Soğuk Savaş Sonrası ABD'nin Siber Güvenlik Politikası

Cyber Security Politics of USA After the Cold War

Gönderilme tarihi/received: 16.06.2020

Kabul tarihi/accepted: 08.07.2020

Derleme / Review

Şeyma KIZILAY[1]

Öz

Uluslararası İlişkiler tarihi ve disiplini içerisinde bir dönüm noktası olarak görülen Soğuk Savaş, yeni bir düzenle birlikte yeni anlayışlar da getirmiştir. Devletlerin güvenlik anlayışlarında zamanla meydana gelen değişim de bu yeniliklerin bir parçası olmuştur. Uluslararası aktörlerin çeşitlendiği bu dönemde savaş kavramında yaşanan dönüşümle savaşın aktörleri yalnızca devletler olmaktan çıkmış ve terör grupları, özel askeri şirketler gibi yeni aktörler ortaya çıkmıştır. Dolayısıyla yeni tehdit alanları ve yeni anlayışlar görülmeye başlanmıştır. Asimetrik tehdit, vekâlet savaşları, siber savaşlar ve siber güvenlik dördüncü nesil savaş kavramı ve güvenlik anlayışı içerisinde yer almaktadır. Bu çalışmada uluslararası alanda önemi artan siber güvenlik kavramının Amerika Birleşik Devletleri (ABD) dış politikasındaki ve stratejilerindeki yeri incelenmiştir. Siber güvenliğin sağlanması adına faaliyet gösteren kurumlar, temel stratejiler ve yaşanan siber olaylar ele alınmıştır. Teknolojinin her alanda etkisini artırmasıyla daha önemli hale gelen siber güvenlik kapsamında, ABD güvenlik politikasında nasıl bir değişikliğin meydana geldiği sorusu araştırmanın hareket noktasını oluşturmaktadır.

Anahtar Sözcükler: Güvenlik, Siber Güvenlik, ABD.

Abstract

In the history and discipline of International Relations, the Cold War brought new insights together with a new order. The change in the security perceptions of states over time has also been a part of these innovations. With the transformation in the concept of war in this period when international actors diversified, the actors of the war have ceased to be states only and new actors such as terrorist groups and private military companies have emerged. Therefore, new threat areas and new understandings began to be seen. Asymmetric threat, proxy wars, cyber wars and cyber security are included in the security concept of the fourth generation war. In this study, the concept of cyber security, which has gained importance in the international arena, has been examined in the foreign policy and strategies of the United States (USA). Institutions operating in order to ensure cyber security, basic strategies and

[1] Bursa Uludağ Üniversitesi, Ortadoğu Çalışmaları Doktora Öğrencisi. kizilay.eylul@gmail.com, ORCID ID: 0000-0001-8424-8633.

cyber events experienced were discussed. In the context of cyber security, which has become more important as technology increases its impact in all areas, the question of what kind of a change in US security policy occurred is the starting point of the research.

Keywords: Security, Cyber Security, USA.

Giriş

Güvenlik kavramı konusunda birçok tanım bulunmakla birlikte disiplin içerisindeki temel teorik yaklaşımlar tarafından farklı algılamalarla güvenlik konusunda nitelendirmeler yapılmıştır. Temel olarak; herhangi bir korkunun olmaması ve güvende hissetme olarak tanımlanan güvenlik kavramı, realist anlayışa göre; ancak güç ile sağlanabilir. Machiavelli, iyi yönetimle, Morgenthau varlığını sürdürmekle, Kenneth Waltz, Edwad Carr ve realist görüşe sahip diğer düşünürler, askeri kapasite ve güç dengesi ile güvenli olunacağını ileri sürmüştür (Brauch, 2012, s.168-169). Devletin güvenliğini uluslararası sistemin güvenliği ile ilişkilendiren İdealistler ise güvenliğin iş birliği ile sağlanacağı üzerinde durmuşlardır. Güvenliğin içeriğini ve kapsamını daha geniş ölçüde ele alan Kopenhag Okulu düşünürleri farklı boyutlardaki güvenlik stratejilerine de dikkat çekmiş ve çeşitli bir yapıdan söz etmişlerdir. Teknolojik gelişmeler ve küreselleşme ile birlikte daha geniş bir yelpazeye sahip olan güvenlik kavramı içerisinde birçok yeni alan ortaya çıkmış ve konjonktürel olarak önemi de artmıştır (Brauch, 2012, s.169-175). Ulusal güvenliğin bir alt kolu olan siber güvenlik kavramı da Soğuk Savaş sonrası dönemde zamanla daha önemli bir alan haline gelerek devletlerin özel olarak strateji geliştirdikleri bir politikaya dönüşmüştür. Askeri kapasite, teknoloji, sanayi ve diğer her alanda genel anlamda süper güç olarak görülen ABD, siber güvenlik alanında da özellikle 2003 sonrası dönemde stratejiler geliştirmeye ağırlık vermiştir. Çalışmada siber tehdit, siber uzay, siber güvenlik gibi kavramların incelenmesinin ardından ABD'nin siber güvenlik stratejileri kapsamında attığı adımlara ve bu yöndeki yasal düzenlemelerine ve oluşturulan kurumlara yer verilerek temel siber güvenlik politikası ortaya koyulacaktır.

1.Siber Kavramlar

Soğuk Savaş sonrası sistemde özellikle 9/11 sonrasında ortaya çıkan belirsizlik ortamı ve asimetrik durum ulusal güvenliğin daha ön planda olduğu bir sürece yol açmıştır. Ulusal güvenliğin kapsamının ve algısının değişmesi onun yalnızca fiziksel ve askeri saldırılar karşısında alınan önlemler anlamına gelmediği bir yaklaşıma dönüşmüştür. Bu yeni yaklaşım kapsamında ulusal güvenlik içerisinde siber saldırılar, terör, salgın hastalıklar ve ekonomik gelişmelerin engellenmesi de ulusal güvenliğin bir parçası haline gelmiştir. Ulusal güvenlik kapsamında devletlerin önemli verilerinin korunması hususu da önem kazanmış, devletler için önem teşkil eden enerji, ulaşım, sağlık gibi kritik alt yapılar ile ilgili olarak siber suçlara ve tehditlere karşı siber politikalar geliştirilmiştir (Göçoğlu ve Aydın, 2019, s.234). Siber ön ekiyle yeni anlamlar kazanan kavramlar ulusal güvenliğin bir parçası olarak günden güne önem kazanarak yeni boyutlar oluşturmuştur. Çalışmanın kapsamı bakımından siber uzay, siber tehdit, siber güç ve siber güvenlik kavramları ele alınmıştır.

