunma Bakanlığı'nca yapılan bir durum değerlendirmesinde; modern güvenlik ortamı ile 1970'li yıllardaki güvenlik ortamının bir kıyaslaması yapılmış ve günümüzde bir dünya savaşı ihtimalinin 1970'lere nazaran üç kat, ikiden fazla devletin katılacağı bir bölgesel savaş ihtimalinin ise yarı yarıya azaldığı sonucuna varılmıştır (Yayla, 2013: 189).

1991 Körfez Harbindeki hava harekâtının mimarı olarak gösterilen ABD'li J.A. Warden, bütün ülkelerin ve stratejik unsurların sistem yaklaşımı ile analiz edilmesi gerektiğini ifade etmiştir. Buradan hareketle iç içe geçmiş beş halkadan söz etmiştir. Bu halkalar, sırasıyla; liderlik, önemli organlar, alt yapı, nüfus ve askeri kuvvetlerdir. Bunların yanı sıra, 2000

yılların başından itibaren internet ağının da önem kazandığı görülmüştür. Siber ağlarla saldırıların düzenlenmesi, ülkelerin önemli kurum ve kuruluşlarına müdahale edilmesi, bu beş halkanın zayıf kaldığını, bunlarla birlikte teknolojik üstünlüğünün de gerçekleşmesi gerektiğinin altı çizilmiştir (Canbey, 2009: 8-10).

21. yüzyıl siber savaş yüzyılı olarak adlandırılabilir. Özellikle ABD Savunma Bakanlığı'nın en çok rahatsızlık ve endişe duyduğu ülkelerin başında Rusya, Çin ve İran'ın gelmesi, ABD'nin bu bölgelerdeki politikasının da değişmesine yol açmıştır. Bundan hareketle ABD Savunma Bakanlığı, Kara, Deniz, Hava ve Uzay alanından sonra Siber Uzayı da beşinci muharebe alanı olarak tanımlamıştır. Yakın zamanda ABD kendi kritik altyapısını kritik bir milli değer olarak tanımlamış ve buna yönelik her türlü politik amaçlı büyük hasara ve can kaybına yol açabilecek siber taarruzu savaş sebebi olarak gördüğünü açıklamıştır (Beydoğan ve Canbey, 2008: 4-6).

Bu gelişmeler doğrultusunda teknolojinin etkisiyle dış politikanın değişim gösterdiği görülmüştür. İleri teknolojiye sahip, harp silah ve araçları, her geçen gün entegre devreler ve elektronik sistemlerle donatılırken, bir o kadar da, siber tehditlere açık hale gelmektedir. Bu nedenle ülkelere dış politika ve iç politika arayışlarında büyük bir değişim ve dönüşüm içerisine girmiştir. Siber savaşın siyasi hayata entegre edilmesiyle harekete geçen devletler, güvenlik konusunda önemli adımlar atmaya çalışmıştır. Özellikle bilgi teknolojilerin günlük hayatın bir parçası haline gelmesi, toplumsal değişimin yaşanmasına da yol açmıştır (Özger, 2016: 19-21).

Bilişim teknolojilerindeki gelişme, vatandaşlar ile hükümet arasında iki yönlü bir iletişim kanalı oluşturmuştur. Bu iletişim kanalı ile vatandaşların ülke yönetimine daha fazla etkide bulunmaları sağlanmış ve bu sayede temsili demokrasiden katılımcı demokrasiye bir geçiş yaşanmıştır. Ayrıca internetin getirmiş olduğu olanakların devlet işleyişlerindeki şeffaflık, katılımcılık ve hesap verebilirlik ilkelerini de etkilemiş ve devlet liderlerini bu yönde zorlamıştır. Bunların yanı sıra, özellikle devletlerarasında yaşanan siber savaş, saldırı, tehdit ve sızma yöntemleri ön plana çıkmaktadır. Bu yöntemlere karşı ulusal güvenliği korumak ve güvenliğe karşı oluşacak zedelenmelere yönelik politikalar üretmek, neredeyse, tüm devletlerin ana politikalarından biri olmuştur (Klark ve Knake, 2011: 19-23).
ABD'nin bu yöndeki politikaları ise,

1) Savunma Bakanlığı bünyesinde Kara, Deniz ve Hava Kuvvetleri Daireleri'nde her birinin kendi görev ve sorumluluklarıyla ilgili faaliyet göstermesi için Birleşik Siber Merkezleri'nin kurmuş olması,

2) Kritik altyapıları korumak,

3) Hükümetin iletişimini ve operasyonel gücünün artırılmasını sağlamak,

4) Ulusal siber güvenlik koşularını ilerletmek,

5) Ulusal Siber İstihbarat Direktörü merkezinin daha da güçlenmesi yönünde yatırımlar gerçekleştirmek ve sağlamlığını korumak gibi maddeler sayılabilir (Sambur, 2016: 167-169).

