NATO'NUN YENİ OPERASYON ALANI: SİBER UZAY

Doğan Şafak POLAT*

Öz

NATO (Kuzey Atlantik Antlaşması Örgütü), üye ülkelerin ortak savunma yeteneklerini geliştirmek, toprak bütünlüklerini, siyasi bağımsızlıklarını ve güvenliklerini korumak maksadıyla 4 Nisan 1949 tarihinde kurulmuştur. Bu husus NATO Anlaşma'sının 5. Maddesi'nde de açıkça ifade edilmiştir. 21. yüzyılda teknolojik gelişmeler sonucunda güvenlik parametreleri değişmiş; kara, deniz, hava ve uzay yanında beşinci bir alan ortaya çıkmıştır. Bu alan siber uzay (cyber space) alanı olarak ifade edilmektedir. Siber uzayda yapılan saldırılara karşı mücadele oldukça güç olup tek bir devletin kapasitesini aşmakta ve müşterek mücadeleyi zorunlu kılmaktadır. Başlangıçta bir savunma örgütü olarak kurulan NATO, geçen süreçte üye devletlerin de onayıyla Stratejik Konsepti'ni değiştirmiş ve Soğuk Savaş sonrası bir güvenlik örgütü haline gelmiştir. NATO, siber uzayda üye devletlerin ihtiyaçlarına cevap verecek şekilde bünyesinde çeşitli kurumlar oluşturmakta; edinilen tecrübe, birikim ve yeteneklerini de üye devletler ile paylaşmaktadır. Siber uzayda ortaya çıkan/çıkabilecek tehditlere karşı NATO bünyesinde alınan önlemler ve bu maksatla yapılan çalışmalar devamlılığı gerektirmekte; İttifak'a üye devletlerin işbirliğini, bilgi ve teknoloji paylaşımlarını zorunlu kılmaktadır.

Anahtar Kelimeler: *Siber Güvenlik, Siber Alan, NATO, Müşterek Siber Güvenlik Mükemmeliyet Merkezi (CCDCOE), Siber Operasyonlar Merkezi (CYOC)*

NATO'S NEW OPERATION DOMAIN: CYBER SPACE

Abstract

NATO (The North Atlantic Treaty Organization) was established on April 4, 1949 to develop the common defense capabilities of member countries and to protect their territorial integrity, political independence and security. This is clearly stated in Article 5 of the NATO Treaty. As a result of technological developments in the 21st century security parameters have changed; a fifth field has emerged besides land, sea, air and space. This field is referred to as cyber space. The struggle against attacks in cyber space is very difficult, and exceeds the capacity of a single state and necessitates fighting in cooperation. NATO, which was initially established as a defense organization, changed its Strategic Concept with the approval of the member states and became a security organization after the end of Cold War. NATO establishes various institutions in the cyber space to meet the needs of the member states, and it shares its experience, knowledge and skills with the member states, as well. The measures taken and the work carried out for this purpose within NATO against the threats that may arise in the cyber space require continuity, and the cooperation of the member states and information and technology sharing become a must.

Keywords: *Cyber Security, Cyber Space, NATO, Cooperative Cyber Defence Centre of Excellence (CCDCOE), Cyber Operations Center (CYOC).*

* Dr. Öğretim Üyesi, İstanbul Arel Üniversitesi, İİBF, Uluslararası İlişkiler Bölümü, doganpolat@arel.edu.tr, ORCID: 0000-0003-0786-1789

Makale Geliş Tarihi: 30.09.2019 Makale Kabul Tarihi: 27.01.2020

GİRİŞ

Harbin kara, deniz, hava ve uzay olmak üzere dört boyutu vardır. Kimi uzmanlarca kara, hava, deniz ve uzaydan sonra beşinci boyut olarak değerlendirilen siber uzay (cyber space) diğer dört boyutu da etkileme kapasitesine sahip olup günümüzde harbin ayrılmaz bir bileşeni olarak değerlendirilmektedir. Siber uzay kavramı "birbiriyle bağlantılı sistem, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için" kullanılmaktadır (Libicki, 2009: 12-13). Siber saldırılar bir ülkenin kritik olarak kabul edilebilecek haberleşme/bilişim sistemlerine, enerji ve ulaşım ağlarına, askeri komuta ve kontrol sistemlerine zarar verecek ölçüde, asimetrik bir muharebe yöntemi olarak ortaya çıkmaktadır. Teknolojik gelişmeler paralelinde siber saldırılar daha yaygın, hızlı, çok karmaşık ve zarar verici hale gelmiştir. Bunun neticesinde siber güvenlik konuları devletleri daha fazla meşgul etmeye başlamıştır. Devletler siber tehdit ve tehlikelerin oluşumundan önce bunlara karşı önlemler almaya çalışmaktadırlar. Devletlerin yanında savunma örgütünden güvenlik örgütüne dönüşen ve geniş bir bilişim altyapısına sahip olan NATO da siber uzayın güvenliği maksadıyla çeşitli çalışmalar yürütmektedir. NATO'nun bilişim altyapısı Brüksel'deki merkezi ile dünyanın çeşitli bölgelerinde askeri birliklerin bulunduğu 60'tan fazla NATO operasyon sahasını kapsamaktadır. 100.000'den fazla asker ve sivil personel NATO ağlarına bağlantılıdır. Bu durum son on yılda NATO'nun giderek daha fazla siber saldırıların hedefi olmasına yol açmaktadır. NATO siber savunma sistemleri her gün NATO ağlarına karşı yapılan basitten karmaşığa çok sayıda siber saldırıyı tespit etmekte ve bunlara engel olarak bilişim sistemlerinin kesintisiz olarak çalışmasına çaba göstermektedir.

Bu çalışmanın amacı, içinde bulunduğumuz yüzyılda siber güvenliğin önemine vurgu yaparak NATO'nun siber tehditlerle mücadelesini ortaya koymaktır. Bir zincirin sağlamlığının en zayıf halkasının sağlamlığı kadar olduğu dikkate alındığında, NATO'nun da siber güvenlik konusunda yetkinliğinin en zayıf üye devletin yetkinliği kadar olduğu çıkarımı yapılabilir. İttifak, Soğuk Savaş sonrasında 2000'li yıllarla birlikte giderek önem kazanan siber alan ile ilgili çalışmalarda önemli mesafeler kat etmiş olsa da her üye devletin siber tehditlerle mücadele kapasitesinin aynı olduğunu söyleyebilmek oldukça güçtür. Çalışma, iki ana bölümden oluşmaktadır. Birinci bölümde siber uzayla ilgili olarak siber, siber tehdit, siber uzay ve siber güvenlik gibi kavramlar ele alınacaktır. İkinci bölümde ise kronolojik olarak siber güvenlik konusunda NATO'nun almış olduğu kararlara ve yapmış olduğu çalışmalara yer verilerek çalışma sonlandırılacaktır.

1. SİBER İLE İLGİLİ KAVRAMLAR

Siber terimi, ilk defa sibernetik kelimesinin kısaltması olarak Amerikalı bilim adamı Norbert Weiner tarafından 1948 yılında yayımlanan "Sibernetik ya da Hayvanlarda ve Makinelerde Kontrol ve İletişim (Cybernetics, or Control and Communication in the Animal and Machine) başlıklı kitapta kullanılmıştır (Whittaker, 2004: 4). Söz konusu terim 1958 yılında, canlılar ve/veya makineler arasındaki iletişim disiplinini inceleyen Matematik ve Sibernetik biliminin öncüsü sayılan Fransız Louis Couffignal tarafından da kullanılmıştır. Daha sonra bilişim alanında kullanımına devam edilmiştir (Çolak, 2011: 65). Siber uzay terimi (cyber space) ise, Kanada'lı William Gibson tarafından ilk defa 1982 yılında yazdığı "Burning Chrome" adlı eserinde kullanmıştır (Bıçakçı, 2010: 106). Gibson, "Neuromancer" adlı bilim kurgu romanında (Gibson, 1984) siber uzayı "bilgilerin elektromanyetik dosyada oluşturulması ile dünyanın her yanına farklı sistemler aracılığıyla dağıtılması ve bilgiye erişim sağlanılan sanal ortamların bütünü" olarak tanımlanmıştır (Çakmak ve Altunok, 2009: 25-26).