Siber Uzay: "Siber" kavramı için tam ve net bir tanım bulunmamakla birlikte iki niteliğinden söz edilmektedir. Bunlar; bilgisayar veya internetle kurulan ilişkilerin nitelenmesi ve fiziksel dünyanın dışındaki bir sanal gerçekliktir (Demirel, 2012, s. 34; Kurnaz ve Önen, 2019, s. 84). ABD Savunma Bakanlığı siber uzay kavramı tanımında bilgisayar sistemlerini, interneti içeren bilgi teknolojisi altyapılarının bulunduğu bir küresel alan nitelemesini kullanmıştır. İkinci bir tanım da "insanların telekomünikasyon yoluyla herhangi bir sınırlama olmaksızın birbirlerine bağlı olabilmeleri" şeklindedir

(Habertobb, 2015, s.12). Türkiye'nin 2016-2019 Siber Güvenlik Strateji Belgesi'nde siber uzay: "Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam" olarak tanımlanmıştır (2016-2019 Ulusal Siber Güvenlik Stratejisi, s.7). Başka bir tanımda ise küresel etki alanı olarak nitelendirilen siber uzay, çeşitli elektronik ve elektromanyetik spektrumdan meydana gelen verilerin depolanması amacıyla tasarlanmaktadır (Yılmaz, 2020, s.67). Siber uzayın kapsamında dünya üzerinde bilgisayar ağlarının tamamı ve onların kontrol ettiği her şey bulunmaktadır. İnternetin bağlı olmadığı ağlar da bu kapsamda yer almaktadır. Devletler açısından kara, hava ve deniz gibi bir alan olarak kabul edilen siber uzay, yeni bir harekât alanı olarak görülmektedir (Ermiş, 2018, s. 2). İnsan eliyle oluşturulmuş olması ve özel sektörün hâkimiyetinde olması hasebiyle diğer alanlardan farklılık arz etmektedir. Bununla birlikte bir özelliği de bilgi sistemlerinde işlenen verilerden oluşmasıdır. Bu alandaki harekât yeteneğinin neredeyse ışık hızında gerçekleşiyor olması aynı hızdaki tehditleri de içermektedir. Son olarak ise, bir bağımlılığı ve sınırı olmaması bakımından coğrafyadan bağımsız bir harekât alanı olma özelliğine sahiptir (Özçoban, 2014, s.52-53). Sınırların olmaması, yüksek hız nedeniyle aynı şekilde tehdit ve risk içermesi siber ortamda tehdit ve saldırının siber olarak gelişmesine neden olmaktadır.

Siber Tehdit-Siber Saldırı: Siber alanda karşılaşılan her türlü saldırı ve riskler tehdit olarak kabul edilmektedir. Aynı zamanda siber saldırılar için kullanılan araçlar da bu kategoride yer almaktadır. Siber tehditler, devletler için önemli ve öncelikli olan kritik alt yapı tesisleri olarak adlandırılan yapıları hedef almaktadır. Bunlar; uluslararası enerji, ulaşım, finans sistemleri, savunma altyapıları, telekomünikasyon sistemleri, sanayi ve teknoloji sırlarının bulunduğu sistemler, e-devlet uygulamalarıdır (Kaya, 2012, s.25). Siber uzaydaki verilerin değiştirilmesi, sahtesinin üretimi, kesintiye uğraması gibi teşebbüsler siber saldırı olarak değerlendirilmektedir. Saldırılar verilere ya da kontrol sistemlerine olmak üzere iki şekilde meydana gelebilmektedir. Bilgisayar sistemlerine yetkisiz olarak girmek, bilgi casusluğu ya da hırsızlığı yapmak, kullanıcıların sisteme girişinin engellenmesi gibi amaçlarla gerçekleştirilen saldırılarda siber silahlar olarak da adlandırılan birtakım yöntemler kullanılmaktadır (Özçoban, 2014, s.56). Zararlı yazılım türü olan virüsler; bilinmeyen yazılımların yüklenmesiyle ortaya çıkan ve faydalı gibi görünüp zararlı fonksiyonlar içeren Truva atları; virüsten farklı olarak herhangi bir müdahale olmaksızın yayılan ve başkası tarafından bilgisayarın ele geçirilmesini kolaylaştıran kurtçuklar; en tehlikeli olarak nitelendirilen botnatlar; istem dışı elektronik postalar (spamlar); şifreleri ve banka hesap bilgilerini çalabilen casus yazılımlar (spyware); hizmet dışı bırakma, aldatma ve yetkisiz girişler siber saldırılarda kullanılan araç ve yöntemlerdir (Kaya, 2012, s.33-34; Aslay, 2017, s.26). Bütün bunlardan yola çıkarak siber alandaki herhangi bir tehdidin önceden tahmin edilebilir olmaması, önlem alınamaması ve alanının dijital olması bu tehditlerin diğerlerinden farklı olmasında temel esastır (Kurnaz ve Önen, 2019, s.85).

Siber Suç-Siber Terör: Siber saldırı ya da tehditler bilinçli ve bilinçsiz olabilirken siber suçlar zarar vermek amacıyla gerçekleştirilen eylemler olarak onlardan ayrılmaktadır. Siber suçlar, belirli bir ağ ya da bilgisayar hedef alınarak gerçekleştirilmektedir. Yetkisiz erişim, siber hırsızlık, müstehcenlik ve şiddet siber suçlar olarak kabul edilmektedir (Demirel, 2012, s.56). Siber alanın terör faaliyetleri için kullanılması ve bu alanda terörizme fayda sağlayacak eylemler gerçekleştirilmesi de siber suçların terörizm boyutunu oluşturmaktadır. Bu kapsamda siber terör/terörizm; siyasi amaçlarla bir devleti ya da vatandaşlarını aşağılamak, korkutmak ve zarar vermek amaçlarıyla bilgisayarlara yapılan kanunsuz saldırılar olarak tanımlanmaktadır. Amaç, korku salmakla birlikte devletleri politikalarını değiştirmeye zorlamak da olabilmektedir (Kaya, 2012, s.22). Başka bir tanıma göre de; terör örgütlerinin toplumu endişelendirmek amacıyla politik nedenlerden dolayı yaptıkları eylemlere siber terör denilmektedir (Özçoban, 2014, s.65). En önemli siber tehdit ya da saldırı kapsamında değerlendirilen unsur olarak siber terörizm karşımıza çıkmaktadır. Korkutmak ve caydırmak amacıyla yapılan silahlı eylemler olarak adlandırılan terörizm siber alana taşındığında, siyasi ve sosyal birimlerde korku oluşturmak ve zarar

vermek amacıyla resmi kurumların bilgi sistemlerine yönelik saldırılarda bulunmak olarak karşılık bulmaktadır. Siber terörizmdeki kilit nokta ise bireye veya mala karşı şiddet içermesi ve hasara yol açmasıdır (Yılmaz, 2020, s.70).

