Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri

Özge GÜLEÇ[1]

Zülfükar Aytaç KİŞMAN[2]

Öz

Soğuk savaşın bitmesiyle ülkelerin güvenlik tedbirleri ve uluslararası güvenlik sistemi tamamen değişmiştir. Soğuk savaşın getirmiş olduğu tehditlerin ortadan kalkmasıyla Kuzey Atlantik Paktı Örgütü (NATO) yeni ve çok farklı bir güvenlik ortamıyla karşı karşıya kalmıştır. Siber uzayda kritik altyapıların korunması meselesi NATO üyesi ülkelerin önemli gündem maddelerinden biridir. Bu konuda çalışma yapan üye ülkeler, kritik altyapıların korunması ile ilgili yasal alanda ve teknik uygulamalarda ciddi yol almıştır. Bu çerçevede İttifakın sistemdeki yapısal değişiklikleri incelenip, yeni duruma uyum sürecinde ne gibi sorunlarla karşılaştığı ve bu sorunlar karşısında ne gibi politikalar uygulandığı ve konunun uluslararası ilişkiler bağlamındaki önemi incelenmiştir. Çalışmanın birinci bölümde, siber güvenliğin tanımı, günümüzdeki önemi, uluslararası ilişkiler açısından siber güvenlik; ikinci bölümde NATO'nun tarihi, NATO'nun siber güvenlik stratejileri ve NATO'nun dahil olduğu siber kriz örnekleri; üçüncü bölümde NATO üyesi ülkelerin siber güvenlik çalışmaları ve sonrasında da sonuç yazılarak öneriler sunulmuştur.

Anahtar Sözcükler: NATO, Siber Güvenlik, Uluslararası İlişkiler.

[1] YL Öğrencisi, Fırat Üniversitesi, Sosyal Bilimler Meslek Yüksekokulu, Pazarlama ve Dış Ticaret Bölümü, E-mail: ozgegulec232323@gmail.com

[2] Dr. Öğr. Üyesi, Fırat Üniversitesi, Sosyal Bilimler Meslek Yüksekokulu, Pazarlama ve Dış Ticaret Bölümü, ORCID: https://orcid.org/0000-0002-5573-5448 E-mail: aytac@firat.edu.tr

Güleç, Ö. & Kişman, Z. A. (2021). Uluslararası ilişkiler açısından siber güvenlik ve NATO'nun siber güvenlik stratejileri. *Akademik Açı*, *1*(1), s. 127-154.

Cyber Security From the Perspective of International Relations and Cyber Security Strategies of NATO

Abstract

With the end of the Cold War, the security measures and international security system of the countries were completely changed. With the disappearance of the threats posed by the Cold War, the North Atlantic Treaty Organization (NATO) faced a new and very different security environment. The issue of the protection of critical infrastructures within the cyber space is one of the important agenda items of NATO member countries. Member States have made significant progress in the the protection of critical infrastructures in terms of legal and technical issues. In this context, the structural changes in the system of the Alliance were examined and the problems faced during the adaptation process to the new state and the policies implemented against these problems and the importance of the issue with regard to international relations were examined. In the first part of the study, the definition of cyber security, its current importance, cyber security in terms of international relations, the history of NATO; in the second part, NATO's cyber security strategies and examples of the cyber crisis involving NATO; in the third part, the cyber security studies of NATO member countries and the conclusion part has been added with suggestions.

Keywords: NATO, Cyber Security, International Relations.

Giriş

Güvenlik, insanoğlunun var oluşundan beri en temel ihtiyaçlarından biri olmuştur. Toplumların ve devletlerin temel taşı olan insan, güvenlik problemleriyle karşılaşmamak için gerekli tedbirler almıştır. Geçmişte uygulanan ilkel güvenlik tedbirleri teknolojinin gelişmesiyle, yerini modern uygulamalara bırakmıştır. Bilgisayarın yaşamımıza girmesiyle, insanlar ve kurumlar bilgisayarları aktif bir şekilde kullanmaya başlamıştır. Emniyet bilgilerinden, şirket sırlarına; ticari konulardan, milli istihbarata kadar birçok bilgi bilgisayarlarda depolanmaktadır. Dış dünyaya açık olan bu bilgisayarların ve kullanılan ağların korunması siber güvenlik alanını oluşturmaktadır. Siber güvenlik, teknolojinin gelişmesiyle daha da önem kazanmıştır. Hayatımızı kolaylaştıran teknolojik gelişmelerin insanoğluna sunduğu en önemli aygıtlardan olan cep telefonları bugün cebimizde taşıdığımız bir iletişim cihazı olmaktan çok hayatımızın tabiri caizse kumandası durumundadır. Ancak teknolojik gelişmelerle kullanımı artan cep telefonu, tablet ve benzeri birçok elektronik alet, sunduğu kolaylıkların yanında birçok güvenlik risklerini de beraberinde getirmiştir. Siber güvenlik, özellikle son yıllarda gelişen teknolojiler ve bu teknolojilerle beraber çoğalan tehditler karşısında elektronik sistemlerin korunması için en iyi metotları sunmayı hedefleyen, gelişmekte olan bir alandır. Bu bağlamda eski tedbirlerin yanı sıra önlemler almak zorunda kalan devletler ve toplumlar kritik bilgi altyapılarını korumak için siber güvenlik alanında çeşitli çalışmalar yapmaktadır. Siber tehdit ve saldırılardan korunmak isteyen ülkeler ve

uluslararası kuruluşlar da siber güvenlik stratejileri ve politikaları oluşturmaktadır.

Uluslararası bir kuruluş olan NATO, kurulduğu 1949 yılından itibaren kendi üye ülkeleri arasında eşsiz bir bağ oluşturarak NATO ittifak ülkelerini her türlü saldırıya karşı korumaya çalışmıştır. Gelişen teknolojilerle yeni bir güvenlik alanı olan siber uzayda da güvenlik politikaları ve stratejileri geliştirmek NATO için son derece önemli hale gelmiştir. Uğranan siber saldırılar sonrasında ittifakın ve üye ülkelerin güvenliğini korumak adına çeşitli siber güvenlik politikaları oluşturulmuştur. NATO'nun konvansiyonel güvenlik politikalarının yanında siber güvenlikle ilgili politika ve stratejiler geliştirmesi uluslararası düzeyde iş birliğinin gerekliliğinin anlaşılması açısından önemlidir. Zira siber saldırıların engellenmesi için uluslararası iş birliğine ihtiyaç vardır. Ancak bu alanda çok az uluslararası antlaşma imzalanabilmiş durumdadır. Belirli uluslararasılar siber saldırılarla mücadele etmeyi hedeflemiştir. Bunda tetikleyici etmenler daha çok bazı Avrupa ülkelerine karşı düzenlenen siber saldırılardır. Bu saldırılar sonrası AB, G8, NATO gibi uluslararası kuruluşlar harekete geçmiş ve siber saldırılara karşı birlikte hareket etmek üzere çaba sarf etmişlerdir (Gürkaynak & İren, 2011, s. 275).