1.1. Siber Uzay

Soğuk Savaş döneminde ABD'de uzay, füze savunma ve nükleer silahlarının testlerinin tespiti maksadıyla 1957 yılında İleri Araştırma Projeleri Ajansı (Advanced Research Projects Agency/ARPA) kurulmuştur. 1960'lı yılların başında ise Savunma Araştırma Projeleri Ajansı (Defence Advanced Research Projects Agency/DARPA) kurulmuş; 1970'li yılların ortasından itibaren bu kurumun çalışma alanı ve yetkinliği geliştirilmiştir (Van Atta, 2018: 12). 1962 yılında ise ARPANET tasarlanarak hayata geçirilmiş ve böylece siber uzayın temeli atılmıştır. ARPANET, Dağınık Servis Engelleme Saldırıları (DDoS)'na karşı dayanıklı olarak tasarlanmıştır (Yılmaz ve Salcan, 2008: 35). 1977 yılına gelindiğinde ise kullanıcı sayısı artan ARPANET, üniversite, sivil sektör ve devlet araştırma faaliyetlerini birbirine bağlayan ulusal bir ağ haline gelmiştir (Pierce, 2018: 62). 1970'li yıllardan itibaren söz konusu ağdaki sunucu sayısının artırılmasıyla birlikte daha fazla bilgisayar ARPANET'e bağlanmıştır. Sistemdeki kullanıcı sayısının giderek artması nedeniyle yavaşlayan sistemi hızlandırmak maksadıyla çeşitli yazılım ve donanım düzenlemeleri yapılmıştır.

1980'lerde ARPANET'in ticari sürümü olarak değerlendirilen internet hızla büyümüş ve 1988 yılına kadar yaklaşık 60.000 internet bağlantılı bilgisayara hizmet verir hale gelmiştir (Pierce, 2018: 63-65). ARPANET'nin kullanıcı sayısının kısa sürede artması ve ağın ABD sınırları dışına açılımı güvenlik

sorunlarını da beraberinde getirmiştir. Bu süreçte en önemli siber saldırı 2 Kasım 1988 tarihinde gerçekleşmiştir. İnternete bağlı sistemlerin yaklaşık yüzde 10'unda Morris solucanı hızla yayılmış ve sistemi olumsuz olarak etkilemiştir. ARPANET'teki tehditlerin artması üzerine, ABD Savunma Bakanlığı, söz konusu ağı korumak için çeşitli çalışmalar başlatmıştır.

1990'lı yıllarda, ABD Savunma Bakanlığı, ARPANET'in askeri operasyonları için kritik öneme sahip olduğunu kabul ederek bir taraftan ağ güvenliği ile ilgili çalışmaları arttırmış, diğer taraftan ise hızlı bir şekilde askeri bilişim sistemlerini, bilgisayar ağları üzerinden birbirleriyle irtibatlandırmıştır. Böylece her türlü yazılım, donanım ve iletişim alt yapısından meydana gelen ve birbirine bağlı ya da bağımsız bilgi sistemlerinin oluşturduğu sayısal ortam olan siber uzay oluşmuştur. Siber uzayın henüz üzerinde anlaşmaya varılmış bir tanımı bulunmamakla birlikte siber uzay kavramı, birbiriyle irtibatlı bir zaman bağımlı bilgi sistemleri kümesini ve bu sistemlerle etkileşim içinde bulunan kullanıcıları ifade etmek için kullanılmaktadır (Ottis ve Lorents, 2010: 267).

Siber uzay, sadece internet ve ona bağlı bilgi sistemlerini değil internete girmeyen bütün bilgi sistemlerini de kapsamaktadır (Çiftçi, 2013: 5). Siber uzay kavramındaki uzay terimi ise sonsuzluğu ifade etmektedir. Son dönemde ortaya çıkan Nesnelerin İnterneti (Internet of Things/IoT) kavramıyla siber uzayın sınırları bilgisayarların dışına çıkarak kamu ve özel sektör binalarına, evlere, arabalara kadar ulaşmıştır.

1.2. Siber Savaş

İnsanlık tarihi boyunca en eski savaşlar kara ve denizlerde gerçekleşmiştir. 20. yüzyılın başından itibaren havacılık alanındaki gelişmeler neticesinde bu durum değişmiş ve hava da yeni savaş alanı olarak ortaya çıkmıştır. 1950'lerden itibaren ise dünyadaki süper güçler arasındaki yeni savaş alanı uzay olmuştur. 21. yy'dan itibaren meydana gelen teknolojik gelişmeler neticesinde bilişim sistemlerindeki yenilikler artmış ve siber savaş tanımlaması yapılmaya başlamıştır(Arquilla ve Ronfeldt, 2001: 2-7). Beşinci savaş alanı olarak kabul edilen siber uzay, diğer dört alanın yanında daha fazla öne çıkmaya başlamıştır (Murphy, 2010). Bunun nedeni diğer dört alanın bilişim sistemlerini (yazılım ve donanım) giderek daha fazla kullanmaları ve siber uzaya bağımlı hale gelmeleridir. Bilgi sistemlerinin yanında bu sistemleri birbirine bağlanmasını sağlayan iletişim araçları (kablo vs.) da bu yeni savaş alanının parçalarını oluşturmaktadır (Clarke ve Knake, 2011: 43-44).

Siber savaş, kuralsız bir şekilde siber silahlar kullanılarak yürütülen asimetrik veya hibrit yaklaşımların kullanıldığı savaş şeklidir. Askeri yapıların tek başına değil sivil altyapılar ile bağlantılı olması nedeniyle siber uzaydaki bu saldırıların, askeri yapılarla sınırlı kalmadığı da bir gerçektir (Ottis, 2010: 178). Siber savaş nedeni sayılabilecek saldırının gerisindeki saldırgan devlet genellikle tespit edilememektedir (Standler, 2002). Siber savaşta amaç, "sahip olunan siber varlıkları; ulusal çıkarlar ve menfaatler çerçevesinde korumak için karşı tarafın kritik bilişim sistemlerine zarar vermek, hizmetlerini durdurmak veya bozmak için bir başka ülkenin bilişim sistemlerini yavaşlatmak, bozmak, hizmetini aksatmak veya ele geçirmek" olabilir (Clarke ve Knake, 2011: 132). Siber uzayda bilgiye erişim coğrafi sınırlardan bağımsız olarak sürekli hızlanmıştır (Çiftçi, 2013: 8-9). Bu durum dışarıdan gelen/gelebilecek tehditlerin ve saldırıların da artmasına yol açmıştır.

Üç tür siber saldırı silah olarak kullanılır. Bunlar sentaktik saldırılar, semantik saldırılar ve karışık saldırılardır (Brenner ve Goodman, 2002: 27-42). Sentaktik saldırıların hedefi bilgisayar işletim sistemleri olup, zararlı kodlar/yazılımlar (Özdemir, 2007), Dağınık Servis Engelleme Saldırıları (DDoS) (Amiri ve Soltanian, 2015:7-12) ve sisteme girmek (bilgisayar korsanlığı-hack)(Rogers ve Devost, 2005: 5-10) şeklinde yapılan saldırılardır. "Semantik saldırılar, bilgisayarların işletim sistemini hedef almazlar, bunun yerine bilgisayar kullanıcısının ulaştığı bilginin doğruluğunu hedef alırlar. Sistem sorunsuz bir şekilde çalışmasına rağmen içerdiği bilgiler doğru değildir. Bu saldırılar, özellikle resmi internet sitelerinin ya da kritik altyapı tesislerinin sistemlerini hedef aldığında ciddi sonuçlar doğurabilir. Nükleer tesisteki bir sistemin hatalı olarak elektriği kesmesi ya da havaalanında kullanılan trafik kontrol sisteminin doğru bilgi vermemesi sonucu meydana gelebilecek hatalı yönlendirmeler örnek olarak gösterilebilir. Karışık saldırılar ise sentaktik ve semantik saldırıların birlikte icra edilmesidir. Kritik işletim sistemlerinin hatalı bilgi ile beslenerek etkisiz hale getirilmesi karışık saldırıya örnek olarak gösterilebilir" (Brenner ve Goodman, 2002: 31-41).

Günümüzde siber uzayda asimetrik savaşlar devam etmekte ve siber tehditler devletler açısından büyük tehlike arz etmektedir. Hem kişiler ve şirketler hem de devletler, sıklıkla zararlı yazılım, botnetler, DDoS saldırıları, virüsler, truva atları, bilgisayar sistemleri zayıflıkları, ağ savunmasızlık problemleri, ihlaller, bilgi hırsızlıkları, kimlik hırsızlıkları vb. siber uzaydaki problemlere ve siber saldırılara maruz kalmaktadırlar. Örneğin ABD'de görülen "NIMDA" isimli saldırı, kritik

altyapılarda yıkıcı bir tahribat bırakmıştır. NIMDA, bilgisayar solucan ve virüsünün karışımı olan bir otomatik siber saldırı olarak tasarlanmıştır. İnanılmaz bir hızla tüm ülkeye yayılarak 86.000 bilgisayara saldırıda bulunmuştur (Yılmaz ve Salcan, 2008: 35-43). Siber tehditler çeşitlenerek artmakta ve devletleri gelecekte büyük tehlikeler beklemektedir. 2014 yılında yayınlanan Pew Araştırma Merkezi (Pew Research Center)'nin raporuna göre, "araştırmaya katılan 1.600 teknoloji uzmanının 3'te 2'si 2025 yılında büyük maddi kayıp ve can kaybının olacağı bir siber savaş beklediklerini ifade etmişlerdir" (Kshetri, 2016: 54).