Siber Güç: Siber alanda inisiyatifi elinde bulunduran unsur olarak nitelendirilmektedir. Aynı zamanda siber alanı stratejik avantaj sağlamak amacıyla kullanmak olarak da tanımlanmaktadır. Siber güç siber alandaki kültür ve politikayı oluşturmaktadır. Bireyin, toplumun ve siber alanın bir arada bulunması demek olan siber güç bu üç alandan oluşmaktadır. Bireyin siber gücü politikayı, toplumun siber gücü sanal eliti meydana getirmektedir. Bu alanların bir araya gelmesiyle de sosyal düzenin yapı taşı oluşmakta ve siber güç ortaya çıkmaktadır (Kaya, 2012, s.22). Genel itibariyle siber güç; bir ülkenin çatışma, kriz ve barış dönemlerinde, sivil ve askeri olarak siber güvenlik, etkin siber savunma ve gerektiğinde uluslararası hukuka uygun olarak siber saldırı ya da taarruz konularındaki teşkilatı ve teknolojisi ile imkânlarını içermektedir. Uluslararası İlişkiler kapsamında değerlendirildiğinde önceki dönemlerde low politics (düşük politika) unsuru olarak görülen siber güvenlik ve bu alanda güç sahibi olma durumu, Wikileaks tarafından açığa çıkarılan gizli belgeler hadisesi ve 2010 yılında baş gösteren ardından yayılan Arap Baharı ile önemi artan ve göz önünde bulundurulması gereken bir etmen olarak görülmeye başlanmıştır. Özellikle Arap Baharı sürecinde sosyal medyanın oynadığı rol internetin siyasette ne derece önemli olduğunu göstermiştir (Çelik, 2018, s. 115).

Siber İstihbarat: Ekonomik, politik ve askeri avantaj sağlamak adına dijital verilerin tamamına ulaşmak maksadıyla uygulanan istihbarata verilen isimdir. Siber istihbaratta faaliyeti yürütenlerin amaçları ve hedefi de belirli olmakta ve bilinçli bir hareketten söz edilmektedir (Güntay, 2014, s.87).

Siber Savaş: Devletlerin birbirlerinin bilgisayar sistemlerinde zarara yol açmak amacıyla gerçekleştirdikleri eylemler olarak tanımlanmaktadır. Siber suçlardan farklı olarak siber savaşın taraflarının devletler olması nedeniyle siber savaş ihtimaline karşı politikalar üretilmesi devletler tarafından önemli görülmeye başlanmıştır (Demirel, 2012, s.44). Siber ortamda gerçekleşmesine rağmen siber savaşın geniş ölçekli ve etkili sonuçları ortaya çıkmaktadır. Bir siber savaş sonucunda petrol ve doğal gaz boru hatlarında patlamalar, uzun süreli elektrik kesintisi, nükleer tesislerde yangın, hava ve kara trafik kontrol sistemlerindeki hatalar sonucu kazalar meydana gelebilmektedir (Özçoban, 2014, s.68-69). Devletlerin bütün imkânlarıyla mücadele ettikleri süreçler olan savaşlar gibi siber savaş da sivil ve asker olarak tüm ülke cephesini içine alan, az maliyetle çok etki yaratması bakımından asimetrik olan bir savaş türü olarak karşımıza çıkmaktadır. Şeref Sağıroğlu (2018)'na göre siber savaş; kendine has bir alan olan siber ortamda kullanılan siber silahlar ve taraflar arasındaki farklılıklar nedeniyle simetrik, asimetrik ve hibrit yaklaşımların kullanıldığı savaş şeklidir.

Siber Güvenlik: Siber uzay kapsamında siber güvenlik tanımı da kurum ve kuruluşların siber uzaydan gelebilecek olası tehdit ve risklere karşı varlıklarını korumak adına geliştirdikleri güvenlik politikaları ve risk yönetimi yaklaşımlarıdır (Habertobb, 2015, s.13). Daha genel ve kısa tanımı ile siber güvenlik; siber ortamdaki veri, süreç, politika, işlem ve sistemlerin güvenliğinin sağlanmasıdır (Sağıroğlu, 2018, s.24). İnternet kullanımının yaygınlaşması, siber ortamın kötü niyetle kullanılmasına da yol açmış ve bu ortamda yapılan saldırıların zararlı boyutlara ulaşması, devletlerin bu yönde adımlar atmasının gerekliliğini ortaya koymuş ve güvenlik algısında değişimlere neden olmuştur. Siber güvenlik siber hayatın gizliliği, bütünlüğü ve erişilebilirliği gibi unsurlar bakımından güvenliğin sağlanması kapsamında izlenen yollar ve yapılan uygulamalar olarak ve siber alanlar ile bilgi alt yapılarına zarar verebilecek tehditlere karşı korumak amacıyla atılan adımlar şeklinde de tanımlanmıştır (Kurnaz ve Önen, 2019: s.84). Bilişim sistemine yetkili dışında kimsenin girememesi (gizlilik), bu sistemlerin yalnızca yetkili sistem ve kişilerce değiştirilmesi (bütünlük) ve yetkililerin ihtiyaç anında bu bilgilere erişimi (erişilebilirlik) noktasında bir ihlalin yaşanması, siber güvenlik alanında değerlendirilmektedir (Sertçelik, 2015, s.26). Uluslararası ilişkilerdeki low politics-high politics (düşük politika-yüksek

politika) ayrımı neticesinde siber güvenlik düşük politika kapsamında değerlendirilirken güvenlik algısında yaşanan değişim ve siber alandaki gelişmelerle birlikte ulusal güvenliğin sağlanmasında ya da düzenin korunmasında tehdit boyutunda bir güvenlik açığı oluşturmasının anlaşılması sonucu yüksek politika olarak görülmeye başlanmıştır. Devletlerin birbirleriyle olan ilişkilerini büyük oranda etkileme kapasitesine sahip olan siber güvenlik, oluşturulan politikalar ile hâkim olmaya çalışılan bir alan haline gelmiştir (Sertçelik, 2015, s.28). Küreselleşme ile her alanda farklılıkların yaşandığı günümüz dünyasında bağımsızlık ve güvenlik konularında temelini rakip devletlerin ağlarında nelerin yer aldığını bilmektir. İnternet uzmanları tarafından gerçekleştirilen siber savaşlar elektronik istihbaratçıları ön plana çıkarmış ve devletlerin en çok önem verdikleri alan siber güvenlik olurken istihbaratçılar da en çok önem verilen kişiler haline gelmektedir. Kullanılan bilişim silahları ile bir ülkenin tamamında elektrik, su, iletişim ve ulaşım gibi ağ ve hizmetler anında etkisiz hale gelebilmektedir. Dolayısıyla devlet sistemlerini olduğu kadar her bir bireyi önemli ölçüde etkilemesi bağlamında her vatandaş siber güvenliğin bir unsuru, bir parçası olmaktadır (Özdemirci ve Torunlar, 2018, s.82). Devlet, birey ve sistem üzerindeki bu etkiler dolayısıyla siber güvenlik; güçlü ve bağımsız bir devlet olma yolunda ağ yapıları üzerindeki hâkimiyet noktasında önem teşkil etmektedir.