Bu makalenin amacı siber güvenlik, NATO ve NATO ittifakının siber güvenlik algısı ve çalışmaları konularını araştırmaktır. Zira siber güvenlik kavramıyla değişen devlet anlayışları ve dünyada yaşanan siber saldırıların sonuçları NATO'nun siber güvenlik stratejileri oluşturmasında önemli bir yere sahiptir. Siber kavramını NATO ittifakıyla değerlendiren bu çalışma

NATO'nun siber güvenlik stratejilerini anlatan çalışmalara katkıda bulunmayı amaçlamaktadır. Konu ile ilgili literatür dinamik bir yapıya sahiptir. Hem teknolojik gelişmelerin hız kesmeden devam etmesi ve bu gelişmelerin bireysel ölçekten devletler ölçeğine kadar pek çok etkisinin olması, konunun çalışılabilirliğini artırmakta ve bu çalışma gibi yeni çalışmalara imkân tanımaktadır. Konunu güncel olarak takip edilmesi bu yönüyle önem arz etmektedir. Bu çalışmada NATO ile ilgili bazı temel bilgilere yer verilerek NATO üyesi devletlerin siber güvenlik ile ilgili ulusal güvenlik stratejileri ve siber güvenlik kavramının önemi güncel rapor, kitap, dergi, makale ve tezlerden yararlanılarak aktarılmaya çalışılmıştır.

1. Siber Güvenlik Nedir?

Teknoloji, yaşamımızın her alanını çok hızlı bir şekilde etkilemektedir. Özellikle teknolojilerin ve internet kullanımının her alanda hayatımıza girmesi ve yaygınlaşmasıyla insan yaşamı kolaylaşmış, zaman ve mekân ayrımı gözetmeksizin günlük yaşamımızda yerine getirmekte zorunlu olduğumuz birçok işlevi kolaylıkla yerine getirme imkânı vermiştir. Günümüzde akıllı mobil cihazların, kullanımının artmasıyla aylık periyodik ödemeler, her türlü bankacılık işlemleri, eğitim, alışveriş daha birçok uzak erişim işlemleriyle hayatımızı kolaylaştırmış ve vazgeçilmediğimiz bir olgu haline gelmiştir (Aytekin, 2015, s. 1). Siber uzay, teknoloji ve bu teknolojileri kullananlara paralel olarak sürekli değişim ve gelişim göstermektedir. Gelişen teknoloji ile cep telefonlarının artan işlem gücü bilgisayarlarla rekabet eder hale gelmiş ve hayatın her safhasında arabalara, varana kadar, yaygınlaşmıştır. İnternet, dolayısıyla siber uzay, kullanımı önceleri sadece iletişim amaçlı iken

günümüzde Internet of Things (IoT) kavramı olarak da ifade edilen bir kapsamda alarak altyapı sektörleri de dâhil olmak üzere, ticaret, gıda, bankacılık, sağlık, ulaşım ve daha birçok alanda işlevsel hale gelmiştir. Devletlerin kurum ve vatandaşlarla iletişiminde interaktif bir şekilde kullanılmaya başlanmıştır (Somuncu, 2018, s. 7). Zaman ve mekân gözetmeksizin kullanılabilen internet, kişisel bilgilerin, yer bildirimlerini, banka hesap bilgilerini, iş verilerini sanal ortamda kaydetmektedir. Bu durum bazı güvenlik problemlerin ortaya çıkmasına neden olmuştur. Bu problemlerden biri Siber Güvenliktir. Dünyada her geçen gün artan siber güvenliğin önemini açıklamadan önce "Siber Güvenlik" tanımlarına bakmak faydalı olacaktır.

Dünyadaki çatışmaların yönelimi küresel düzeyde teknolojik, ekonomik, kültürel ve politik gelişmeye göre zaman zaman değişmektedir. Son yıllarda bahse sıklıkla konu olan siber çatışmalar da yeni tip bir çatışma türü olarak dünyanın çatışma eğilimini etkilemiştir (Akyeşilmen, 2017, s. 173-174). Siber güvenlik; bilgi, veri güvenliğinin alt yapıları olan bilgisayar ve bilişim sistemleri güvenliği kavramının internet kullanımının yaygınlaşması sonucu ortaya çıkan risklere dair yeni bir kavramsal çerçeve olarak tanımlanabilir (Güngör, 2015, s. 19). Bu bağlamda Siber Güvenlik, siber alan bilgi sistemlerinin her türlü tehdit ve saldırıya karşı korunması, bu alanda işlenen bilgilerin gizliliğini ve erişilebilirliğini kontrol edilmesi ve güvenceye alınması, siber saldırıların ve siber güvenlikle ilgili olayların tespit edilmesi ve otomatik kontrol yanıt mekanizmalarının tekrar ön plana koyulması anlamına gelir (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013, s. 9).

Nispeten yeni bir kavram olması hasebiyle bu konuda temel yaklaşımların geliştirilmesi gerekli hale gelmiştir. En genel çerçeve ile "Siber Güvenliğin" temin edilebilmesi için aşağıda sıralanan maddelerin bilinmesi ve azami seviyede uygulanması gerekmektedir (İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku Enstitüsü, 2012, s. 4):

- Siber güvenlik stratejisinin belirlenmesi ve oluşturulması,
- Devlet bünyesinde siber güvenlik yapıların oluşturulması,
- Uyum içerisinde çalışabileceği akıllı bir alt yapının kurulması,
- Siber güvenlik alanındaki hukuki yapının oluşturulması,
- Bu sahada çalışacak nitelikli personel ihtiyacının karşılayacak eğitim programlarının verilmesi,
- Gelişimleri takip ederek bu alanda AR-GE merkezlerinin kurulması.

1.1. Uluslararası İlişkiler Açısından Siber Güvenlik

Günümüzde, ağ üzerinden yapılabilecek bilgi hırsızlığı, siber saldırı gibi tüm entegre sistemlere zarar verebilecek tehditler önemli bir sorun haline gelmiştir. Dolayısıyla daha kapsamlı bir kurumsal boyutun yanı sıra siber güvenlik tehditleri, siber istihbarat, siber suç gibi kavramları da içine alacak şekilde toplumsal, ulusal ve uluslararası boyutlara ulaşmıştır. Bu da devletlerin siber alanı bir hâkimiyet unsuru olarak görmeye başlamalarına neden olmuş ve siber güvenlik alanları daha bağımsız bir hale dönüşmüştür (Güngör ve Güney, 2017, s. 138). Siber tehdit ve saldırılardaki artış nedeniyle, birçok ülke bu alanda güvenlik stratejilerine önem vermeye başlamıştır. Özel kurumlar

dahi bu alan hakkında görüşlerini aldıkları özel BT uzmanlarını bünyelerine katma ve yetiştirme ihtiyacı duymaktadırlar. Siber saldırılara karşı gerek resmî kurumlarca gerekse de özel firmalarca büyük yatırımlar yapılmakta ve büyük bütçeler ayrılmaktadır. Bu amaçla, ülkeler bireysel vatandaşların bilgi güvenliğini sağlamak için çeşitli altyapı, kamu bilgi ve dokümanları ve siber güvenlik politikaları oluşturmakta ve uygulamaktadırlar (İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku Enstitüsü, 2012, s. 4).