1.3. Siber Terörizm

Siber terör, 1980'lerde Barry Collin tarafından türetilen bir kavramdır (Gedik, 2018: 34). Siber terörizmin birçok tanımı yapılmıştır. Siber terörizm, "terörist faaliyetlerin siber alan kullanılarak gerçekleştirilmesi olarak ya da terör örgütlerinin siber alanı araç olarak kullanmaları" olarak tanımlanabilir (Kravasin, 2000). Siber terör, "belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla" kullanılır (Wilson, 2003: 4). Başka bir tanıma göre siber terörizm, "politik veya sosyal hedeflerin gerçekleştirilmesi için bir devleti veya vatandaşlarını aşağılamak veya korkutmak üzere bilgisayarlara, ağlara veya bilgilerin depolandığı yerlere gerçekleştirilen kanunsuz saldırı veya saldırı tehditleri" olarak ifade edilmiştir (Denning, 2000). Siber terörizm, "bilgisayar ve iletişim teknolojisi kabiliyetlerinin politik olarak motive olmuş ulus-altı gruplar veya gizli ajanlar tarafından şiddet, bir toplumu etkilemek veya bir hükümetin politikalarını değiştirtmek maksatlı olarak silah veya hedef olarak kullanılması" şeklinde de tanımlanabilir (Andress ve Winterfeld, 2011: 198). FBI ise siber terörizmi, "alt-ulus grupları veya gizli örgütler tarafından savaşçı olmayan hedeflere karşı şiddetle son bulan bilgi, bilgisayar sistemleri, bilgisayar programları ve verilere karşı önceden planlanmış siyasi güdümlü saldırı" olarak tanımlamıştır (Singer ve Friedman, 2018: 134-135).

Terör örgütlerinin kullandıkları yöntemlerin çeşitliliği, eylemlerin zaman ve mekânlarının öngörülememesi, gelişen teknolojinin terör örgütlerine sağladığı avantajlar, terörizm kavramını da değiştirmiştir. Terör örgütleri, siber terör aracılığı ile devletlerin bilişim sistemlerini yasa dışı yollarla ele geçirmeye ve devlet kurumlarının alt yapılarına zarar vermeye çalışmaktadırlar. Bunun yanında siber teröristler, toplum düzenini bozmak maksadıyla ekonomik ve sosyal alanda da saldırılar gerçekleştirerek vatandaşların tedirgin olmalarını sağlarlar (Hatipoğlu, 2017: 165).

Teröristler, klasik yöntemlere oranla çok daha ucuz olması; ani ve beklenmeyen saldırı ile düşmanı hazırlıksız yakalaması ve savunma imkânı vermemesi; tanınma, bilinme olasılığının olmaması; sınırlar ötesine geçişin çok kolay olması gibi nedenlerden dolayı siber terörü tercih ederler. Ayrıca siber terörün bir medya potansiyeli olması da tercih edilmesini sağlamaktadır (Heickerö, 2014: 555). Terör örgütleri propaganda amacıyla da siber yeteneklerini kullanmakta ve ideolojilerini geniş mecralara taşımaktadırlar. Terör örgütleri web siteleri üzerinden yardım kuruluşu kisvesi altında örgüte finans ve insan kaynağı sağlayarak etki alanlarını artırmaya çalışmaktadırlar (Schweitzer, Siboni ve Yogev, 2011: 42).

İnternet, kimliklerini ve bulundukları yeri gizleyen teröristler (Ottis, 2011: 34) tarafından iletişim kurmak, hedef belirlemek ve örgüt için istihbarat toplamak için kullanılmaktadır (Schweitzer vd., 2011: 41-42). Teröristler, genel olarak internet aracılığı ile iletişim kurmakta ve yine internet üzerinden örgüt içi eğitim ve yönetim sağlanmaktadırlar (Kara, 2013: 6-7). Böylece terör örgütleri benimsedikleri ağ tabanlı örgüt yapısı ile örgüt içi iletişim koordinasyon sağlamakta, eylemlerini oluşturdukları bu ağ üzerinden planlayıp icra etmektedirler (Koybko, 2015: 159-161). Son dönemde El Kaide ve IŞİD/DEAŞ gibi terör örgütleri interneti etkin olarak kullanmakta ve uluslararası güvenliği tehdit etmektedirler. Siber uzayın terör örgütleri tarafından etkin olarak kullanılması ve siber saldırılar gerçekleştirmeleri karşısında devletler zor duruma düşmektedirler (Gökçe, Şahinaslan ve Dinçel, 2014: 215). Ayrıca birçok terör uzmanının da belirttiği üzere yalnızca siber terörizmle mücadele etmekle görevli kurum, kuruluş ve uzmanların sayılarının yetersiz oluşu da mücadelede zafiyet yaratmaktadır (Brenner, 2007: 468-469).

1.4. Siber Güvenlik

Siber güvenlik, bütünlük, gizlilik ve erişilebilirlik prensipleri ışığında siber uzayda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar ve teknolojilerin bütünü olarak ifade edilmektedir (Hill, 2015: 119-134). Siber güvenlik kavramı kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır. Siber güvenlik, kurum kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlar (Çiftci, 2013: 8). Siber tehditler birçok gelişmiş devlet

tarafından milli güvenliğe karşı en büyük tehditler arasında görülmeye başlanmıştır. Ancak çok gelişmiş teknolojiye rağmen bir siber saldırının ne zaman yapılabileceğini tahmin etmek oldukça güçtür. Siber tehdit unsurlarının terör örgütleri tarafından da kullanılmaya başlaması ülkeleri yeni stratejiler belirlemeye ve daha fazla tedbir almaya itmektedir (Güntay, 2017: 88). Söz konusu alanın büyüklüğüne karşı siber saldırıları gerçekleştirecek unsurların büyük olmasını gerektirmez. Siber saldırılar asimetrik saldırılar olarak kabul edilir ve saldırganlar ne kadar küçük ise o kadar avantajlı olurlar (Geers, 2010: 15). Siber uzay diğer harekât alanlarından farklı olarak daha çok teknik (yazılım ve donanım) konuları içermesi nedeniyle askerlerden çok özel sektörün hâkim olduğu bir alandır. Bu nedenle siber güvenlik konularında askerler ile teknik personelin (özel sektör, üniversite) işbirliği içinde çalışmaları önem arz etmektedir.

Teknolojik gelişmelerle birlikte ortaya çıkan siber tehditler karşısında devletler güvenlik ihtiyaçlarının karşılanması ve menfaatlerinin devam ettirilmesi kapsamında önemli sıkıntılar yaşamaktadırlar. Siber saldırın tamamına yakınının kritik öneme sahip altyapı sistemlerine ve bilişim sistemleri üzerinde depolanan belge ve bilgilere karşı yapılmış olması devletlerin siber uzay güvenliği konusuna daha fazla yatırım yapmalarını ve işbirliği içinde hareket etmelerini zorunlu kılmaktadır. Özellikle Soğuk Savaş sonrası ortaya çıkan teknolojik gelişmeler paralelinde artan siber tehditler karşısında NATO, ağlarını ve operasyonlarını, devamlı olarak korumak için çaba göstermekte; siber güvenlik konusu ise NATO'nun en önemli gündem maddelerinden birisini teşkil etmektedir.

2. SİBER GÜVENLİK VE NATO

Soğuk Savaş sonrasında NATO, sahip olduğu güç temelinde devamlılığını sağlayacak değişiklikleri gündeme getirme ihtiyacı duymuştur. Bunun sonucunda "Stratejik Konsept" değişikliği gündeme gelmiş ve NATO için yeni görev alanları belirlenerek İttifak'ın devamlılığına karar verilmiştir (Hasgüler ve Uludağ, 2005: 204-209). 1990 Londra Zirvesi'nde "alan dışı" kavramıyla tehdit alanının ve içeriğinin genişlemesine dikkat çekilmiş ve Kuzey Atlantik bölgesi dışında da barış ve güvenliği bozabilecek tehditlere karşı mücadeleyi esas alan bir örgüt olma yolunda adımlar atılmıştır. 7-8 Kasım 1991 tarihleri arasında gerçekleştirilen Roma'daki Zirve'sinde değişen güvenlik anlayışı kapsamında "Yeni Stratejik Konsept" kabul edilmiş ve Kuzey Atlantik bölgesi dışından da gelecek tehditlerle mücadele edilebilmesi maksadıyla sorumluluk sahası genişlemiştir (Peksarı, 2007: 53).