Siber güvenlik konusunda algı ve tespitlerin odaklandığı konuları Murat Demirel şu şekilde sıralamıştır: Kişilerin bilerek ya da farkında olmaksızın fiziksel dünyaya ve siber uzaya yönelik oluşturdukları tehditlerin önlenmesi, siber uzay verilerinin korunması ve yönetilmesi, yazılım ve donanımlardaki tasarım ve üretim hatalarını gidermek ve iletişim ve enformasyon altyapısının güvenliği (Demirel, 2012, s.40).

Siber tehditlerin artması bu tehditlere yönelik alınan önlemlerin artırılmasını da gerekli kılmıştır. Bu kapsamda yasal düzenlemeler ve müdahale birimleri oluşturulmaya başlanmıştır. Kritik altyapıların iletişim teknolojileriyle olan bağımlılık ilişkisi uluslararası toplum açısından siber güvenliği daha önemli kılmıştır. Bunun yanı sıra siber olaylarla uluslararası alandaki ilişkilerin kapsamlı ve karmaşık hale gelmesi siber güvenliğe verilen önemi artırmaktadır. Siber güvenliğin sağlanmasına yönelik çalışmalar konusunda sekiz önemli unsura dikkat çekilmektedir. İlk olarak ulusal strateji ve politikalar geliştirilmesi gelmektedir. İkinci unsur; bu konuda kurumsal yapıların oluşturulmasıdır. Devamında; yasal çerçeve oluşturmak gelmektedir. Bununla birlikte teknik tedbirler de önem kazanmaktadır. Ulusal koordinasyon ve iş birliği gelişimi bu konudaki beşinci önemli unsuru oluşturmaktadır. Diğer unsurlar ise; uluslararası uyum ve iş birliğini geliştirmek, farkındalığı artırmak ve kapasite geliştirmektir (Ünver ve Canbay, 2010, s.99).

2.ABD'nin Siber Güvenlik Politikası

2.1.ABD'nin siber güvenlik stratejisinin tarihsel gelişimi

ABD güvenlik stratejileri kapsamında siber alanla ilgili olarak 1930'lu yıllarda teknolojik hamleler yapmaya başlamıştır. Bu yıllarda Alman Donanması'nın ENIGMA ismindeki kripto cihazından esinlenilerek SIGIBA adında bir cihaz üretilmiş ve II. Dünya Savaşı döneminde ENIGMA'nın üst versiyonu olan cihazın şifresini çözmek üzere çalışmalar yapılmıştır (Darıcılı, 2017, s.3). Diğer bir girişim ise 1958 yılında kurulan İleri Araştırma Projeleri Ajansı (Advanced Research Project Agency-ARPA)'dır. Kurumun oluşturulmasında Sovyet Sosyalist Cumhuriyetler Birliği-SSCB ile diğer alanlarda olduğu gibi bilimsel alanda da rekabet edilmesi etkili olmuştur. Bilim insanlarının bir araya getirilmesinin amaçlandığı bu proje aynı zamanda internet tarihinin başlangıcı olarak görülmüş ve ismi ARPANET olarak anılmıştır (Darıcılı, 2017, s.4). İngiliz ve Fransız ağlarıyla ARPANET'in birleştirilmesi sonucu ilk defa uluslararası boyut kazanan internetin, temel altyapı hizmeti de TELENET kamusal alanı ile gerçekleşmiştir. ABD'nin internet ağ sistemleri konusunda güvenliği dikkate almaya

başlaması, 1980'li yıllarda ARPANET'e yönelik gerçekleşen virüs sızıntısı sonucu meydana gelen elektrik kesintisi ile olmuştur. İlerleyen yıllarda tehditlerin artması sonucu askeri veri iletişimi için ABD Savunma Bakanlığı tarafından Militarynet (MILNET) adında yeni bir alt yapı oluşturulmuştur (Darıcılı, 2017, s.5). Siber teknoloji ile gerçekleştirilen ilk siber saldırı hadisesi de yine Soğuk Savaş yıllarında 1982'de yaşanmıştır. Rusya'nın Kanada'dan doğal gaz boru hatlarının kontrolünü sağlayan yazılımı çalma girişimi, ABD tarafından fark edilerek yazılıma Truva Atı virüsünün yüklenmesiyle tuzaklanmıştır. Virüslü yazılımın bozulması sonucu boru hatlarındaki akışın seviyesi bozulmuş ve Sibirya doğal gaz boru hattında patlama meydana gelmiştir (Sertçelik, 2015, s.31). Bu yıllarda siber savunma, siber saldırı, siber suç gibi kavramlar çok göz önünde bulunmazken teknolojik gelişmeler ve küreselleşme ile birlikte siber alandan daha çok söz edilmeye başlanmıştır. Öyle ki ilerleyen yıllarda ulusal güvenliğin temel alanlarından biri haline gelen siber güvenlik, ABD için özellikle 11 Eylül hadisesi sonrasında dikkate alınan unsurlar arasında yer alan önemli bir politika sahası olma özelliği taşımaktadır.

2.2.*Soğuk savaş sonrası siber güvenlik stratejisi*

Soğuk Savaş'ın sona ermesinin ardından birçok alanda olduğu gibi siber alan ve siber güvenlik kavramlarına yönelik yaklaşımlarda da değişimler meydana gelmiş, bu süreçte ABD'de siber güvenlik konusunda kurumsal altyapı oluşmaya başlamıştır. Siber güvenlik politikalarının şekillenmesinde başkan direktifleri, siber stratejik planlamalar etkili rol oynamıştır. Siber güvenlik gelişmeleri konusundaki ilk resmî belge niteliğinde olan başkanlık direktifi 1995 yılında yayımlanmıştır. 1997'de yayımlanan ilk resmi dokümanda ise kritik altyapılar tanımlanmıştır. Daha sonra meydana gelecek olan strateji ve doktrinlere temel oluşturacak olan belgede; iletişim, ulaşım sektörleri, kamu sağlığı alanı, enformasyon, acil müdahale altyapısı, bankacılık ve finans ve enerji ABD kritik altyapıları olarak belirlenmiştir (Darıcılı, 2017, s.6).

Güvenlik politikalarının şekillendirilmesine yönelik belgeler oluşturulurken bir yandan da kurumsal olarak gelişmeler yaşanmış ve 1998'de siber saldırılara karşılık verebilmek ve altyapıyı ilgilendiren tehditlerin bilgi koordinasyonunun sağlanması amacıyla Ulusal Altyapı Koruma Merkezi (NIPC) kurulmuştur. Merkezin Federal Soruşturma Bürosu (Federal Investigation Bureau-FBI) bünyesinde kurulması, ABD'nin siber tehdit algılamasının siber suçlara ve tehditlere yönelik tedbirlere odaklandığını göstermektedir (Demirel, 2012, s.91). Bu durum 11 Eylül saldırıları sonrasında değişerek siber güvenlik algısında dönüşüm yaşanması sonucu farklılaşmıştır. 9/11'den sonra siber güvenlik ulusal güvenliğin bir parçası olarak görülmeye başlanmıştır. Bu dönemde asimetrik tehditlerin öne çıkması söz konusu değişikliğe temel teşkil etmiş ve NIPC bünyesinde bulunduğu FBI'den ayrılarak 2002'de kurulan İç Güvenlik Bakanlığı (The Department of Homeland Security-DHS) kapsamına alınmıştır (Demirel, 2012, s.92).