Daha kapsamlı olacak şekilde Avrupa Konseyi, G8, BM, NATO, gibi uluslararası kuruluşlar çeşitli stratejiler üreterek siber güvenlik ve altyapısının korunması ve güçlendirilmesi konusunda çalışmalar yapmaktadırlar. Avrupa Konseyi konuyla ilgili olarak 2004'te yürürlüğe giren uluslararası bir siber suç sözleşmesine ilişkin bir anlaşmaya varmıştır. Avrupa Konseyi Siber Suçlar Konvansiyonu, siber suç konusunda ilk ve tek uluslararası sözleşme olan Avrupa Birliği Siber Suçlar Konvansiyonu'nda uluslararası arena ve siber suçlara karşı mücadelede çok önemli bir rol oynamaktadır. Avrupa Konseyi'ne üye devletlerin kırk ikisi sözleşmeyi imzalamış ve bunlardan yirmi beşi kanunu onaylamıştır (Turhan, 2010, s. 71-72). G8 ülkeleri 1995'ten bu yana siber güvenlik, bilgi toplumunun ve kritik bilgi altyapısının korunması gibi alanlarla daha fazla ilgilenmiş ve 1995'teki Halifax Zirvesi'nde, mevcut uluslararası anlaşma ve örgütlerle mücadele mekanizmalarını incelemek ve değerlendirmek üzere Kıdemli Uzmanlar Grubu atanmıştır. Bu zirveden sonra, G8 Kıdemli Uzman Grubu tarafından birçok öneri kabul edilmiştir. G8 Kıdemli Uzman Grubu, ileri teknoloji suçlarının önemini anlayan ilk uluslararası forum olarak nitelendirilmektedir (Turhan, 2010, s. 78). Birleşmiş Milletler (BM) Bilgi

Güvenliği Devlet Uzmanları Grubu'na (GGE) liderlik etmektedir. İstikrar ve siber alandaki anlaşmazlıkların önlenmesi için gerekli adımları belirlemeyi amaçlayan çalışma grubunun, uluslararası normlar oluşturmak temel amaçları arasındadır. Sorumlu devlet davranışlarını ve siber uzayda devletlerin politikalarını sınırlayan bu normlar, kural ve ilkelerin belirlenmesi konusunda bir rapor yayınlamıştır. Çalışma grubu 2004 yılından itibaren aktif olarak faaliyet göstermektedir (Dijital Türkiye, 2017, s. 14).

Ülkelerin siber güvenlik yapılanmaları birbirinden farklılıklar gösteren unsurlara sahip olmakla birlikte genel itibarla benzerlikler görülmektedir. Bazı ülkeler siber güvenlikle ilgili alt yapılarını teşkil etmek üzere yeni kurumlar oluştururken bazı ülkeler ise mevcut kurumlarının görev alanını genişleterek bu yeni güvenlik kavramına adapte olmaya çalışmışlardır (Ada, 2018, s. 61). Yine ülke bazında bakıldığı zaman siber saldırılara ve olası siber tehditlere karşı her ülkenin tutumu değişmektedir. Bazı ülkeler siber alanı daha az kullanıyorken, bazıları da kendi çıkarları doğrultusunda daha sık kullanmaktadır. Siber etkinlikleri çok sık kullanan ülkelere baktığımızda, teknolojik olarak daha ileri düzeyde oldukları ve genellikle küresel bir siber güvenlik oluşumunu desteklemedikleri gözlenebilir. Bunun sebebi uluslararası bir düzenlemenin kendi çıkarlarına ve hareket alanlarına uygun olmama ihtimalidir. Bununla birlikte, siber saldırıların kötü niyetli insanlar veya kuruluşlar tarafından gerçekleştirilmesi ve daha büyük devletlerin daha fazla acı çektiği gerçeği, siber alandaki gelişmelerin klasik uluslararası ilişkiler faaliyetlerinde bulunmasını gerektirmiştir. Çünkü siber uzaydaki gelişmeler

uluslararası ilişkiler alanında yeni aktörler yaratmış ve yeni güvenlik riskleri oluşturmuştur (Gürkaynak & İren, 2011, s. 265).

Siber güvenliğin devletlerarasındaki ilişkiler açısından önemli rol oynadığına dair birçok veri mevcuttur. Siber alanının uluslararası ilişkiler boyutunda görüldüğü ve günümüzde "siber politikalar" adıyla çalışmaların yapıldığı ve devletlerin güncel çalışmalarında ciddi bir artış görülmektedir. Değişen dünya açısından çıkar mücadelesinin ön planda olduğu, siber güvenlik ve temelindeki araçlarla siber saldırılara karşı, devletler siber saldırının nerede geldiği ile ilgili tespitler yapabilmekte ve bu durum uluslararası sistemi olumsuz etkilemektedir. Siber tehditlerin varlığı ve olası siber saldırılar devletleri sıcak çatışmalara sürükleyecek hale gelmiştir (Güntay, 2018, s. 80-81). Ancak siber güvenliğin sağlanması ve siber savaşla mücadele, yalnızca devletlerin çabalarıyla mümkün değildir. Devlet ve devlet dışı birçok kurum, kuruluşların küreselleşen dünyada topyekûn hareket ettiği görülmektedir. Örneğin, Avrupa Konseyi tarafından imzalanan ve 2004'te yürürlüğe giren Budapeşte Konvansiyonu ilk sözleşme ve bu sözleşmeyi ifade eden Şubat 2005'teki AB'nin 2005/222 / JHA hükmüdür. Hüküm daha sonra 14 Ağustos 2013 tarihinde Bilgi Sistemlerine Saldırı Yönergesi olarak değiştirmiştir. İmzalanan bu anlaşma aynı zamanda AB için siber sahada yapılan ilk anlaşmadır (Tarhan, 2018, s. 47).