Aralık 1994'te Rus birliklerinin Grozni'ye girmeleri ile Çeçenler başta internet olmak üzere bütün medya araçlarını kullanmış ve bilgi savaşının ilk örneklerini vermişlerdir (Bıçakçı, 2012: 205-226). Siber uzayın etkisini anlamakta geciken Ruslar, bir süre sonra bu saldırılara karşı çeşitli siteler açarak cevap vermişlerdir (Petit, 2003). Bu dönemde siber uzayın öneminin farkında olan NATO, Siber Savunma ve Yönetim Kurulu (Cyber Defence and Management Board /CDMB) ve Askeri Otoriteler ve Muhabere ve Bilgi Sistemleri Ajansı (Military Authorities and Communications and Information Agency /MACIA) gibi oluşumlar meydana getirmiştir. Üye ülkelerin ağ yapısı ve askeri yeteneklerinin farkı nedeniyle NATO Ağ ile Etkinleştirilmiş Güç Programı (Network-Enabled Capability/NNEC) ve Ağ Merkezli Savaş (NCW) için bilişim alt yapısının oluşturulmasına önem verilmiştir. Bu kapsamda 1 Haziran 1996 tarihinde NATO İstişare, Komuta ve Kontrol Ajansı (NATO Consultation, Command and Control Agency/NC3A) kurulmuştur. Ajansın amacı, teknolojik gelişmeleri takip etmek olarak belirlenmiştir. NC3A yapısı içinde siber güvenlik ve bilgi paylaşımı sağlanması maksadıyla görevli bir bölüm de yer almaktadır.

Yeni kurulan bu kurumlar "ortak savunma için müşterek planların tasarlanması; askeri kuvvetlerin görev yapabilmesi için gerekli altyapı ve tesislerinin kurulması; müşterek eğitim programları ve tatbikatların düzenlenmesi konularında daimi bir danışma ve işbirliği olanağı sunmaktadır" (Ada ve Çakır, 2017: 637). Dönemin değişen tehdit yapılarına uygun olarak NATO, ortaya çıkması muhtemel hibrit çatışmaların en önemli unsuru olan siber savaş kabiliyetini edinmek maksadıyla çeşitli toplantılar düzenlemiştir. İlk aşamada askeri komuta-kontrol ağları ve sistemleri siber savaş gereklerine göre düzenlenmeye başlanmıştır. NATO'nun 1998'de düzenlediği "Harekât Sistemlerine Enformasyon Teknolojilerinin Uygulanması" ve 1999'da düzenlediği "21. Yüzyılda NATO Enformasyon Sistemlerini Korumak" başlıklı toplantıları, "NATO'nun yeni döneme uyum sağlama çabasının yansımaları olarak kabul edilebilir" (Bıçakçı, 2016: 205-226). Çünkü 1999 yılında, Sırp hedeflerinin bombalanması sırasında Sırp bilgisayar korsanları tarafından NATO karargâhına ve üye ülkelerin askeri haberleşme sistemlerine çeşitli siber saldırılar düzenlenmiştir.

NATO'nun 50. Kuruluş yılı olan 1999 yılında Washington Zirvesi gerçekleştirilmiştir. Söz konusu Zirve sonrası açıklanan bildiride İttifak'a karşı geniş çaplı bir saldırı ihtimalinin kısa vadede gerçekleşebileceği, ittifak üyelerinin güvenliklerinin, askeri ve askeri olmayan tahmini güç birçok risklerle karşı karşıya

bulunduğunu bildirilmiştir (Pulat, 2002: 38). Bu kapsamda etkin bilgi sistemlerine sahip olunmasının İttifak'ın savunma gücünü arttıracağı vurgulanmıştır (NATO, 1999a). Zirve'de kabul edilen "Yeni Stratejik Konsept"te teknolojinin hızla yayılması ve silah üretim bilgilerine kolaylıkla erişilebilmesi nedeniyle devletler yanında devlet-dışı aktörler de tehdit algısına dâhil etmiştir. Söz konusu Konsept ile birlikte NATO, Hibrit Savaş kavramını benimsemiş ve devlet ve devlet-dışı unsurların İttifak'ın bilgi sistemlerine karşı çeşitli operasyonlar düzenleyerek zarar verebileceği ifade edilmiştir (NATO, 1999b). 1999 Zirvesi'nden hemen sonra, devlet ve hükümet başkanlarının katılımıyla Washington'da düzenlenen "21. Yüzyılda İttifak" başlıklı bir toplantı gerçekleştirilmiştir. Bu çerçevede etkili enformasyon sistemlerine sahip olunmasının savunma gücünü arttıracağı dile getirilmiştir (NATO, 1999b).

11 Eylül sonrasında en çok tartışılan konulardan birisi de NATO'ya ya da Müttefiklere karşı yapılabilecek Dijital Felaket ya da Dijital 9/11 senaryosu olmuştur (Bıçakçı, 2014: 119). Her ne kadar ilk DDoS (Distributed Denial of Service) saldırısı NATO Halkla İlişkiler web sitesine 1999 yılında gerçekleşmiş olsa da NATO'nun muhabere ve bilgi sistemlerinin korunması hususu resmi olarak ilk defa 2002 yılında gerçekleştirilen Prag Zirvesinde gündeme alınmıştır. Prag Zirvesi'nde gelişen bilgi teknolojileri ışığında NATO'nun siber saldırılara karşı savunma birimi olarak kurulan Yükselen Güvenlik Tehditleri Bölümü'nde siber güvenlik; terörizm ve kitle imha silahlarıyla birlikte beş önemli tehditten biri kabul edilmiştir.

NATO, doktrinini siber savaşa göre değiştirmiş ve konunun hukuki ve teknik yönlerinin tartışılması için çalışmalar başlatmıştır. Bu kapsamda NATO'nun siber saldırılara karşı kendini koruyabilecek şekilde yeteneklerini geliştirmesi hususu *Prag Yetenek Taahhütleri*'nin içerisinde yer almış ve Prag Zirvesi NATO'nun siber güvenlik konusuna verdiği önemi göstermesi açısından bir başlangıç olmuştur. Daha sonra NATO, İttifak'ın askeri ve sivil unsurları arasında bilgiyi hızlı ve güvenli bir şekilde bilgi sistemleri altyapısı üzerinden iletmek maksadıyla NATO Ağ ile Etkinleştirilmiş Güç Programı (Network-Enabled Capability-NNEC)'nı başlatmıştır (NATO, 2003). NATO bilişim sistemlerini ve altyapısını savunma kabiliyetlerini artırmak, zararlı yazılımlarla mücadele etmek ve siber saldırılara karşı koyma kabiliyetini artırmak maksadıyla siber tatbikatlar icra etmektedir. Bu maksatla NATO Muhabere ve Bilgi Sistemleri Ajansının bir birimi olan Bilgisayar NATO Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident

Response Capability-NCIRC) birimi Mons'da SHAPE karargâhında bulunmakta ve NATO'nun bilgi sistem ağlarını siber saldırılara karşı 24 saat esasına göre korumaktadır (NATO, 2011). NATO bünyesinde kurulan NATO Muhabere ve Bilgi Ajansı Bilgisayar Olaylarına Müdahale Teknik Merkezi (NCIA NCIRC TC) ile NATO'nun kullandığı muhabere ve bilgi sistemlerinin tedarik, idame ve işletilmesi görevlerini yürütmektedir. Siber Savunma Birimi, NATO Muhabere ve Bilgi Ajansı (NCIA)'na bağlı görev yapan Alt Yapı Servisleri Direktörlüğü altında hizmet sağlamaktadır. 29 NATO üyesi ülkenin siber savunması, merkezi olarak NCIA NCIRC Harekât Birimi tarafından yürütülmektedir. Harekât Birimi, siber saldırılar ve bilgisayar olayları ile ilgili önleme, tespit etme, tedbir alma ve düzeltme faaliyetlerini yürütmektedir. 200 uzman kişiden oluşan söz konusu birim NATO operasyonlarını desteklemekte ve Müttefiklerinin karşılaştıkları siber saldırıların analizini yaparak çözümler üretmektedir. NATO bünyesinde kesintisiz siber güvenliğin sağlanması görevini yürüten bu Birim'nin bir diğer sorumluluğu da web sitelerinin güvenlik takiplerinin yapılmasıdır.