FBI ve DHS'nin de içinde bulunduğu, siber güvenlik politikası kapsamında faaliyet gösteren kurumlardan oluşan üçlü bir yapıya sahip olan ABD, bu kurumlar ve alt kurumlarının yürüttüğü faaliyetler kapsamında siber güvenlik stratejisine şekil vermektedir. Söz konusu üçlü yapının diğer unsurunu Savunma Bakanlığı oluşturmaktadır. Resmi siber organizasyonu olarak da adlandırılan bu üçlü sistematik yapı, ülkedeki eyalet sistemi nedeniyle karmaşık bir görünüm ortaya koymakla birlikte ABD'nin siber güvenlik atılımları, uygulamaları ve stratejileri konusunda temel oluşturmakta ve kurumsal alt yapı dayanağı özelliği taşımaktadır (Darıcılı, 2017, s.7). Savunma Bakanlığı ABD'nin siber güvenlik algısının askeri yönünü ortaya koyan bir yapı niteliğinde karşımıza çıkmaktadır. 1947 yılında kurulan ABD'nin silahlı kuvvetlerinden sorumlu bakanlığın karargâhı, 11 Eylül'de zarar gören merkezi alanlardan biri olan Pentagon'dur. Savunma Bakanlığı barındırdığı kurumlar hasebiyle siber güvenlik stratejisinin önemli bir ayağını oluşturmaktadır. Bu kurumlar içerisinde şifre çözme, veri analizi, karşı

istihbarat gibi faaliyetlerde bulunan ve 1952 yılında kurulan Ulusal Güvenlik Ajansı (National Security Agency-NSA) öne çıkmaktadır (Darıcılı, 2017, s.8). Savunma Bakanlığı siber uzayı bir savaş alanı olarak görmüş ve "Siber Uzay Harekatları için Ulusal Askeri Stratejisi" belgesi ile bunu resmileştirmiştir. Belgeye göre siber uzay; elektromanyetik enerjinin kullanıldığı ağ sistemlerinden meydana gelen bir fiziksel etki alanı olarak tanımlanmıştır. Bu alanda hareket serbestisi sağlanması için ABD Hava Kuvvetleri Siber Komutanlığı kurulmuştur (Akyazı, 2013, s.218).

FBI'ın siber güvenlik açısından önemi casusluk faaliyetlerine karşı istihbarat oluşturması ile ilişkilendirilmektedir. FBI'ın önemli olmasını sağlayan temel özelliğini siber güvenlik stratejisinin uygulanmasında siber saldırılara karşı koyma görevi oluşturmaktadır. FBI kapsamındaki birimler; Siber Ulusal Güvenlik ve Siber Suç Bölümleri'dir (Darıcılı, 2017, s.10).

Üçlü siber organizasyonunun son unsuru olan DHS, terörle mücadele konusunda asıl yetkili olan kuruluş olma özelliğine sahiptir. 2002 yılında çıkarılan Kamu Güvenliği Yasası kapsamında kurulan DHS'nin siber güvenlik konusundaki amaçları; siber güvenliğin ilerletilmesi, kritik altyapıların korunması, kritik önemdeki kaynakların direncinin korunması, hükümetin iletişim gücünün sürdürülebilirliğini sağlamaktır (Başa, s.33). İzleme, acil müdahale ve güvenlikten sorumlu merkez ve birimlerden oluşan DHS'nin yedi gün yirmi dört saat işleyen bir mekanizması bulunmaktadır. DHS kapsamında siber güvenlik konusunda temel sorumluluğa sahip olan birim, Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi'dir. Ülke genelindeki siber olayların izlenmesinden ve karşılık verilmesinden sorumlu olan birim, özel ve resmi birimler arasındaki iletişim ve iş birliğini de sağlamaktadır. Kurum içerisindeki diğer acil müdahale ekipleri Ulusal Siber Güvenlik Birimi kapsamında yer almaktadır. Aynı zamanda siber güvenliğin sağlanmasına yönelik olarak Ulusal Siber Güvenlik Koruma Sistemi kullanılmaktadır (Darıcılı, 2017, s.9).

Siber güvenlik stratejisi bakımından ABD, siber güvenlik konusunda ilk kapsamlı belge niteliği taşıyan 2003 tarihli Güvenli Siber Uzay (Secure Cyberspace) belgesinin alt alanını oluşturan Siber Uzay Güvenliği Ulusal Stratejisi belgesinde temelde üç önceliğe dikkat etmektedir. İlk olarak, kritik altyapılara yönelik gerçekleşecek olan saldırıların önlenmesi gelmektedir. İkincisi; olası saldırılara yönelik güvenlik açıklarının giderilmesidir. Son önceliği ise; saldırıların yol açacağı zararların minimum düzeye indirilmesi oluşturmaktadır (The National Cyberspace Strategy, 2003, s.14). Belgede ulusal öncelik olarak da beş öncelik ön plana çıkarılmıştır. İlk öncelik siber saldırılara yönelik karşı koyma sisteminin geliştirilmesini amaçlayan ulusal siber uzay güvenliği yanıt sistemidir. İkincisi; ulusal siber uzay güvenliği tehdit ve güvenlik zafiyetlerini azaltma programıdır. Ulusal siber uzay farkındalık ve eğitim programı, ulusal güvenlik ve uluslararası siber uzay güvenliği iş birliği ve devletin siber uzay güvenliğini sağlamak diğer önceliklerdir (The National Cyberspace Strategy, 2003, s.15). ABD güvenlik stratejisinde siber güvenliğin önemi yıllar geçtikçe artmaya devam eden bir seyir izlemiş ve bu kapsamda atılan adımlarda gelişme yaşanmıştır. Bu adımlardan biri de 2009 yılında dönemin Başkanı Barack Obama tarafından oluşturulan Siber Uzay Politika Revizyonu'dur. Söz konusu belgede siber güvenlik sorumluluğu alan kurumlar arasında iş birliğinin sağlanması ve bütüncül bir yapıya sahip olması öngörülmüştür (Darıcılı, 2017, s.6). Aynı zamanda 2013 yılında siber güvenlik sistemlerinin geliştirilmesi amacıyla kritik altyapıların kritik alt yapı şirketleri ile ve endüstri ortakları ile birlikte adım atmaları ve gerekli stratejiler izlemeleri konusunda Başkan Obama talimat vermiştir (Kara, 2013, s.54). 2015 yılında ise siber saldırı düzenleyenler hakkında dava açılabilmesi için emniyet güçlerine fazla yetki verilmesi yönünde gelişmeler yaşanmış, konuyla ilgili yeni yasa tasarıları gündeme gelmiştir ("ABD Başkanı", 2015). Dönemin Ulusal Güvenlik Stratejisi'nde diğer belgelerden farklı olarak diğer güçlerin stratejisine de yer verilerek yeni oluşan tehditlerden söz edilmiştir. Bu kapsamda Rusya Federasyonu'nun siber güvenlik konusunda gücünün artması ve Çin Halk Cumhuriyeti'nin siber casusluk faaliyetleri ABD için büyük tehdit olarak ifade edilmiştir (Darıcılı, 2017: 7). Tehditlerin ciddi boyutta olduğunun düşünülmesi ABD'yi siber güvenlik konusunda operasyonel bir güç olma yoluna