2. Nato ve Siber Güvenlik

2.1. Nato Hakkında

İkinci dünya savaşı sırasında ve özellikle de savaş sonrasında geniş alanları kontrolü altına almanın çabası içinde olan Sovyetler Birliği, 1940-1945 yılları arasında Avrupa'da 450.000 Km. toprağı ve 24 milyon kadar nüfusu sınırlarına katmıştır.1945-1948 yılları arasında 1 milyon Km. toprak ile 92 milyon nüfusu da himayesine almayı başaran Sovyetler Birliğini dengelemek ve durdurmak isteyen Amerika Birleşik Devletleri ise bazı tedbirler başvurmayı gerekli görmüştür. Bu tedbirlerin en etkilisi hiç şüphesiz "4 Nisan 1949' da 12 Batılı ülke arasında kurulan ve kısa adı NATO olan (North Atlantic Treaty Organization) Kuzey Atlantik İttifakı olmuştur. Antlaşmanın ilk başlığında NATO ülkelerinin demokrasi ilkeleri ile kişi hürriyetleri ve hukuk üstünlüğüne dayanan özgürlüklerini ve ortak savunmaları ile barış ve güvenliklerini korumak amacıyla bir araya geldikleri belirtiliyordu. NATO anlaşmasının en dikkat çeken özelliklerinden birisi üye ülkelerden birine yapılmış bir saldırının diğer ittifak ülkelerine yapılmış sayılacağı olmasıdır (Armaoglu, 1989, s. 229-230). Bu savunma temelli ittifak Soğuk Savaş dönemi boyunca üye sayısını ve etki alanını genişletmiştir. Günümüzde NATO'nun 29 üyesi bulunmaktadır. Yıllara göre NATO üyesi olan ülkeler ve üye oluş tarihleri Tablo 1'de gösterilmiştir.

Tablo 1: Yıllara göre NATO üyesi olan ülkeler ve üye oluş tarihleri (NATO, 2017).

Fransa (1949)	Lüksemburg (1949)	Bulgaristan (2004)
Belçika (1949)	Norveç (1949)	Estonya (2004)
Birleşik Devletleri (1949)	Türkiye (1952)	Letonya (2004)
Birleşik Krallık (1949)	Yunanistan (1952)	Litvanya (2004)
Danimarka (1949)	Almanya (1955)	Romanya (2004)
Hollanda (1949)	İspanya (1982)	Slovakya (2004)
İzlanda (1949)	Polonya (1999)	Arnavutluk (2009)
İtalya (1949)	Macaristan (1999)	Hırvatistan (2009)
Kanada (1949)	Çek Cumhuriyeti (1999)	Karadağ (2017)
Portekiz (1949)	Slovenya (2004)	K. Makedonya (2020)

NATO ilk kurulduğu zamanlarda, geleneksel ittifaklardan ayrı bir özellik göstermiyordu. Bu anlayış 1950 yılında Kuzey Kore'nin Güney Kore'ye saldırmasıyla değişti. Saldırının, kısa bir süre sonra Batı Avrupa'ya da yönelebileceğini düşünen üyeler; ortak bir harekât planı hazırlamaya başladılar. Bu andan itibaren NATO geleneksel ittifaklardan uzaklaşarak askeri bir ittifak haline gelmiş oldu. Çin'de komünistlerin başarıya ulaşmaları ve 1949 yılında Sovyetlerin atom bombası patlatarak bu güçlü silahın ABD'nin tekelinde olamayacağını göstermesi de NATO'daki bu geçişi etkileyen diğer önemli unsurlardır (Sarınay, 1988, s. 76). 1960 sonlarına kadar SSCB ve ABD arasında uzun yıllar süren nükleer silahlarda ve gönderme araçlarında yarış olmuştur. Bu durumların yaşanmasıyla ekonomilerine getirilen yükler sonucunda 1970'lerin başında kutuplar arası yumuşama dönemine girilmiştir. Yaşanan barışçıl ortam sonucunda silahsızlanma görüşmeleri de yapılmaya

başlanmıştır (Gürkaynak, 2005, s. 9). Bu yumuşama (detant) döneminde bile NATO etkisini kaybetmemiş ve önemli bir savunma ittifakı olma özelliğini sürdürmüştür.

NATO İttifakı temel hedefi olan güvenlik görevini yerine getirmek için aşağıda belirtilen belli başlı maddeleri yapmaya çalışır.

- NATO, siyasi ve askeri yollarla mükelleflerini korur. Ayrıca, savunma reformları, barışı koruma gibi konularda NATO üyesi olmayan ülkelerle iş birliği çağrısı yapar.
- NATO, üye ülkelerinin topraklarındaki ve topraklarının dışındaki çatışmaları engellemeye çalışır.
- NATO, çıkan anlaşmazlıkları barışçıl yollarla çözülmesini sağlar, barışçıl çabalar sonuç vermediğinde tek başına veya uluslararası örgütlerle iş birliği içine girer.
- NATO, üyelerinin doğal afetlerle mücadelesinde yardım eder ayrıca bilim ve çevre konularında iş birliğine teşvik edecek faaliyetlerde bulunur (NATO Otan).

NATO, görevlerini yerine getirmek amacıyla askeri olmayan alanlarda da (siyasi ve ekonomik) üye ülkelere danışmanlık ve üyeleri arasında iş birliği ortamı sağlamaktadır. Bunlara ek olarak uzmanlaşma gerektiren sahalardaki çalışmaların eş güdümlenmesi maksadıyla, NATO üyesi ülkeler aracılığıyla kurulan ajansları da içinde bulunduran karmaşık bir sivil ve askeri yapı oluşturulmuştur. Uzmanlaşmaya gidilmiş söz konusu sahalara, askeri kuvvetlerin komuta ve kontrolünü, siyasi danışmanlığı ve kuvvetlerin devamını sağlamak amacıyla gerekli lojistik desteğin muhafazasını

kolaylaştıran bir iletişim sistemi örnek olarak verilebilir (Ortaklık ve İş Birliği,1995, s. 19). NATO'nun çok daha geniş bir perspektifte iş birliği sağlıyor olma özelliği "NATO, demokrasiler ittifakıdır ve üyesi olan tüm ülkelerin parlamentoları NATO ülkelerinin halkı ile NATO liderleri arasındaki en önemli iletişim kanalıdır. NATO'nun aldığı tüm kararlar üye ülkeler arasında tartışma ve istişare sonrasında, oy birliği ile alınmaktadır" ifadesinde daha net olarak anlaşılmaktadır (Ada, 2018, s. 28).

2.2. NATO'nun Siber Güvenlik Stratejileri

Eski savaş sistemlerin etkisinin azalmasıyla birlikte her geçen gün büyüyen ve karmaşık hale gelen siber tehditler ve savaşlar ülkelerin ulusal güvenlikleri açısından daha zararlı hale gelmiştir. Kimilerine göre "kirli savaş" olarak görülen kimilerine göre ise "savaşanların her türlü şiddet ve suç eylemiyle beraber, medyanın ve bilgi akışının da silah olarak kullanılabileceği" bir kavram olarak gördüğü hibrit savaşlar; tarafların birbirleriyle sadece sahada çatışmadığı aynı zamanda, hedef kitlelerinin "zihinleri kazanma savaşı" amacıyla ellerinden geleni yaptığı çatışmadır. Hibrit Savaş'ın hedef kitleleri yalnızca halk değil, aynı zamanda uluslararası aktörlerdir. Askeri avantaj sağlamak kadar, "manevi güç ve zafer" elde etmek için yapılan bu savaşlar hedef ülkenin stratejik internet noktalarını çökertme biçiminde gerçekleştirilir (Altınışık, 2017). Hibrit savaşın bir parçası olarak görülen Siber Savaş da yine ülkelerin hem toplumlarını etkileme hem de bazen direk olarak ülkelerin savunma anlamda stratejik sayılabilecek hedeflerine yönelebilmektedir. NATO ittifakı da soğuk savaşların bitmesiyle birlikte hibrit savaşın parçası olarak görülen bu siber saldırılardan ciddi boyutta etkilenmiş