Tehditlerin niteliği değiştikçe uygulanan metotlarda da değişim gündeme gelmiştir. NATO da kendisini buna göre uyarlamaktadır. Siber savunmanın ulusal sınırları aşan doğası nedeniyle İttikak'ın siber savunma kapasitesini artıracak yeni küresel ortaklıklar ittifak tarafından desteklenmektedir. NATO hâlihazırda bilgi teknoloji firmaları olan Microsoft, Google ve IBM, Uluslararası Standartlar Birliği (International Standards Organization-ISO) ve Internet Mühendisliği Görev Kuvveti (Internet Engineering Task Force/IETF) ile işbirliği yürütmektedir (Huges, 2009: 4).

NATO'nun siber güvenliği yeni bir askeri alan olarak gördüğü ve buna yönelik savunma stratejisi oluşturmaya çalıştığı görülmektedir. Bu durum NATO'nun zirvelerinde dile getirilmektedir. Zirve bildirgelerinde, genişleyen güvenlik yelpazesi ile NATO'nun 29 üye ülkesinin hem siyasi hem de askeri liderlerinin ağ güvenliği ile kendi ülke güvenlikleri arasında direkt bir ilişki olduğu anlaşılırken bunun düşmanca eylemlere karşı korunması gerektiğinin kabul edildiği yorumu yapılabilir. Hatta söz konusu tehdit karşısında önlem almak isteyen dokuz NATO üyesi (ABD, Almanya, İngiltere, Fransa, Hollanda, İspanya, İtalya, Kanada, Norveç) 2003 yılında bilgi paylaşımı içeren bir anlaşma imzalamıştır. 2004 yılında Prag Zirvesinden sonra NATO İletişim ve Enformasyon Sistemleri Servisi Ajansı (NATO Communication and Information Systems Services Agency/NCSA) oluşturulmuştur. "Ajans, ağ ile etkinleştirilmiş güç kavramını hayata geçirebilmek

için merkez karargâhı ile diğer görev güçleri arasındaki iletişimi sağlamaktadır. Kosova operasyonundan anlaşıldığı üzere siber saldırılar ilk olarak iletişim kanallarına odaklanmaktadır. Prag Zirvesi'nde alınan kararlardan biri de kritik alt yapıların terörizme karşı korunması için NATO siber savunma programının oluşturulması olmuş, NCSA siber saldırılara karşı ilk müdahaleyi yapacak unsur olarak belirlenmiştir" (Bıçakçı, 2014: 205-226). "NCSA içindeki merkezlerden en önemlisi, muharip unsurların bilgi güvenliği ve ittifak genelinde güvenli iletişimi sağlamakla yükümlü NATO Bilgi Güvenliği Teknik Merkezidir (NATO Information Assurance Technical Centre/NIATC)" (NATO, 2019). NATO'nun 2007 yılına kadar iletişim, bilgisayar güvenliği ve siber güvenliği konularını birlikte değerlendirdiği görülmektedir. "NIATC, bilgisayar ağlarını Bilgi Güvenliği Operasyon Merkezi ve NATO Bilgisayar Olayları Müdahale Gücü Teknik Merkezi'yle (NATO Computer Incident Response Capability Technical Centre-NCIRC) işbirliği içinde ve 7/24 esasında takip etmektedir. Bu gelişmeye müteakip 2006'da yapılan Riga Zirvesi'nde ağ ile güçlendirilmiş komuta-kontrol kavramı üzerinde durulmuş ve bilişim alt yapısının savunmasının iyileştirilmesinin gerektiğine vurgu yapılmıştır" (NATO, 2006).

2-4 Nisan 2008 tarihleri arasında gerçekleştirilen Bükreş Zirvesi'ne üye ülkeler arasında olan Estonya'nın yaşadığı kriz damga vurmuştur. O zamana kadar hiçbir ülkede görülmeyen boyutta bir dijital saldırıya maruz kalan Estonya'da kurumlarının neredeyse tamamının dijitalleşmiş olması ve vatandaşların gündelik birçok işini internet üzerinden gerçekleştirmesi yaşanan bu saldırı sonucunda altyapının çökmesine sebep olmuştur. Rus devleti ve Estonyalı Ruslar dünya genelinde aldıkları destekle hareket ederek dünya'nın birçok farklı noktasından siber saldırılarına yaklaşık bir ay süresince (28 Nisan–23 Mayıs 2007 devam etmişlerdir. O zamana kadar böylesine bir tehdit algısı öngörmeyen ve stratejik planlar üretme gereği duymayan NATO, bir ay boyunca siber saldırılara maruz kalan müttefiki Estonya'ya anlık destek sağlayamamıştır. Yapılan bu siber saldırılar ile bir devletin kritik alt yapı sistemlerinin internet üzerinden gelebilecek siber tehditlere karşı ne kadar açık olabileceği ortaya çıkmıştır. Müttefiklerine karşı yapılan üst düzey siber saldırılar, NATO'nun siber dünyasını güçlendirmesi ve bu yönde savunmasını geliştirmesi gerektiğini ortaya koymuştur. Bunun üzerine Siber güvenlik NATO'nun Bükreş Zirvesi'nde toplantının ana gündem maddesi haline getirilmiş ve 21. yüzyılın tehditleri bağlamında siber güvenliğin bir tehdit olarak görüldüğü belirtilerek stratejik ve taktik seviyede mücadele organları oluşturulması kararı alınmıştır.

01 Ağustos–01 Eylül 2008 tarihleri arasında Gürcistan'ın bilişim sistemlerinin kritik alt yapısındaki açıklıklar kullanılarak Estonya'da yapılana benzer tarzda bir siber saldırı gerçekleştirilmiştir. Estonya'da yaşanan olay neticesinde NATO iki önemli tedbir alma yoluna gitmiştir. İlk olarak böyle bir siber saldırının tekrar yaşanması ihtimaline karşı savunmanın ortak bir strateji ile yapılabilmesi için Bürüksel'de Siber Savunma Yönetimi Otoritesi (Cyber Defence Management Authority/CDMA)'ni oluşturmuştur. İkinci olarak "Siber savunma kapasitesini bir merkezde toplayarak harekât kabiliyetini daha arttırmayı amaçlayan NATO, Ekim 2008'de Estonya/Tallinn'de bir NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence/NATO CCD COE) kurmuştur" (NATO, 2019). Bu merkezin görevleri "siberle ilgili konularda ittifak için doktrinler ve kavramlar üretmek; NATO'ya üye ülkeler için eğitim kursları, atölye çalışmaları düzenlemek; tatbikatlar yapmak; araştırmalar yapmak ve gelişmeler üzerine toplantılar düzenlemek; geçmişteki ve hâlihazırdaki saldırıları çalışarak dersler çıkarmak; devam eden saldırılarda eğer istenirse tavsiyeler vermek" olarak sıralanmıştır (NATO CCDCOE, 2019). NATO bünyesinde faaliyet gösteren ve 30 personelden oluşan CCDCOE, siber güvenlik konusunda önemli gelişmelere imzasını atmıştır. Birincisi, siber dünyanın genelini ilgilendiren konularda hukuki bir zemin oluşturmak için 2009 ve 2012 yılları arasında, uluslararası hukuk uzmanlarınca yazılan ve savaş hukuku ile uluslararası insani hukukun siber savaşa uygulanabilirliğini irdeleyen *Tallinn El Kılavuzu*'dur. İkincisi, NATO ülkelerinin katılımıyla siber güvenlik konusunda gerçekleştirdiği Uluslararası Siber İhtilaf Konferansları (Conference on Cyber Conflict/CyCon)'dır. Üçüncüsü ise, NATO üye ülkelerinin tamamının katıldığı ve müştereken icra edilen tatbikatlardır. Her yıl CCDCOE koordinasyonunda gerçekleştirilen tatbikatlara üye ülkelerin tamamından gelen bilişim uzmanları, askeri personel ve karar vericiler katılmaktadırlar. Bu kapsamda dünyanın en geniş katılımlı siber tatbikatı olan "Locked Shields" tatbikatı 2010 yılından itibaren her yıl icra edilmektedir. Böylece NATO CCDCOE koordinasyonunda icra edilen söz konusu tatbikatlarla, İttifak üyesi devletlerin ulusal bilgi teknolojisi (BT) sistemlerinin korunabilmesi için siber uzmanların becerilerinin ve yeteneklerinin geliştirilmesi amaçlanmaktadır (NATO CCDCOE, 2019).