yöneltmiş ve bunun dünya tarafından da fark edilmesi adına Nisan 2015'de kabul edilen ABD Savunma Bakanlığı Siber Strateji Belgesi ile ABD Silahlı Kuvvetleri siber alanda yeni görevlerle yetkilendirilmiştir. Siber bilgilerin korunması, askeri ve gizli operasyonların planlanması söz konusu görevler arasında bulunmaktadır (Darıcılı, 2017, s.7).

2.3. *Yakın dönem siber güvenlik stratejisi*

Donald Trump ile 2017'de ABD'nin yeni dönemi başlamış ve her alanda olduğu gibi siber güvenlik konusunda birtakım yenilikler yaşanmıştır. Kritik altyapıların korunması için siber güvenliğe 1,5 milyar dolar yatırım yapılmış ve her bakanlığın kendi siber güvenliğinden sorumlu olacağına karar verilmiştir ("Trump'tan Devrim", 2017). 2018 yılında imzaladığı Ulusal Siber Güvenlik Strateji Belgesi "saldırgan" olarak nitelendirilmiştir. Bunda, söz konusu belgede siber saldırılara karşı daha saldırgan adımlar atılmasının öngörülmesi etkili olmuştur. Siber suç işleyenlere yönelik ihbar ve yasal işlem konularında daha etkili sistemler oluşturulması gerektiği üzerinde durularak ABD'nin siber güvenlik konusunda küresel üstünlük tesis edilmesi, siber güvenliğin sağlanmasında normlar oluşturarak bu normlara küresel düzeyde uyulmasının sağlanması için çalışılacağının üzerinde durulmuştur ("Trump'tan Daha", 2018). Belgede siber alan için Amerikan halkı açısından ekonomi ve savunmadan ayrılmayan bir parça olarak bahsedilmiş, siber güvenlik ve savunmanın koordineli ve caydırıcı şekilde icra edilmesi gerektiği üzerinde durularak ihtiyaç duyulduğunda bilişim sistemlerine karşı kullanılan zararlı yazılımları ABD'ye karşı kullananların cezalandırılacağı ifade edilmiştir (The Department of Homeland Security, 2018, s.6). Ulusal beş temel öncelik varlığını korumaya devam etmiş 2018 tarihli Birleşik Devletler Anayurt Güvenliği Bakanlığı Siber Güvenlik Stratejisi Belgesi'nde de söz konusu öncelikler yinelenerek amaçları belirtilmiştir. Bu kapsamda önceliklerin amaçları; gelebilecek tehditleri en aza indirmek, siber tehditlere karşı ulusal güvenlik programını geliştirmek, ulusal saldırıları engellemek ve böyle bir durum söz konusu olduğunda uluslararası alanda tepki oluşmasını sağlamak, kritik altyapıları korumak, federal hükümetin bilgi sistemlerini korumaktır (The Department of Homeland Security, 2018, s.3). Aynı zamanda belgede saldırılara yönelik karşı cevap ve tehditlere karşı önlem açısından sekiz öncelikten ve eylemden söz edilmektedir. Tehditlere karşı eylemler genelde kamu ve özel sektör arasında iş birliğinin sağlanması ve siber uyarı ağlarının geliştirilmesine odaklanırken, yazılım açıklarını giderme, hukuki düzenlemeler yapma, aciliyet sistemlerinin güvenliği konuları tehditlere yönelik alınan önlemler arasında yer almaktadır (The National Cyberspace Strategy, 2003). Yine belgede kritik alt yapılar konusunda yedi kilit öneme sahip alandan söz edilmiştir. Bu alanlar; enerji ve güç, ulaşım, iletişim, sağlık, ulusal güvenlik, finans ve bilgi teknolojileridir (The White House, 2018, s.10).

Savunma Bakanlığı Siber Strateji Belgesi de ABD'nin siber güvenlik konusundaki öncelikleri ile ilgili bilgiler içeren bir diğer kaynak olarak öne çıkmaktadır. Rusya ve Çin'in büyük tehdit olduğunun belirtildiği belgede, özellikle Rusya ve Çin olmak üzere, Birleşik Devletler'in varlığına ve güvenliğine yönelik tehdit oluşturan ülkelere odaklanılacağının altı çizilmiştir. Aynı zamanda bir çatışma veya kriz söz konusu olduğunda bilgi toplamak ve askeri siber kapasiteyi artırmak için siber uzay operasyonlarının yapılacağından bahsedilmiştir. Geleceğe yönelik plan ve stratejilerden biri de; güvenliğin ve hem şimdi hem gelecekte askeri kapasiteyi artırmak için sistemlerin ve ağ bağlantılarının güçlendirilmesidir (The Department of Defence, 2018, s.1). Sürekli bir gelişim halinde olan siber stratejiler ABD'nin güvenlik gündeminde de yer almakla birlikte gitgide daha üst sıralara taşınmıştır. ABD; hükümet uygulamalarının, hayati önemdeki hizmet dağılımlarının daha güvenli olmasını sağlayan unsurun siber uzay olduğuna inanmaktadır (The Department of Homeland Security, 2018, s.27).