ve çok çeşitli saldırılara uğramıştır. NATO bu saldırıların sonrasında yeni ortaya çıkan bu tehditlere karşı korunmak amacıyla son yirmi yılda çeşitli stratejiler ve yöntemler üretmiştir. NATO'nun siber güvenlik stratejiler oluşturmasına zemin hazırlayan önemli siber krizler gerçekleşmiştir. NATO da bu krizlerden hareketle siber savunma, siber saldırılara karşı iş birliği gibi alanlarda stratejiler benimsemiştir. Ancak Siber Savunma, konvansiyonel savaş taktiklerine göre dizayn edilmiş askeri güçler için yeni bir alandır ve farklı parametreleri barındırmaktadır. Siber Savunma konusunda düşülebilecek önemli bir yanılgı NATO merkezli bir siber savunma stratejisinin üye devletlerce hemen kabul edilebileceği ve üye devletlerin bu stratejiye hızlı bir şekilde adapte olabilecekleri hususudur. Üye ülkelerin kendi özellik ve altyapılarına göre NATO tarafından geliştirilen/geliştirilecek olan siber güvenlik strateji ve uygulamalarına karşı pozisyon almaktadırlar (Somuncu, 2018, s. 67).

2.2.1. NATO'nun Dâhil Olduğu Siber Kriz Örnekleri

NATO'nun siber güvenlik stratejileri oluşturmasında internetin gelişmesi ve yaygın kullanımıyla beraber artan siber tehditler ve saldırılar etkili olmuştur. Kosova saldırısı, Estonya'ya yönelik siber saldırılar ve Gürcistan krizi NATO'nun strateji oluşturmasında ana tetikleyiciler olmuştur (Arı ve Özdal, 2015, s. 411). Bu bağlamda NATO zaman zaman siber güvenlikle ilgili krizlerle karşı karşıya kalmıştır. Bu krizlerden önemli olanları şu şekilde sıralanabilir:

2.2.1.1. NATO-Kosova Krizi (1999)

Kosova krizi sırasında NATO uçakları yanlışlıkla Çin elçiliğine çarpmış ve Çin Kırmızı Hacker İttifakı NATO ve ABD askeri web sitelerine saldırmıştır. Bu siber saldırı neticesinde, NATO'nun resmî web sitesinin sık sık kesintiye uğradığı ve NATO üye devletlerinin e-posta hesaplarının günlerce erişim dışı olduğu tespit edilmiştir. Bu olay dünya tarihindeki ilk siber savaş olarak tanımlanmaktadır. NATO bu olaydan sonra siber güvenlik alanında ilk adımı atmıştır. NATO, Kosova Savaşı'nda amacına ulaşmış gibi görünse de, siber saldırılar karşısında yetersiz kalmıştır. NATO ülkelerinin web sitelerinde bırakılan mesajlar, saldırganların kim olduğunu ve neden yaptıklarını açıkça göstermektedir. Dolayısıyla bu siber saldırı NATO'yu yeni bir stratejik belge hazırlamaya zorlamıştır (Ada ve Çakır 2017, s. 638). Kosova krizinden sonra çıkarılan resmi NATO belgelerinin hemen hepsi siber güvenlik ve "bilgi sistemlerinin korunması" konularını içermekte idi. Ancak bilgi sistemlerinin nasıl korunacağı, nasıl güvence altına alınacağı ve neyin güvenli olacağı gibi sorulara cevap verememekteydi. Bu belgelerde siber tehditlere nadiren değinilmiş olmasına ve kesin bir çözüm sunmamasına rağmen NATO'nun siber güvenlik konusundaki ilk adımı bu şekilde atılmıştır (Bıçakçı, 2012, s. 212).

2.2.1.2. Estonya Siber Savaşı (2007)

Nisan ve Mayıs 2007'de, Estonya'nın savunma sistemini felç eden kamu ve özel kuruluşların, özellikle devlet kurumlarının, bankaların ve medyaların web sitelerini hedef alan büyük çapta siber saldırılar NATO'nun

siber saldırılar ile ilgili tehdit algısını tamamen değiştirmiştir. Bir başka deyişle, İttifak siber saldırıları "21. yüzyılda siyasi, ekonomik ve BT güvenliğine zarar verebilecek öncelikli bir risk tehdidi olarak tanımlamıştır. Sonraki yıl yapılan 2008 Bükreş Zirvesi'nde, üye devletlerin siber saldırılara karşı kapasitelerinin geliştirilmesi ve bu bağlamda savaş stratejilerinin oluşturulması ihtiyacı bir kez daha güçlü bir şekilde teyit edilmiştir. Bu çerçevede NATO, onayladığı siber savunma politikası kapsamında "Sanal Savunma Yönetim Otoritesini" (CDMA) ve Estonya merkezli Merkez Siber Savunma Mükemmeliyet Merkezini (CCD COE) kurmuştur (Seren, 2016, s. 16-17).

2.2.1.3. Gürcistan Siber Savaşı (2008)

Gürcistan'da ayrılıkçı grubun provokasyonuna Gürcistan güçlerinin karşılık vermesi üzerine 7 Ağustos 2008'de gerçekleşen olayların hızla büyümüş ve akşam saatlerinde hadiseler Gürcistan'a siber saldırılarla sıcak bir çatışmaya dönüşmüştür. Gürcistan'ın bilgi altyapısının Estonya kadar gelişmiş olmaması, saldırının yol açtığı zararın etkisini azalttığı, ancak olayların gelişimi ve saldırı sırasında izlenen yöntemlerin Estonya'dakilerle neredeyse aynı olduğu görülmüştür (Bıçakcı, 2014, s. 101-130). Gürcistan'a yapılan siber saldırıların en önemli sonucu gerçek bir melez savaş olmasıdır. Geleneksel savaş yöntemlerini kullanarak, Rusya aynı anda siber saldırılara başlamıştır. Bu savaş, Rusya'nın karma savaşı olarak tanımlanabilir. Ayrıca hem geleneksel hem de siber alanda cereyan eden çatışmalar NATO'nun melez savaşa olan inancını güçlendirmiştir (Bıçakçı, 2012: 205-226). Gürcistan'daki siber saldırıların ardından Kasım 2008'de NATO Ortak Siber Savunma Mükemmeliyet Merkezi (CCDCOE), "Gürcistan'a Karşı Siber Saldırılar:

Belirlenmiş Hukuki Dersler" başlıklı bir açıklama yapmıştır. Rapor, Silahlı Çatışma Kanunu'nun SOO'nun Rusya-Gürcü Savaşı sırasındaki siber saldırılara karşı uygulanabilirliği hakkında fikirler öne sürmektedir (Ada ve Çakır, 2017, s. 639).