2010'da gerçekleştirilen NATO Lizbon Zirvesi'nde, yeni güvenlik tehditlerinin tanımlanması, bu tehditlerle baş etmek için neler yapılması gerektiği konusunda kararlar alınmış ve Zirve aktif katılım ve modern savunmayı önceleyen yeni bir Stratejik Konsept'in benimsenmesiyle son bulmuştur. Zirve'de NATO'nun

savunma ve caydırıcılık konumunun gözden geçirilmesinin devam edilmesine ve siber savunma yeteneklerinin güçlendirilmesine karar verilmiştir (Lizbon Summit Declaration, 2010). Böylece NATO'nun bir yandan geleneksel toplu savunma görevini yerine getirirken bir yandan da yeni tehditlere karşı savunma ve caydırıcılık yeteneğinin modernizasyonuna karar verilmiştir. Bu kapsamda siber saldırılar ve terörist saldırılardan korunmaya yönelik güçlendirilmiş önlemler alınması ve siber savunmanın sürekli olarak NATO gündeminde tutulması kararlaştırılmıştır.

Haziran 2011 tarihinde NATO Savunma Bakanları, "Gözden Geçirilmiş NATO Siber Savunma Politikası"nı kabul etmişlerdir. Bu politika, siber savunma konusunda gerçekleştirilecek olan topluluk bazındaki çabaları içermektedir. Ekim 2011 tarihinde Bakanlar tarafından, "Siber Savunma Eylem Planı"nın detayları üzerinde görüş birliğine varılmıştır. "NATO'nun siber savunma politikasına göre İttifak'ın siber güvenlik politikasındaki öncelikler; koordinasyon temelli bir yaklaşımla siber saldırılara karşılık verecek mekanizmalar geliştirmek için plan ve kapasite gelişimi sağlamak, tüm üye devletler bazında bir politika oluşturmak adına devletlerin siber savunma politikalarını uyumlu hale getirmektir" (NATO, 2011). "Bu bağlamda NATO, kendince merkezileştirilmiş ancak üye devletlerinin her birinin asgari siber savunma gerekliliklerinin karşılandığı bir politika ortaya koymaktadır" (NATO, 2011).

Şubat 2012'de NATO, "Bilgisayar Olayları Karşılama Kapasitesinin (NATO Cyber Incident Response Capability/NCIRC) 2012 yılı sonunda tamamen operasyonel hale gelebilmesi için 58 milyon Avroluk bir kontrat imzalanmıştır" (NATO, 2012). Ayrıca, istihbarat paylaşımı ve durumsal farkındalık için bir "Siber Tehdit Farkındalık Birimi" oluşturulmuştur (NATO, 2012). 2012 yılında ABD'nin Chicago şehrinde gerçekleştirilen Zirve'de "güvenlik tehditleri bağlamında siber saldırı, nükleer silahların ve atma vasıtalarının yayılması, terörizm, enerji ulaşım yollarına saldırı ve çevreye yönelik tehditlere dikkat çekilmiş; sürekli gelişen ve karmaşıklaşan siber tehditlerle etkin biçimde ve işbirliği içinde mücadele edilmesi gerektiği vurgulanmıştır" (Chicago Summit Declaration, 2012). Zirve Sonuç Bildirisi'nden ayrı olarak yayımlanan "Savunma Yetenekleri: 2020 NATO Kuvvetlerine Doğru" başlıklı sonuç bildirisinde daha başarılı operasyonlar gerçekleştirmek amacıyla siber saldırılara karşı savunmayı artırmak için ciddi ilerlemeler sağlandığı ifade edilmiştir.

2014 Galler Zirvesi'nde sürekli daha karmaşık ve yaygın hale gelen siber saldırılarla mücadele etmek maksadıyla güçlendirilmiş siber savunma politikası onaylanmıştır. Zirvede NATO liderleri siber saldırıların ortak savunma ile ilgili 5. Maddeyi tetikleyebileceğini ifade etmişlerdir. NATO kendisine ait bir siber savunma politikası belirlemiş ve siber tehditlere karşı stratejik seviyede bir eylem planı geliştirmiştir. Teknolojinin gelişmesine paralel olarak siber tehdit konuları da artacağından Müttefikler arasındaki diyalog süreci ve koordinasyonun devam ettirilmesine karar verilmiştir. Siber tehdit unsurları ile mücadelede faydalanılabilecek hukuki bir dayanak olmadığı için bu kapsamda da çalışmaların başlatılmasına karar verilmiştir. Ayrıca siber tehditlere karşı kapsamlı siber savunma planlarının yapılması için Müttefiklerin kendi ülkelerindeki kurumları sürekli olarak desteklemelerinin önemi ifade edilmiştir.

NATO, 2016 Varşova Zirvesi'nde siber uzayı -aynen kara, deniz, hava ve uzay gibi- bir harekât sahası olarak tanımlamıştır. NATO'nun yeni güvenlik konseptinde mücadele edilmesi gereken öncelikli alanlar içerisinde yer alan "siber güvenlik alanında üye ülkelerin daha fazla işbirliği içerisinde olması gerektiğine vurgu yapılmıştır. Bu durum NATO askeri komutanlarının siber tehditlere karşı operasyonları daha iyi gerçekleştirmelerine ve görevlerini yerine getirmelerine imkân sağlamıştır. Siber tehditlerin sürekli şekil değiştirmesi; bu tehditlerin kaynaklarının belirgin olmaması ve uluslararası hukukta bu alanda ciddi boşluk bulunması NATO'nun Varşova'da aldığı daha fazla işbirliği kararının kâğıt üstünde kalmaması" gerektiğini göstermektedir (NATO, 2016). İttifak üyeleri, aynı zamanda 2016 yılında kabul edilen Siber Savunma Taahhüdü (Cyber Defence Pledge) gibi girişimlerle kendi ulusal ağlarının ve altyapılarının da siber güvenliğini güçlendirmektedirler. NATO, Müttefiklerin siber savunma yeteneklerini artırmak için ortak bir yaklaşım geliştirecek hedefler belirlemektedir. Siber Koalisyon (Cyber Coalition) gibi dünyanın en geniş savunma tatbikatına ve eğitime yatırım yapmaktadır. Zirve kapsamında, NATO-Avrupa Birliği (AB) Ortak Deklarasyonu da imzalanmıştır. Böylece iki örgüt arasında mülteci krizi ve siber tehditler gibi üst düzey işbirliği gerektiren alanlarda daha fazla işbirliğinin önü açılmıştır. Misyonlar, operasyonlar, tatbikatlar ve eğitimler dâhil olmak üzere siber güvenlik ve savunma alanında koordinasyonun artırılmasına karar verilmiştir.

2018 Brüksel Zirvesi'nde siber güvenlik alanında müttefiklerinin savunmasını güçlendirmek maksadıyla Mons/Belçika'da bir Siber Operasyonlar Merkezi'nin kurulmasına karar verilmiştir. 2023 yılında tamamen faaliyete geçecek olan bu

merkez NATO'nun siber uzaydaki askeri operasyonlarında etkin olarak kullanılacak ve durumsal farkındalık sağlayacaktır. Bu merkezin yanında halen hizmet vermekte olan Roma/İtalya'daki NATO Savunma Koleji'nde ise siber savunma kapsamında stratejilerin belirlenmesi maksadıyla çeşitli eğitimler verilmektedir. Ayrıca Oberammergau/Almanya'daki NATO Okulu'nda, İttifak'ın operasyonlarını, stratejisini, politikalarını ve doktrinlerini desteklemek üzere siber ile ilgili çeşitli eğitimler verilmektedir. NATO siber işgücünün eğitimi ise Oeiras/Portekiz'de halen inşa edilmekte olan NATO Muhabere ve Bilgi Sistemleri Akademisi tarafından sağlanacaktır.

3-4 Aralık 2019 tarihleri arasında gerçekleştirilen Londra Zirvesi'nde de siber güvenlik konusu gündeme gelmiş ve özellikle Zirve Sonuç Bildirisi'nin 3. ve 6. maddelerinde bu konuya yer verilmiştir. "Sonuç Bildirgesi'nde İttifak'ın siber tehditlerle karşı karşıya kaldığı ifade edilmiştir. Bu tehditlere karşı "güvenliğe 360 derece yaklaşımına" uygun olarak NATO'nun mevcut askeri kapasitesini ve planlarını uyarlayacağı ifade edilmiştir. Bu kapsamda NATO'nun 5G dâhil, iletişim sistemlerini siber saldırılara karşı koymak için mücadele araçlarını artıracağı ve bu saldırılara engel olmak amacıyla kabiliyetini güçlendireceği ifade edilmiştir" (NATO, 2019).