Aslında siber denilen saldırı ve savaşlar, sadece siyasi boyutu etkilememektedir. Ekonomik, askeri ve sosyokültürel alanları da etkilemektedir. Ancak siyasi boyutunun etkilenmesi sonucu tüm birimlerin etkilendiği de görülmektedir. ABD'de gerçekleşen 2017 seçimlerinde bu durum göze çarpmaktadır. 2017 seçimlerinde Cumhuriyetçi Trump'ın Demokratlara karşı zaferle çıkması, bazı belirsizlikleri de beraberinde getirmiştir. Rusya tarafından seçimlere müdahale edildiği iddia edilmiş ve bazı sorunlar yaşanmıştır. Trump, bu tür iddiaları reddetmiş olsa da, devletin bazı üst yetkilerinin onay vermiş olması, Trump'ı da kararından caydırmıştır. Seçimlere yapılan siber saldırılar, Trump'ın kazanmasını sağlamış ve bir Trump-Putin dostane ilişkilerinin olabileceği, kararı ortaya atılmıştır. Nitekim yapılan açıklama ve politik davranışlar, iki ülke liderlerinin dost olduğu yönünde bir tahmin yürütülmüştür. 2017'de yapılan G-20 Zirvesi bu durumu somutlaştırmaktadır. Çünkü Trump-Putin G-20 Zirvesi'nden sonra "ortak siber faaliyet" yürütme kararı almaları, iki ülke liderlerinin dostane ilişkilerinin olduğunu göstermiştir (Darıcılı, 2017: 16-19).

Amerikan toplumu ve bazı devlet yetkilileri arasındaki uyuşmazlık durumunun sürdüğüne yönelik diğer hamle CIA tarafından gerçekleştirilmiştir. FBI'ın Trump'ı destekler nitelikteki teşebbüslerine karşılık CIA hazırladığı bir rapor ile ABD'de gerçekleştirilen seçimlere Rusya tarafından müdahale edildiği öne sürülmüştür. Washington Post isimli Amerikan gazetesinde ele alınan bu sava göre Rusya'nın seçimlerin Trump'ın zaferiyle sonuçlanmasına yönelik olarak girişimlerde bulunduğu kanısına varılmıştır. CIA tarafından hazırlanan bu raporda Rus hükümetinde görevli bazı üst düzey yetkililerle yakın ilişki içerisinde bulunan bazı insanların, siber saldırılar yoluyla Trump'ın rakibi olan Demokrat Parti'ye ait gizli ve özel bilgilerini Wikileaks'e ileten kişilerin belirlendiği ifade edilmiştir. Söz konusu rapor ABD kongresinde bulunan senatörlere de gönderilmiştir. Dönemin Amerikan Başkanı Obama ise raporda yer alan iddiaların doğruluğunun incelenmesine yönelik yönerge vermiş ve incelemenin yemin töreni öncesinde yapılmasını söylemiştir (Muradoğlu,2016).

Tüm bu gelişmeler doğrultusunda ABD, hem içte hem de dış politikada, ulusal güvenliğini sağlamak ve korumak adına, küresel güçlere karşı daha ılımlı politikalar yürütmeye çalıştığı (Trump-Putin örneği) görülmüştür. Bunun yanı sıra, kurum ve kuruluşlardaki sistemlerini de güçlendirme stratejisini geliştirme ve daha kararlı adımlar atma yoluna gitmiştir.

Sonuç

Dünya devletlerinin en temel endişeleri 21. yüzyıl çağında ileri teknolojinin saldırı, tehdit ve savaş şeklinde kullanılıyor olması olmuştur/olmaktadır. Özellikle ABD, Rusya ve Çin gibi küresel güçlerin, 21. yüzyıla ayak uydurmaları sonucu, güvenlik teriminin yeniden ele alınmasını olanak görmüştür. Seçim zamanlarında siber saldırıların ve siber tehditlerin çok sık dillendirilmesi, sadece küresel güçleri değil, 3. dünya devletlerini de büyük bir endişeye sürüklemektedir.