3. Nato Üyesi Ülkelerin Siber Güvenlik Çalışmaları

Bugün dünyadaki en önemli uluslararası kuruluşlardan biri olan Kuzey Atlantik Antlaşması Örgütü 30 ülkeyi bir araya getirmiştir. NATO üye ülkelerine bakıldığında siber güvenlik alanına en çok önem veren devletlerin ABD ve Almanya olduğu görülmektedir. Çalışmanın bu bölümünde NATO üye ülkelerinden; ABD, Almanya, Estonya, Birleşik Krallık, Fransa, Kanada ve Türkiye'nin siber güvenlik faaliyetleri kısaca incelenmiştir.

3.1. ABD

ABD, siber güvenlik, siber uzay konularında diğer ülkelere önder konumdadır. Özellikle Avrupa ve Asya'daki ülkelere siber sorunlarla mücadele konusunda örnek olarak bir rol model durumuna gelmiştir. 11 Eylül 2001'deki ABD'deki saldırıların ardından siber güvenlik ve kritik bilgi altyapılarının korunması alanlarında çeşitli değişiklikler yapılmıştır. Siber güvenliğin sağlanması için DHS bünyesinde Altyapı Koruması (OIP) ve Siber Güvenlik ve İletişim Departmanı (CS&C) kurulmuştur. OIP, mevcut altyapıların korunması konusundaki çalışmalarını koordine etmekten, mevcut altyapı sektörlerindeki güvenlik açığı değerlendirmesine yönelik çalışmaları desteklemekten ve uluslararası güvenlik kültürünün oluşturulmasını teşvik eden uluslararası programlar ve ilişkiler kurmak ve sürdürmekten ve ayrıyeten

kritik altyapıların korunmasından sorumludur. Öte yandan CS&C, siber tehditler, risk yönetimi, acil durumlarda iletişim ve müdahale merkezlerinin kurulması gibi konularda özel sektör ile işbirliği kurmaya yetkilidir (Turhan, 2010, s. 103).

3.2. Almanya

Almanya siber güvenlik yarışına ABD'den daha sonra başlamıştır. 2011 yılında ilk ulusal siber güvenlik stratejisini oluşturmuş, ancak o yıldan sonra büyük ve hızlı bir gelişme göstermiştir. Almanya 2015 yılında siber güvenlikle ilgili stratejisini günün şartlarına göre revize etmiştir. Stratejilerinde, Almanya kritik bilgi sistemi altyapılarının korunmasına önem vermektedir. Ek olarak, internet kullanımının her geçen gün artması ve yayılmasıyla, sadece her ülkenin kendi sistemlerinde değil diğer ülkelerin sistemlerindeki saldırılardan da etkilenebilecek duruma gelinmiştir. Bu nedenle de siber güvenlik ve siber savunma mekanizmalarının uluslararası düzeyde önemi ve iş birliğinin gerekliliği Almanya'nın ilgili stratejilerinde vurgulanmaktadır. Ayrıca stratejide Birleşmiş Milletler, Avrupa Birliği, NATO, G8 ve diğer uluslararası kuruluşların birlikte çalışması gerektiğini vurgulamaktadır. Almanya'daki kritik altyapıların siber tehditlerden korunmasından ve bu konudaki çalışmaların koordinasyonundan sorumlu olan Federal Bilgi Güvenliği Ofisi'nin (BSI), 2011 yılında hazırlanan ve daha sonradan güncellenen stratejik planın ardından yetkileri arttırmıştır. Ancak Almanya günümüzde siber güvenlik konusunda ABD tarafından geliştirilen askeri yazılımlarına kısmen bağlı kalmaya devam etmektedir (Sanalp ve Denker, 2016, s. 28,30).

3.3. Estonya

2007'de Estonya'ya yapılan siber saldırılar, ülkenin siber yeteneklerini ve politikalarını ciddi şekilde sorgulamasına sebep olmuştur. Olaylar sonucunda Estonya'daki siber savunma faaliyetleri Savunma Bakanlığı nezaretinde yürütülmeye başlanmıştır. Ayrıca, Estonya'da Savunma Birliği adlı bir kuruluş ülkenin siber savunma kuvvetlerini iyileştirmek için çalışmalar yürütmektedir. Savunma Birliğinin bir parçası olan Siber Güvenlik İttifakı, görevlerini üç ana başlık altında yerine getirmekle sorumludur. Bu görevler;

- Estonyalıların elektronik hayatlarını korumak,

- BT uzmanlarının eğitimi,

- Siber Savunma ile ilgili kamuoyu bilgilendirme faaliyetlerinde bulunmak şeklinde sıralanabilir. Bir NATO üyesi olan Estonya, NATO altındaki Bilgi Güvenliği alanında uluslararası iş birliğinin önemini tecrübe etmiş ve bu amaçla aktif bir rol oynayan ülkelerden birisidir. Bu iş birliğiyle savunma yetkinliğini arttırmanın yanı sıra NATO üyesi ülkelere de katkı sağlamaktadır. 2008 yılında Tallinn'de bir NATO kuruluşu olarak kurulan Siber Savunma Mükemmeliyet Merkezi, üye ülkeler arasındaki iş birliğini artırmak, bilgi paylaşmak ve siber güvenlik alanında araştırma yapmak için çalışmalar yapmaktadır (İstanbul Bilgi Üniversitesi Bilgi ve Teknoloji Hukuku, 2012, s. 22, 23).

3.4. Birleşik Krallık

Ekim 2010'da İngiltere hükümeti Ulusal Güvenlik Strateji Raporunu İngiliz parlamentosuna sunmuş ve bu rapor kabul edilerek yayınlanmıştır. Bu rapor, Birleşik Krallık'ın karşılaşabileceği riskleri gruplara ayırmış ve siber saldırıları en yüksek risk grubu olarak kabul etmiştir. Raporda ayrıca siber saldırı alanındaki diğer ülkelerin siber saldırıları ve terörist grupların ve örgütlü ağların yönlendirdiği siber saldırılar da konu edilmiştir. Ulusal Güvenlik Strateji Raporu, birçok ülkenin Birleşik Krallık'a siber saldırılar gerçekleştirdiğini açıkça göstermektedir ve siber güvenliğin, rapor yılı boyunca ve takip eden beş yıl boyunca en yüksek dereceli ulusal güvenlik risklerinden biri olarak görülmesi gerektiğini vurgulamaktadır (İstanbul Bilgi Üniversite Bilgi Teknolojisi ve Teknolojisi Hukuk Enstitüsü, 2012, s. 30).