NATO, değişen ihtiyaçlar doğrultusunda siber güvenlik çalışmalarını genişletmeye devam etmektedir. NATO üyesi Estonya'ya karşı yapılan siber saldırıya karşı ABD, 2009 yılında İran'ın nükleer tesislerini hedef alarak kendi kendine kopyalanarak çoğalabilen birçok virüs ve saldırıdan çok daha etkili olan Stuxnet (solucan) yazılımını kullanmıştur. Bu saldırı siber uzayda gerçekleştirilen saldırılar içerisinde bir evrim niteliği taşımaktadır (Collins ve McCombie, 2012: 80). Bu yeni savaş düzeninde sadece iyi bir orduya sahip olmak yeterli olmadığı; bilgi ve iletişim teknolojileri konusunda da güçlü olmak gerektiği ortaya çıkarmıştır. NATO, yenilenen Stratejik Konsept'inde de siber uzaya yer vermiştir. Estonya ve Gürcistan'a karşı yapılan siber saldırılar sonrasında NATO'nun siber saldırılara karşı geleneksel uluslararası hukuktan kaynaklanan meşru müdafaa hakkını kullanacağını açıklaması tartışmaları beraberinde getirmiştir. "Siber saldırılar, yalnızca siber saldırı ile birlikte ya da siber saldırı aracılığıyla klasik anlamda askeri silah kullanıyorsa silahlı saldırı olarak kabul edilebilir. Siber saldırı sonucu yönlendirilen bir bombanın bilgisayar destek merkezini veya internet kablolarını vurması ve bu silahlı saldırının "yeterli ağırlık" (Sthan, 2003) ölçüsüne ulaşması buna örnek olarak verilebilir" (Schmitt, 1999). "Ancak bir silahlı

saldırının, konvansiyonel askeri kuvvet kullanılmasıyla gerçekleştirilmek zorunda olmadığının kabul edilmesi, potansiyel riskler ortaya çıkarmaktadır. Siber saldırıların, silahlı saldırı olarak kabul edilmesi durumunda BM Antlaşması'nın 51. maddesinin uygulama alanı genişleyecek ve uluslararası ortamı yeni karışıklıklara sürükleyecektir" (Yayla, 2013: 203). Son yıllarda siber saldırıların giderek artması karşısında NATO'nun 5'inci Madde'sinin uygulamaya geçip geçmeyeceği konusunda tartışma başlamıştır. NATO Genel Sekreteri Stoltenberg, "ciddi bir siber saldırı NATO için kuruluş anlaşmamızdaki 5'inci maddeyi tetikleyebilir. Bu, bir Müttefikimize yönelik saldırının herkese karşı yapılmış sayılmasına yönelik ortak taahhüdümüzdür." ifadesini kullanmıştır (BBC, 2019).

SONUÇ

İçinde bulunduğumuz yüzyılda güvenlik ortamında tehdit yelpazesi genişlemiş, güvenliğe yönelik risk ve tehditler, çok boyutlu ve asimetrik hale dönüşmüştür. Yeni güvenlik ortamı tahmin edilebilir olma özelliğini büyük ölçüde yitirmiş ve istikrarsız bir hale gelmiştir. Değişen bu güvenlik algısı sebebiyle siber tehdit, siber savaş, siber terörizm ve siber güvenlik konuları NATO'nun güvenlik stratejileri kapsamına girmiştir. Siber savunma konusu NATO'nun yeni Stratejik Konseptinde yer almış ve NATO'nun bünyesinde siber tehditlerle mücadele maksadıyla çeşitli stratejiler ve birimler oluşturulmuştur. Ancak NATO'nun siber savunma konusunda daha hızla ilerlemesinin önünde çeşitli engeller bulunmaktadır. NATO tarafından belirlenen stratejiler ekonomik sorunlar, teknolojik yetersizlikler ve yeterli eğitime sahip personelin bulunmaması gibi nedenlerden dolayı Müttefikler tarafından hemen kabul edilerek uygulanmamaktadır. Ayrıca siber güvenlik açısından NATO'nun üyeleri arasında dijital bir bölünmüşlük de mevcuttur. Bir yanda gelişmiş sinyal izleme sistemleri kullanan siber ordulara sahip ABD ve İngiltere gibi ülkeler yer alırken diğer tarafta dijital yarışta çok geride bulunan Romanya, Bulgaristan, Litvanya ve Çek Cumhuriyeti gibi ülkeler bulunmaktadır. NATO'nun siber savunma konusunda hızla ilerlemesinin önündeki engellerden bir diğeri de tehdidin sürekli değişken ve varlığını sürdürüyor olmasıdır. Siber tehdidin asimetrik oluşu ve saldırı yapıldıktan sonra saldırganların hızla izlerini silebiliyor olması siber tehditlerle mücadelede en önemli engellerden birisini teşkil etmektedir.

Yukarıda sayılan nedenlerden dolayı günümüzün yapılanmasıyla hem NATO'nun hem de Müttefiklerin siber saldırılara karşı hızla cevap verebilmeleri mümkün görünmemektedir. Siber tehditlerle mücadele kapsamında öncelikle siber

saldırılara karşı NATO'nun 5. Maddesinin nasıl yürürlüğe gireceğinin açıklığa kavuşturulması gerekmektedir. Bu maksatla öncelikle siber tehdit, siber saldırı gibi kavramların tanımlanması ve siber saldırılara karşı nasıl orantılı bir karşılık verileceği belirlenmelidir. Bunun yanında NATO kapsamında Siber uzay ile ilgili doktrinlerin oluşturulmasına ve geliştirilmesine devam edilmelidir. NATO tarafından alınan kararlar Müttefikler tarafından ivedilikle uygulamaya geçirilmeli ve siber güvenlik konusunda gerekli yatırım ve çalışmalar yapılmalıdır. Bunun yanında NATO'nun güçlenerek siber saldırılara karşı koyabilmesi için NATO üyelerinden teknolojik gelişmişlik açısından önde olan devletlerin kendi imkânlarını ve kabiliyetlerini diğer Müttefiklerle kıskanmadan paylaşmaları önemlidir. NATO'nun siber güvenlik konusunda yetkinliğinin en zayıf üye devletin yetkinliği kadar olduğu çıkarımı yapılabilir. NATO üyesi ülkelerden birisinin kritik altyapılarına karşı gerçekleştirilecek bir siber saldırının diğer ülkeleri de ilgilendiren sonuçları olabilecektir. Bu nedenle Müttefiklerin siber savunma imkân ve kabiliyetlerinin bir bütün olarak değerlendirilmesi önem teşkil etmektedir.

Sonuç olarak, NATO'nun daha fazla kaynak ayırarak CCDCOE koordinasyonunda icra edeceği tatbikatlar ile siber savunma yeteneğini geliştirmesinin ve 2019 Londra Zirvesi'nde de ifade edildiği gibi etkin planlama ve strateji oluşturmasının İttifak'ın siber tehditlerle mücadelesine olumlu katkı sağlayacağı değerlendirilmektedir.

KAYNAKÇA

Ada, M. ve Çakır, H. (2017). Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi, *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, Cilt 5, Sayı: 2, ss. 632-656.

Amiri, I. ve Soltanian, M. (2015). *Theoretical and Experimental Methods for Defending Against DDoS Attacks*, Elsevier.

Andress, J. ve Winterfeld, S. (2011). *Cyber Warfare*, Elsevier.

Arquilla, J. ve Ronfeldt, D. (2001). The Advent of Netwar (Reviseted). In J. Arquilla & D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, ss. 1-25.

BBC (2019.). *NATO: Cyber-attack on one nation is attack on all*. 27.Agu.2019. Erişim Tarihi: 28 Haziran 2019,.https://www.bbc.com/news/technology-49488614

Brenner, S. W. (2007). "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare", *Journal of Criminal Law and Criminology*, No: 2, Vol. (97), ss. 379-476.

Brenner, S. W. ve Goodman, M. D. (Bahar 2002). "In Defense of Cyberterrorism: An Argument for Anticipating Cyber Attacks", *University Of Illionis Journal of Law, Technology and Policy*. Vol. 2002, Erişim Tarihi: 6 Eylül 2019, https://pdfs.semanticscholar.org/4e3a/5bb4112234fa3fb33a89eeb7e5f3a7950b6c.pdf

Bıçakcı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. *Uluslararası İlişkiler, 10* (40), 101-130.

Clarke, R. ve Knake, R. K. (2011). *Siber Savaş Ulusal Güvenliğe Yönelik Yeni Tehdit* (Çev. M. Erduran), İstanbul Kültür Üniversitesi, İstanbul.

Collins, S. ve McCombie, S. (2012). Stuxnet: The Emergence Of A New Cyber Weapon And İts İmplications. *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 7, No. 1, ss. 80-91.