2.4. Stratejik siber olay örnekleri

Siber varlıkları etkileyen ve zarar görmelerine neden olan durumlar anlamına gelen siber olaylar elektronik ortamlardaki verilerin ele geçirilmesi, gizliliğin ve bütünlüğün ihlalinden oluşmaktadır (Sağıroğlu, 2018, s. 24). Yıllar içerisinde meydana gelen siber ataklar ve saldırılar devletlerin politikalarına etki ederek yeni adımlar atılmasını ve stratejilerin geliştirilmesini sağlamıştır. ABD siber güvenlik stratejisinin bugünkü halini almasında da önceki dönemlerde meydana gelen olayların etkisi kaçınılmaz olmuştur. Bunlardan biri 1990 yılında meydana gelen Körfez Savaşı'dır. İstihbarat birimi ile Irak ordusunun telsiz frekans sistemleri tespit edilerek iletişim sistemleri dinlenmiştir. Irak ordusunun iletişim sağlamak için denediği her yolun etkisiz hale getirilmesi sonucu Irak ordusu içerisinde haber alma konusunda ciddi bir sorun olmuş ve komuta kontrol sisteminin yıkılmasına yol açmıştır. Böylece siber güvenliğin savaşlar üzerindeki etkisini anlatan önemli bir örnek olarak Körfez Savaşı siber ortamın ele geçirilmesiyle kazanan olunabileceğini gösteren ilk savaş olmuştur (Kara, 2013, s.42). Bu dönemlerde bilgi ve iletişim güvenliği olarak adlandırılan siber güvenlik ilerleyen yıllarda bu alanda yapılan teşkilat ve teçhizat oluşumlarıyla bilişim güvenliği önlemlerine ilave bir katman olarak eklenmiş ve özellikle son yıllarda askeri ve sivil kurumların en üst düzey yönetimlerinin sorumluluğuna ve yetkisine alınmıştır. Bu kapsamda önemli olarak değerlendirilen bir siber olay örneği de ABD'nin Irak işgalinde meydana gelmiştir. II. Körfez Savaşı olarak da adlandırılan 2003 Irak işgalinde de ABD'nin siber alanda attığı bir adım işgalin kolayca gerçekleştirilmesine zemin hazırlamıştır. Iraklı subaylara ABD Savunma Bakanlığı e-posta hesabı üzerinden gönderilen bir mesaj ABD'ye işgal gerçekleştiğinde karşı koyacak güçlü bir orduyla karşılaşmamalarını sağlamıştır. Gönderilen mesajda Irak'ın işgal edileceği ve zarara uğramak istemiyorlarsa askeri araçları sırayla bırakıp gitmeleri istenmiştir. Birçok subayın gelen mesaja itaat edercesine hareket etmesi sonucu işgale karşı bir taarruz oluşmamıştır (Kara, 2013, s.45). Siber güvenliğin Savunma Bakanlığı'nca fazlasıyla ciddiye alınmasında etkili olan bir olay da 2007 yılında yaşanmıştır. Pentagon'un ağına sızmak için e-posta hesaplarına yabancı bilgisayar korsanları tarafından saldırı gerçekleştirilmiştir (Sertçelik, 2015, s.35). ABD siber güvenlik tarihinde yer eden bir gelişme de 2013 yılında yaşanmıştır. Ulusal Güvenlik Kurumu'ndan birinin birçok gizli belgeyi kamuya açıklaması sonucu, belgeler bir durumu ortaya çıkarmıştır. Belgeler ile Ulusal Güvenlik Kurumu'nun Google veri merkezleri arasındaki hatlarını dinlediği ve kişisel verileri elde ettiği iddia edilmiştir (Sertçelik, 2015, s.38). ABD'nin siber güvenlik politikasının bugünkü halini almasında yıllar içerisinde meydana gelen siber olaylarla birlikte değişen güvenlik algısı etkili olmuş ve alınan tedbirlere yansımıştır.

Siber güvenlik zafiyetleri sonucu meydana gelen aksaklıkların caydırıcılığı devletleri bu alanda yüksek güvenlik önlemleri almaya yönelik faaliyetlere odaklanmaya yönlendirmiştir. Teknik olarak ortaya çıkan aksaklıklar sonucunda bilgi ve iletişim sorunları meydana gelirken teknik sorunların yanı sıra diplomatik, siyasi ve ekonomik yansımalar da görülmektedir. Devletlerin gizli verilerinin ele geçirilmesi sonucu meydana gelebilecek karışıklıklar devletler arasında savaşa neden olan süreçlere zemin hazırlayabilecek güçlü etkilere sahiptir. Diplomatik ve siyasi krizlerin yanı sıra ülkeler kendilerine karşı gerçekleşen siber saldırıların etkilerini silmek ve yeniden düzenlemeler yapmak adına ekonomik olarak da sorunlar yaşamaktadırlar. Devletlerin teknik alandaki saldırılara maruz kalması bütün güvenlik sistemlerinin verilerinde meydana gelecek aksamalara yol açmakla birlikte gizliliği korunması gereken dataların yayılması ülkeler arası siyasi ve diplomatik krizlere sebep olabilecek etkiler meydana getirmektedir. Dijital topraklar olarak nitelendirilen siber alanın güvenliği ulusal bilgilerin, kişisel verilerin korunması bağlamında değerlendirilerek ülkelerin önemli değerleri arasında sayılmaktadır. Siber güvenliğin önemi ülkenin geleceği ile ilişkilendirilmesi hasebiyle elzem görülmektedir. Ulusal güvenliğin yanı sıra ticari imajı korumak ve rekabet gücünü sürdürmek de siber güvenliğin önemini artırmaktadır (Sağıroğlu, 2018, s.36-37).

Sonuç

Devletler, hükümetler, uluslararası sistem ve düzen için her daim elzem olan "güvenlik", "güvende olma" duygusu ve bu yönde yapılan çalışmalar gelişerek ve dönüşerek varlığını sürdürmüştür ve halen sürdürmektedir. Farklı boyutlarda ele alınarak askeri, ekonomik, toplumsal, ulusal ve uluslararası güvenlik anlayışları meydana gelmiş, çeşitlenerek gelişen bu anlayış devletlerin varlıklarını sürdürmek adına politikalarını şekillendirmesini sağlamıştır. Güvenlik anlayışını etkileyen birçok faktörden biri olan teknolojinin gelişmesi ve küreselleşme ile yeni bir boyut ortaya çıkmış ve internetin yaygın kullanımı ile devletlerin güvenliklerini sağlamaları adına yeni bir alan meydana gelmiştir. Siber uzay modern dönemde devletler için yeni bir mücadele alanı anlamına gelirken, siber güç, siber savaş, siber tehdit, siber istihbarat gibi birçok kavram da hayatımıza girmiştir. Siber uzayda etkili ve güçlü olmak ve gelecek saldırılara karşı hazırlıklı olmak, karşı koyabilmek amacıyla devletler siber güvenlik ve siber savunma politikaları geliştirmişlerdir. Soğuk Savaş döneminin rekabetinden siber alan da etkilenmiş Soğuk Savaş sonrası süreçte yine güçlenen, yükselen devletler arasında siber alan mücadele alanı olmaya devam etmiştir.