Bilgi ve iletişim teknolojilerinde yaşanan devrim, insanlığa bugüne kadar hayal edilemeyecek olanaklar sunmuş ve toplumsal dönüşümün yaşanmasına neden olmuştur. Uluslararası ilişkiler disiplini içerisinde ulusal güvenliği yerel, bölgesel ve küresel seviyede olmak üzere, askeri, ekonomik, çevresel ve siyasal bileşenlerinin oluşturduğu bütün bir olarak değerlendirilecek bir ortam hazırlanmıştır. Siber saldırılar üzerinden gerçekleşen terörizm faaliyetlerinin olması, devletlerin siber üzerine ortak anlaşmalara imza atmalarına olanak vermiştir. ABD-Rusya örneğinde görüldüğü gibi, diğer devletlerinin de önlem almaya gayret gösterdikleri görülmüştür. Hassas bir konu olan ulusal güvenlik boyutunun korunması, her devlet için bağımsızlık ve egemenlik ilkelerinin vazgeçilmez unsurlarıdır. Bu nedenle sibere karşı sadece ABD, Rusya ve Çin değil, diğer dünya devletlerinin de sibere yönelik faaliyetler oluşturduğu ve stratejilerle politikalar ürettiği görülmektedir.

Bu gelişmelerle birlikte, ABD başta olmak üzere, bilgi teknolojilerinde önde gelen ülkeler, kritik altyapı sistemlerinin savunmasında da önde olmak amacıyla siber güvenlik politikaları ve stratejileri oluşturmakta, siber komutanlıklar kurma gibi yeni yapılanmalara gitmekte ve siber savunma yeteneklerini geliştirmektedir. Çünkü 21. yüzyıl çağı, geride kalan diğer tüm çağlardan büyük bir farklılık göstermektedir. Artık insan gücünün yerini teknolojik gücün aldığı ve bu yönde savaş ve saldırıların gerçekleştiği bir çağ olmuştur. Bu nedenle ABD'nin

de bu çağ içerisinde yerini almak ve dünya siber güç merkezi olmak amacıyla politikalar üretmeye çalıştığı görülmektedir.

Kaynakça

Akyazı, U.(2013). Siber Harekât Ortamının Siber Güvenlik Tatbikatları Kapsamında Değerlendirilmesi. İstanbul: Harp Akademileri Basımevi.

Akyeşilmen, N.(2018). Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik, Ankara: Orion Kitabevi.

Alkin, K. ve Güresel C. F.(2004). Dünya Ekonomisine Yönelik Global Tehditler; Dünyada Güvenlik ve Tehdit Kavramının Evrimi ve Global Güvenlik İçinde Ulusal Güvenlik Perspektif. İstanbul Ticaret Üniversitesi Fen Dergisi. 3(6),ss.9-34.

Alp, Ö.(2018). Akıllı Şehirlerde Siber Güvenlik. Yayınlanmamış Yüksek Lisans Tezi, İstanbul: Bilgi Üniversitesi.

Arıboğan, D.Ü.(2007). Uluslararası İlişkiler Düşüncesi: Tarihsel Gelişim, İstanbul: Bahçeşehir Üniversitesi Yayınları.

Arkun, M.E.(2003). Türkiye İçin Bir Enformasyon Politikasının Ana Öğeleri Neler Olmalı? Bilgi Dünyası, (2), ss.175-191.

Baldwin, D.A.(2003). Güvenlik Kavramı. Ç. Şahin(çev.), Avrupa Dosyası, Cilt:2, ss.5-35.

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

Beydoğan, T. A. ve Canbay, C.(2008). Siber Güvenliğin Sağlanması ve Kritik Bilgi ve Altyapıların Korunması: Gelişmekte Olan Ülkeler İçin Yol Haritası, 17. ITS Konferansı, Kanada: Montreal, 24 – 27 Haziran.

Bıçakçı, S.(2013). 21. Yüzyılda Siber Güvenlik, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Bilgi Teknolojileri ve İletişim Kurumu (2009). Siber Güvenliğin Sağlanması: Türkiye'de Mevcut Durum ve Alınması Gereken Tedbirler. https://s3.amazonaws.com/academia.edu.documents/45165390/Siber_Guvenligin_Saglanmasi__Turkiyedeki_Mevcut_Durum_ve_Alinmasi_Gereken_Tedbirler.pdf?AWSAcce

ssKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1547921914&Signature=ZSy4uCzW2FN%2BCp8oNKhkd4MbCYI%3D&response-content disposition=inline%3B%20filename%3DUlusal_Siber_Guvenligin_Saglanmasi.pdf (Erişim Tarihi:19.12.2018).

Canbey, C.(2009). Güvenliğin Sağlanmasında İletişimin Rolü, E-Akademi Dergisi, Sayı 91. http://www.eakademi.org/incele.asp?konu=G%DCVENL%DD%D0%DDN%20SA%D0LANMASINDA%20%DDLET%DD%DE%DDM%DDN%20ROL%DC&kimlik=1646239406&url=makaleler/ccanbay-1.htm (Erişim Tarihi: 24.12.2019).

Clark, R.A. ve Knake R.K. (2011). Siber Savaş, İstanbul: İstanbul Kültür Üniversitesi Yayınevi.

Çeçen, A.(2005). Türkiye'nin Güvenliği. G. Güngörmüş Kona(ed.). Uluslararası Çatışma Alanları ve Türkiye'nin Güvenliği. ss.107-126.