3.5. Kanada

Kanada'da siber güvenliğin sağlanması ve siber olaylarla mücadelede ulusal ve uluslararası mevzularda liderlik görevi üstlenen Kanada Siber Olaylara Müdahale Merkezidir (CCIRC). CCIRC, gerçek zamanlı olarak herhangi bir siber tehlike olup olmadığını incelemekte ve anında müdahale etmektedir. Merkez, kritik altyapı sektörlerine olaylara müdahale, koordinasyon ve destek sağlama, izleme ve siber güvenlik tehditleri analiz etme; bilgi teknolojileri alanlarında danışmanlık sağlama ve farkındalığın artırılması ile ilgili eğitim faaliyetleri yürütmektedir (Turhan, 2010, s. 114-115).

3.6. Fransa

Fransa'nın siber alandaki ulusal stratejisi; siber güvenliği sağlamak ve bu alanda kararlı politikalar çizmek olarak belirlenmiştir. Fransa'nın bilgi güvenliği konusundaki çalışmaları, İkinci Dünya Savaşı'na kadar uzanmaktadır. 1943'te Fransız ulusal direnişi altındaki Fransız topraklarının çoğunluğu ile 1943'te Fransız ulusal direnişiyle kurulan Direction Technique du Chiffre (DTC), savaş sırasında Almanların şifreli iletişimi önlemeye çalışmış ve direnişin de iletişiminin gizliliğini sağlamıştır. Savaştan sonra, 1953 yılında, birim, Service Central Technique du Cchiffre STC-CH'ye dönüşmüştür. 1977 yılında kurulan İletişim Güvenliği ve Parola Hizmetleri Merkezi (Service Central du Chiffre et Sécuritédes Télécommunications), 1986 yılında Bilgi Sistemleri Güvenliği Merkezi'ne (Service Central de la Sécuritédes Systèmes D'information-SCSSI) dönüştürülmüştür. Merkez daha sonra Direction Centrale de la Sécuritédes Systèmes Bilgi Sistemleri Güvenlik Merkezine (DCSSI) dönüştürülmüştür. Fransa'da bilgi güvenliği politikalarının uygulanmasını koordine etmek amacıyla, DCSSI 2008'de Fransız Ulusal Bilgi Güvenliği Ajansı (ANSSI) ile değiştirilmiştir. Fransa'ya yeni bir kavramsal güvenlik çerçevesi sağlayan Ulusal Güvenlik ve Savunma Hakkında Beyaz Kitap (Défense et Sécuriténationale: Le Livre Blanc), Fransa'nın siber ortamdaki savunma kapasitesinin arttırılması gerektiğini vurgulamaktadır. Devletin en önemli görevlerinden biri olarak, ulusal bilgi sistemlerinin güvenliğinin sağlanması ve hem ISS'ler hem de kritik altyapı sağlayıcıları ile kamu kurumları arasında etkin koordinasyonun temin edilmesi olarak belirtilmiştir. Beyaz Kitap, Fransa'nın ulusal güvenlik tehdidinin başında siber saldırılar

görmekte ve bu riski en aza indirmek için bir koordinasyon yapısı oluşturulması önermektedir. Beyaz Kitap ile önerilen koordinasyon yapısı, kitabın yayınlanmasından sonra kurulmuş ve ANSSI olarak adlandırılmıştır. ANSSI'nin görevlerinden bazıları şunlardır:

- Siber Güvenlik Operasyon Merkezi ile iş birliği içinde, devlete yönelik siber saldırılara karşı zamanında hareket etmek ve kamu kurumlarının ve elektronik kamu hizmetlerinin sunulduğu ağların bu tür saldırılara hazırlanmak için gerekli önlemleri almasını sağlamak,

- Kamu ve özel sektör kuruluşlarının bilgi güvenliği risklerini önlemek,

-Kamu kurumlarının ağ ve ürün güvenliği alanında ihtiyaç duyduğu güvenlik ekipmanını sağlamak veya geliştirmek

-Devletin bilgi güvenliği politikalarının askeri kurumlarla iş birliği ve uyum içinde uygulanmasını sağlamak (Güngör, 2015, s. 85-86-87).

3.7. Türkiye

Türkiye'nin siber güvenlik stratejisi çalışma tarihi oldukça yakındır. Siber güvenlik açısından öne çıkan en önemli çalışmalardan biri, bu alanı düzenleyen bazı yasaların onaylanmasıdır. 2004 yılında kabul edilen 5070 sayılı Elektronik İmza Kanunu ile 2008 yılında iletişim sektörünü düzenlemek üzere kabul edilen Elektronik İletişim Güvenliği Yönetmeliği bu düzenlemelerden ilk olanlardır. Ayrıca, Yüksek Planlama Kurulu kararında yer alan Bilgi Toplumu 2006/38, 2006 yılında 28242 sayılı Resmi Gazete'de yayımlanmıştır. Ayrıca konu ile ilgili bir Strateji ve Ek Eylem Planı

geliştirilmiştir. Bu plan içerisine öncelikle bilgi güvenliği için yasal düzenlemeler yapılması ve bilgisayar etkinlikleri ve kamu kurumlarının bilgi güvenliğini sağlamaya yönelik faaliyetler için acil bir müdahale merkezi kurulması yer almıştır. Bu kapsamda, Bilgisayar Olayları Müdahale Ekibi (TR-BOME), TÜBİTAK Bilgi ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi (BİLGEM) kurulmuştur. Siber güvenlik konusunda en somut adım, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetimi ve Koordinasyonu ile ilgili 2012/3842 Bakanlar Kurulu Kararıdır. Siber güvenlikle ilgili kararları belirlemek, 155 Siber Suç ve Türkiye'nin Siber Güvenlik Politikası planlarını, programlarını, raporlarını hazırlamak, ilkeleri ve standartları onaylamak ve uygulamalarını ve koordinasyonlarını sağlamak için" Siber Güvenlik Konseyi" kurulmuştur. Konsey içerisinde Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Dışişleri Bakanlığı Müsteşarlığı, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarlığı, Ulusal İstihbarat Teşkilatı Müsteşarlığı, Genelkurmay Başkanlığı, Haberleşme Elektronik ve Bilişim Sistemleri Müdürlüğü, Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) Başkanlığı, Mali Suçları Araştırma Kurulu Başkanlığı, Telekomünikasyon İletişim Başkanlığı ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'ndan üyelerin bulunması kararlaştırılmıştır. Ulusal siber güvenliğin sağlanması amacıyla politika ve strateji geliştirme ve eylem planları hazırlama görevi Ulaştırma Bakanlığına verilmiştir. Ulaştırma Bakanlığı da ilgili kurum ve kuruluşların görüşlerini alarak bir siber güvenlik eylem planı hazırlamıştır (Hekim & Başıbüyük, 2013, s. 154-155).