1945-1991 döneminde Sovyet Rusya-ABD rekabetinin etkisiyle siber güvenlik ABD için askeri alanda yer almış ve Federal Soruşturma Bürosu bünyesinde varlık göstermiştir. Soğuk Savaş'ın sona ermesi güvenlik anlayışını çeşitlendirirken siber güvenlik anlayışına da etki etmiş ve siber güvenlik ulusal güvenliğin bir alt dalı olarak görülmeye başlanmıştır. ABD siber güvenlik sisteminde üç önemli kurumun oluşturduğu bir yapı öne çıkmış ve yıllar içerisinde söz konusu yapı yenilenerek gelişmelere ayak uydurulmuştur. FBI, İç Güvenlik Bakanlığı ve Savunma Bakanlığı üçlüsünden oluşan bu yapı ABD'nin siber güvenliği hem askeri hem ulusal açıdan değerlendirdiğini ortaya koymaktadır. Zira Çin'in ve Rusya Federasyonu'nun siber alanda güçlenmesi ABD'yi siber güvenliği askeri alana taşımasına zemin hazırlamış, tehdit olarak görülen bu güçlere karşı ABD, mütecavizlere karşı saldırılara yönelik daha sert ve saldırgan şekilde karşılık verileceğini öngören politikaları agresif olarak nitelendirilmektedir. Değişen savaş yapısı, mücadele alanı ve algısı bugünün savaşlarını konvansiyonel silahlarla birlikte asimetrik etkiye sahip siber saldırı araçlarından oluşan hibrit savaşa dönüştürmüştür. Söz konusu yeni düzen teknoloji zemininde hayat bulan siber dünyada siber yöntemlerle rekabet edileceğinin göstergesidir. Dünya genelinde her alanda süper güç olduğu iddiasındaki ABD mücadelenin bu alanında da etkisini göstermek istemektedir. Bu kapsamda siber güvenlik politikasının yıllar geçtikçe daha önemli hale geldiği ve üst sıralarda yer aldığı anlaşılmaktadır.

Kaynaklar

ABD başkanı Obama'dan siber güvenlik paketi. (2015, 14 Ocak). BBC Türkçe https://www.bbc.com/turkce/haberler/2015/01/150113_obama_siber_guvenlik adresinden erişildi.

Akyazı, U. (2013). Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler. *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı* içinde (s.216-220). https://www.iscturkey.org/assets/files/2016/03/2013-paper105.pdf adresinden erişildi.

Anadolu Ajansı, (2018, 21 Eylül). *Trump'tan daha saldırgan siber güvenlik stratejisi.* https://www.ntv.com.tr/dunya/trumptan-daha-saldirgan-siber-guvenlik-stratejisi,ZZTiHD3DV0abezSnBGds4A adresinden erişildi.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovstive Technologies*, 1(1), 24-38.

Başa, Ş. ABD İç Güvenlik Bakanlığı. https://www.academia.edu /9830086/ adresinden erişildi.

Brauch, H.G. (2012). Güvenliğin yeniden kavramsallaştırılması: Barış, güvenlik, kalkınma ve çevre kavramsal dörtlüsü. Mustafa Aydın vd (Der.) *Uluslararası İlişkilerde Çatışmadan Güvenliğe* içinde (s.167-196). İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Çelik, S. (2018). Siber uzay ve siber güvenliğe multidisipliner bir yaklaşım. *Academic Review of Humanities and Social Sciences,* 1(2), 110-119.

Darıcılı, A.B. (2017). Demokrat parti hack skandalı bağlamında ABD ve RF'nin siber güvenlik stratejilerinin analizi. *Uluslararası Çalışmalar Dergisi,* 1(1), 1-24.

Demirel, M. (2012). *Asimetrik tehdit kavramı bağlamında 11 Eylül 2001 sonrası dönemde Amerika Birleşik Devletleri'ndeki siber tehdit algılamasının ve geliştirilen güvenlik politikalarının incelenmesi*. (Yayımlanmamış Yüksek Lisans Tezi). Kara Harp Okulu/Savunma Bilimleri Ensitüsü.

Department of Defence. (2018). Cyber strategy. https://afyonluoglu.org/siberguvenlik/world-css/ adresinden erişildi.

Ermiş, U. (2018). Bir güvenlik sorunu olarak siber uzay. TASAM. https://tasam.org/tr-TR/Icerik/50249/bir_guvenlik_sorunu_olarak_siber_uzay adresinden erişildi.

Güntay, V. (2014). Siber güvenliğin uluslararası politikada etki aracına dönüşmesi ve uluslararası aktörler. *Güvenlik Stratejileri,* (27), 79-111.

Göçoğlu, V., Aydın, M. (2019). Siber güvenlik politikası: ABD, Rusya ve Çin üzerine karşılaştırmalı bir analiz. *Güvenlik Bilimleri Dergisi,* 8(2), 229-252.

Habertobb. (2015). Siber güvenlik geleceği şekillendiriyor. *Ekonomik Forum.* Sayı: 251. http://haber.tobb.org.tr/ekonomikforum/2015/251/012_021_KAPAK_KONUSU.pdf adresinden erişildi.

Kara, M. (2013). *Siber saldırılar-siber savaşlar ve etkileri*. (Yayımlanmamış Yüksek Lisans Tezi*)*. İstanbul Bilgi Üniversitesi.

Kaya, A. (2012). *Siber güvenliğin milli güvenlik açısından önemi*. (Yayımlanmamış Yüksek Lisans Tezi*)*. Kara Harp Okulu/Savunma Bilimleri Enstitüsü.

Kurnaz, S., Önen, S.M. (2019). Avrupa Birliği'ne uyum sürecinde Türkiye'nin siber güvenlik stratejileri. *International Journal of Politics and Security*, 1(2), 82-103.

Özçoban, C. (2014). 21.*Yüzyılda ulusal güvenliğin sağlanmasında siber istihbaratın rolü*. (Yayımlanmamış Yüksek Lisans Tezi*)*. Harp Akademileri/Stratejik Araştırmalar Enstitüsü. İstanbul.

Özdemirci, F., Torunlar, M. (2018). Bilgi-değişim-siber güvenlik-bağımsızlık. *Bilgi Yönetimi Dergisi*, 1(1), 78-83.

Sağıroğlu, Ş. (2018). Siber güvenlik ve savunma: Önem, tanımlar, unsurlar ve önlemler Şeref Sağıroğlu ve Mustafa Alkan (Ed). *Siber Güvenlik ve Savunma* içinde (s. 21-45). Ankara: Grafiker Yayınları.

Sertçelik, A. (2015). Siber olaylar ekseninde siber güvenliği anlamak. *Medeniyet Araştırmaları Dergisi*, 2(3), 25-42.

TC. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. 2016-2019 Ulusal Siber Güvenlik Stratejisi. https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf adresinden erişildi.

The White House. (2003). The National Strategy to Secure Cyberspace. https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf adresinden erişildi.

The White House. (2018). National Cyber Strategy of The United States of America. https://afyonluoglu.org/siberguvenlik/world-css adresinden erişildi.

Trump'tan devrim gibi karar: Her bakanlık kendi siber güvenliğinden sorumlu olacak. (2017, 25 Mart). https://siberbulten.com/uluslararasi-iliskiler/trumpdan-devrim-gibi-karar-her-bakanlik-kendi-siber-guvenliginden-sorumlu/ adresinden erişildi.

US. Department of Homeland Security. (2018). Security strategy. https://afyonluoglu.org/siberguvenlik/world-css adresinden erişildi.

Ünver, M., Canbay, C. (2010). Ulusal ve uluslararası boyutlarıyla siber güvenlik. *Elektrik Mühendisliği,* Sayı 438, 94-103.

Yılmaz, B.A. (2020). Siber terörizm ve değişen istihbarat anlayışı. *Anadolu Strateji Dergisi,* 1(1), 65-81.