Çakmak, H. ve Altunok, T. (2009). *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, Ankara, Barış Platin Kitapevi yayınları.

Çiftçi, H. (2013). *Her Yönüyle Siber Savaş*, İstanbul: TUBİTAK Popüler Bilim Kitapları.

Çolak, H. (2011). Siber Terör, Yargılama Usulü ve Önleyici Tedbirler, *Kazancı Hakemli Hukuk Dergisi*. ss. 62-142.

Denning, D. E. (2001). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Erişim Tarihi: 2 Temmuz 2019, http://www.nautilus.org/info-policy/workshop/papers/denning.html

Denning P. J. ve Denning, D. E. (2010). The Profession of IT Discussing Cyber Attack, *Viewpoints*, September 2010 Vol. No.9, s. 29. Erişim Tarihi: 1 Temmuz 2019, http://calhoun.nps.edu/bitstream/handle/10945/35515/cacm Sep10.pdf? sequence=1

Gedik, D. (2018). *Siber Güvenlik ve Terörizmin Evrilişi: Türkiye Üzerine Etkileri*. (Yayınlanmamış Yüksek Lisans Tezi). Düzce Üniversitesi, Sosyal Bilimler Enstitüsü, Düzce.

Geers, K. (2010). Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL. (Yayınlanmamış Doktora Tezi). Tallinn University Of Technology Faculty of Information Technology, Tallinn.

Gibson, W. (1984). *Neuromancer*, (Çev. M. Altıntaş), Gündüz Yayınları, İstanbul.

Gökçe, K. G., Şahinaslan, E. ve Dinçel S. (2014). *Mobil Yaşamda Siber Güvenlik Yaklaşımı,* 7'nci Uluslararası Bilgi Güvenliği ve Kriptoloji ve Konferansı, (214-221).

Güntay, V. (2017). Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği, *Güvenlik Bilimleri Dergisi*, Trabzon, Kasım 2017, 6 (2), ss. 81-108.

Hasgüler, M. ve Uludağ, M. B.(2005). *NATO, Devletlerarası ve Hükümetler-dışı Uluslararası Örgütler*, Nobey Yayın, Ankara.

Hatipoğlu, C. (2017). Teknolojik Savaşlar: Siber Terörizm Tehditleri, 3nd International Congress on Political, Economic and Social Studies (ICPESS), 09-11 Nov. 2017.

Heickerö, R. (2014). Cyber Terrorism: Electronic Jihad. *Strategic Analysis*, 38(4).

Hill, R. (2015). *Dealing With Cyber Security Threats: International Coorporation*, ITU and WCIT. 7th International Conference on Cyber Conflict, 119-134.

Huges, R. B. (Nisan 2009). *NATO Cyber Defence*. Erişim Tarihi: 07 Temmuz 2019, https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf

Kara, M. (2013). Siber Saldırılar - Siber Savaşlar ve Etkileri. (YayımlanmamışYüksek Lisans Tezi). İstanbul Bilgi Üniversitesi, İstanbul.

Kravasin, S. (2000). *What is Cyber Terrorism?* Computer Crime Research Center. Erişim Tarihi: 18 Temmuz 2019, http://www.crime-research.org/library /Cyber-terrorism.htm

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

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. USA, RAND Corporation, Project Air Force. Erişim Tarihi: 16 Temmuz 2019,.https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Lisbon Summit Declaration. 20.11.2010. Erişim Tarihi: 18 Temmuz 2019, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_strategic-concept-2010-tur.pdf

Murphy, M. (2010). 'War in the Fifth Domain; Cyberwar'.*The Economist*, 3 July 2010. Erişim Tarihi: 16 Temmuz 2019, https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

NATO (1999a). *An Alliance for the 21st Century Washington Summit Communique issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. on 24th April 1999.* Erişim Tarihi: 18 Temmuz 2019, http://www.nato.int/cps/en/natolive/official_texts_27440.htm

NATO (1999b). *The Alliance's Strategic Concept, 24 Nisan 1999*. 23. Madde. Erişim Tarihi: 19 Temmuz 2019, http://www.nato.int/cps/en/natolive /official_texts_27433.htm

NATO (2003). *The Prague Summit and NATO's Transformation.* 2003. Erişim Tarihi: 2 Haziran 2019, http://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf

NATO (2006). "Riga Summit Declaration, 29 Kasım 2006", http://www. nato.int/docu/pr/2006 /p06-150e.htm (Erişim Tarihi: 22.07.2019).

NATO (2011). NATO CIS Cervices Agency, *NATO Cyber Defence Management*. Erişim Tarihi: 21 Temmuz 2019, http://www.nato.int/cps/en/natolive/ news_85161.htm

NATO (2012a). *Chicago Summit Declaration*. 20.5.2012. Erişim Tarihi: 26 Temmuz 2019, http://www.nato.int/cps/en

NATO (2012b). *NATO Rapid Reaction Team to Fight Cyber Attack*. 13.3.2012. Erişim Tarihi: 23 Temmuz 2019, http://www.nato.int/cps/en/natolive/ news_85161.htm

NATO (2016). *Warsaw Summit Key Decisions.* February 2017. Erişim Tarihi: 23 Temmuz 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_ 2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf

NATO CCDCOE (2019). *Exercises*. Erişim Tarihi: 13 Ağustos 2019, https://ccdcoe.org/exercises/

NATO CCDCOE (2019). *About us*. Erişim Tarihi: 146 Ağustos 2019, https://ccdcoe.org/

NATO (2019). *NATO Cyber Defence*. Erişim Tarihi: 12 Ağustos 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_190 2-factsheet-cyber-defence-en.pdf

NATO (2019). *NATO London Declaration.* Erişim Tarihi: 12 Aralık 2019, https://www.nato.int/cps/en/natohq/official_texts_171584.htm

Ottis, R. (2011). A Systematic Approach to Offensive Volunteer Cyber Militia. (Yayımlanmamış Doktora Tezi). Faculty of Information Technology, TUT Press.

Ottis, R. ve Lorents, P. (2010). "Cyberspace: Definition and Implication", International Conference on Information Warfare and Security, XII. Reading: Academic Conferences International Limited.

Petit, B. S. (2003). Chechen Use of the Internet in the Russo-Chechen Conflict. (Yayımlanmamış Yüksek Lisans Tezi). The U.S. Army Command and General Staff College Fort Leavenworth, Kansas.

Pierce, B. M. (2018). DARPA's Quest For a Beneficent Cyber Future, *DARPA Defense Advance Research Projects Agency 1958-2018*. Erişim Tarihi: 22.07.2019, https://www.darpa.mil/attachments/DARAPA60 publication-no-ads.pdf

Rogers, R. ve Devost, M. (2005). *Hacking a Terror Network: The Silent Threat of Covert Channels*, Elsevier.

Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Research Publication 1 Information Series, 1999, ss. 21-22. Erişim Tarihi: 12 Temmuz 2019, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993

Schweitzer, Y., Siboni, G. ve Yogev E. (2011). "Cyberspace and Terrorist Organizations", *Millitary and Strategic Affairs*, 3(3).

Singer, P.W. ve Friedman, Allan (2018). *Siber Güvenlik ve Siber Savaş* (Çev. A. Atay), Buzdağı Yayınları.

Standler, B. R. (2002, September 4). *Computer Crime*. Erişim Tarihi: 25 Temmuz 2019, http://www.rbs2.com/ccrime.htm

Sthan, Carsten (2003). "Nicaragua is Dead-Long Live Nicaragua-the Rigt to Self Defence Under Article 51 of UN Charter and International Terrorism", *Terrorism as a Challenge for National and International Law: Securtiy versus Liberty*, Berlin&Heidelberg. Erişim Tarihi: 20 Temmuz 2019, http://edoc.mpil.de/conference-on-terrorism/index.cfm

Whittaker, J. (2004). *The Cyberspace Handbook***,** Oxon, Routledge.

Wilson, C. (2003). Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. 34. No. 90. Erişim Tarihi: 20 Eylül 2019, https://fas.org/irp/crs/RL32114.pdf

Van A. ve Richard H. (2018). Darpa Innovation Icon at 60, *DARPA Defense Advance Research Projects Agency 1958-2018.* Erişim Tarihi: 22 Temmuz 2019, https://www.darpa.mil/attachments/DARAPA60publication-no-ads.pdf

Yayla, M. (2013). Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma, *TBB Dergisi* 2013 (107). Erişim Tarihi: 22 Temmuz 2019, http://tbbdergisi.barobirlik.org.tr/m2013-107-1293

Yılmaz, S. ve Salcan, O. (2008). *Siber Uzayda Güvenlik ve Türkiye*, İstanbul, Milenyum yayınları.