Çifci, H.(2013). Her Yönüyle Siber Savaş, Ankara: Tübitak Popüler Bilim Kitapları.

Daban, C.(2016). Siber Güvenlik ve Uluslararası Güvenlik İlişkisi, Cyberpolitik Journal, Vol.1,No.1http://cyberpolitikjournal.org/wpcontent/uploads/2017/02/Journal_Dergi_pdf .pdf (14.12.2018).

Darıcılı, A. B.(2017). "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi", Uluslararası Çalışmalar Dergisi, 1(1).ss.1-24.

Dedeoğlu, B.(2008). Uluslararası Güvenlik ve Stratejiler, İstanbul: Yeniyüzyıl Yayınları.

Duygu, N.(2015). Uluslararası Sistem Açısından Güvenlik ve Güvenlik Algısında Yaşanan Değişmeler,(http://www.tuicakademi.org/uluslararasi-sistem-acisindan-guvenlik-ve-guvenlik-algisinda-yasanan-degismeler/) (Erişim Tarihi: 20.12.2018).

Eralp, A.(1996). Devlet, Sistem ve Kimlik: Uluslararası İlişkilerde Temel Yaklaşımlar, İstanbul: İletişim Yayınları.

Gündüz, A.(2015). Milletlerarası Hukuk, İstanbul: Beta Yayınları.

Hekim H. ve Başıbüyük O.(2013). "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, 4(2).s.135-158.

Karadağ, U.(2016). Birleşmiş Milletler Antlaşması'na Göre Meşru Müdafaa Hakkı, İnönü Üniversitesi Hukuk Fakültesi Dergisi, 7(2). ss.171-185.

Kara, M.(2013). Siber Saldırılar-Siber Suçlar ve Etkileri, Yayınlanmamış Yüksek Lisans Tezi. İstanbul: İstanbul Bilgi Üniversitesi.

Libicki, M.C.(1995). What is Information Warfare?, Washington: National Defence University Press.

Muradoğlu,A.(2016).Trump'a Karşı CIA Hamlesi, https://www.yenisafak.com/yazarlar/abdullahmuradoglu/trumpa-karsi-cia-hamlesi-2034780 (Erişim Tarihi: 13.01.2019).

O'Connel, M.E.(Summer 2002). "Lawful Self-Defense To Terrorism", University Of Pittsburgh LawReview, Vol. 63, Issue 4, ss.889-908.

Özger, Ö.(2016). Gözetim Kavramının Tarihsel Gelişimi ve Elektronik Gözetim, Cyberpolitik Journal, Vol.1, No.1.ss.11-37. http://cyberpolitikjournal.org/wp-content/uploads/2017/02/Journal_Dergi_pdf.pdf (Erişim Tarihi:13.01.2019).

Sambur, B.(2016). "Siber Çağda ABD Seçimleri Ve Siber Bir Mit Olarak Trump", Cyberpolitik Journal, Vol. 1, No. 1.ss.169-175.

Şentürk, H. et.al., (2012). Cyber Security Analysis of Turkey, International Journal of Information Security Science, Vol.1, No.4.ss.112-125.

Tan H. ve Aktaş A.Z.(2011). "Bir Kuruluşun Bilgi Güvenliği İçin Bir Yaklaşım", IV. Ağ ve Bilgi Güvenliği Sempozyumu Bildiriler Kitabı, TMMOB Elektrik Mühendisleri Odası, Ankara.

Turgut, R.(2003, Mayıs). Küreselleşmenin Askeri Boyutları ve Güvenlik Stratejilerine Etkileri.Küreselleşme ve Uluslararası Güvenlik Birinci Uluslararası Sempozyumu,(1). s.41-44.

Türk Dil Kurumu,(1 Ocak 2009).Büyük Türkçe Sözlük (t.y.), "Güvenlik", http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c433e42013c60.29375572 (Erişim Tarihi:10.01.2019).

Walt, S.M.(2003). "Güvenlik Çalışmalarının Rönesansı", Avrasya Dosyası, 9(2), ss.71-106.

Yayla, M.(2013). “Hukuki Bir Terim Olarak Siber Savaş”, Türkiye Barolar Birliği Dergisi, Sayı 104. ss.178-194.

Yeşilyurt, H.(2015), “Ulusal Güvenlik Perspektifinde Siber Güvenlik”, Fatih Tombul ve diğerleri (Ed.), Siber Suçlar, Tehditler, Farkındalık ve Mücadele içinde (169-193), Ankara: Global Politika ve Strateji.

Yılmaz, S. ve Salcan, O.(2008). Siber Uzay’da Güvenlik ve Türkiye, İstanbul: Milenyum Yayınları.