Sonuç

Teknolojik gelişmelerin hızlı bir biçimde ilerlemesi ile insanların yaşamında birçok değişim olmuştur. Bu değişiklikler birçok alanda fayda sağladığı gibi bazı tehlikeleri de beraberinde getirmektedir. Bu tehlike ve tehditler bireysel ve toplumsal boyutu aşıp devletler için de geçerli olmaya başlamıştır. Siber saldırılar var olan güvenlik tedbirlerinin arttırılmasını teşvik etse de ama çoğu ülke kritik bilgi ve altyapılarını korumakta yetersiz kalmaktadır. Siber uzaydaki güvenlik açıklarının diğer ülkelere de zarar verme ihtimali ve potansiyeli çok yüksek olduğundan ötürü küresel bir hal alan siber savaşlar, saldırılar vb. için ortak düzenlemeler ve çözümler gerekmektedir. Hâlihazırda üyeleri arasında birincil olarak savunma iş birliği kuran NATO'nun siber saldırılara karşı benimsediği strateji ve aldığı tedbirler ile NATO üyesi bazı ülkelerin siber güvenlik hususundaki çalışma, tedbir ve politikaları bu çalışmaya konu edilerek meselenin, ulusal boyuttan çok uluslararası bir boyutunun olduğu ve klasik "blok" çerçevesinde cereyan etmese bile Soğuk Savaş sonrası oluşan yeni dünya düzeni dinamiklerinden de tamamen bağımsız olmadığı vurgulanmak istenmiştir. 1999 Kosova krizi sırasında Çin'in ABD'nin ve NATO'nun web sitelerine saldırması dünyada ilk siber saldırı olarak görülmüştür. Sonrasında da 2007 yılında ise NATO üyesi Estonya'nın uğradığı siber saldırı sonucunda ülkede pek çok online işlem gerçekleştirilememesi saldırının ardından Estonya'da ordu bünyesinde siber savaş birimi kurulmasına sebep olmuştur. Estonya krizinin ardından birçok siber saldırıya uğrayan NATO güçlü stratejiler oluşturularak siber güvenlik adına çeşitli stratejiler geliştirmeye çalışmalar yapmaya başlamıştır. Bu durum

NATO üyelerinden herhangi birisine yapılacak geleneksel olmayan herhangi bir saldırının da NATO ve üyesi ülkeler için kayda değer bir güvenlik meselesi olduğunun göstergesidir. Bireysel olarak NATO ülkelerinin BT altyapılarına veya NATO'nun bizzat kendi BT altyapılarına yapılan siber saldırılar, NATO ittifakının savunma amaçlı ve silah sistemlerinde kullandığı bilgi işlem altyapılarını da tehlikeye atmaktadır. Günümüzde teknolojik gelişmelerin geldiği nokta düşünüldüğünde siber saldırı, siber savaş, siber güvenlik vb. gibi kavramların ne kadar ulusal ve uluslararası güvenlik stratejileri içerisinde yer alması gerektiği anlaşılacaktır. Zaten NATO üyesi çeşitli ülkelerin özellikle ABD, Almanya, Fransa gibi güçlü ülkelerin, siber tehlikenin farkında oldukları ve ciddi çalışmalar yürüttüğü ve siber tehditlere karşı önlem aldıkları görülmektedir. NATO'nun dünya üzerindeki savunma ve güvenlik anlamındaki etki alanı düşünüldüğünde NATO ve/veya üyeleri tarafından benimsenen siber güvenlik strateji ve tedbirleri, konunun Uluslararası İlişkiler alanının odak noktası haline gelmeye başladığını göstermektedir.

Kaynaklar

Makaleler

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

Akyeşilmen, Nezir. "Rethinking Cybersecurity: A Quick Transformation." Cyberpolitik Journal 2.3 (2017): 173-179.

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

Bıçakcı, S. (2014). Nato'nun Gelişen Tehdit Algısı: 21. yüzyılda siber güvenlik. Uluslararası İlişkiler Dergisi, 10(40), 100-130.

Darıcılı, B. (2015). Nato'nun Siber Güvenlik Stratejisi'nin Analizi. Uluslararası İlişkiler Konferansı Uluslararası Sistemde Yeni Düzen Arayışları, 21-22 Ekim 2015, s.407-417.

Güngör, U., & Güney, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş. Karadeniz Araştırmaları, (55), 131-146.

Güntay, V. (2018). Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler. Güvenlik Stratejileri

Gürkaynak, M., & İren, A. A. (2011). Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 16(2), 263-279.

Gürkaynak, M. (2005). Soğuk Savaş Sonrasında Nato ve Avrupa Güvenliği. Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, (1), 7-27.

Hekim, H., &Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Dergisi, 14(27), 79-111. Güvenlik Politikaları. Uluslararası Güvenlik ve Terörizm Dergisi, 135-158.

Raporlar

Dijital Türkiye Platformu, (2017). Türkiye'nin Siber Güvenlik Stratejisine Yönelik Değerlendirmeler. İstanbul: Dijital Türkiye.

İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, (2012). Siber Güvenlik Raporu. İstanbul: İstanbul Bilgi Üniversitesi Bilişim Ve Teknoloji Hukuku Enstitüsü.

Seren, M. (2006). Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık. Ankara: Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA) Analiz, (183).

Ulaştırma D. & Bakanlığı, H. (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Ankara, 8(2018), 2013-2014.

Tezler

Ada, M. (2018). NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi. Ankara: Adli Bilişim Ana Bilim Dalı, Yüksek Lisans Tezi.

Aytekin, A. (2015). Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi. Ankara: Yayımlanmamış Yüksek Lisans Tezi, Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi.

Güngör, M. (2015). Ulusal Bilgi Güvenliği Strateji ve Kurumsal Yapılanma. Ankara: Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı Uzmanlık Tezi.

Sanalp, S. (2016). Çeşitli Ülkelerde Usom ve Some Yapılandırılması ve Türkiye Modeli Önerisi. İstanbul: İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Bilgi Üniversitesi Doktora Tezi.

Somuncu, G. (2018). NATO'nun Güvenlik Alanında Yeni Bir Boyut: Siber Güvenlik. İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi.

Tarhan, K. (2018). Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik. Konya: Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi.

Turhan, M. (2010). Siber Güvenliğin Sağlanması Dünya Uygulamaları ve Ülkemiz İçin Çözüm Önerileri. Ankara: Bilgi Teknolojileri ve İletişim Kurumu Uzmanlık Tezi.

Kitaplar

Armaoğlu, F. (1989), 20. Yüzyıl Siyasi Tarihi, 1914-1995 (Ankara: Türkiye İş Bankası Kültür Yayınları,229-230).

NATO. (1995). NATO El Kitabı Ortaklık ve İşbirliği. Brüksel: NATO Basın Yayın ve Enformasyon Bürosu.

Sarınay, Y. (1988). Türkiye'nin Batı İttifakına Yönelişi ve NATO'ya Girişi. Ankara: Kültür ve Turizm Bakanlığı Yayınları Kültür Eserleri Dizisi.

İnternet Kaynakları

Siber Güvenlik Nedir? https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security Erişim Tarihi: 24.03.2019

NATO. (2017). Kuzey Atlantik Antlaşması Örgütü (NATO) https://www.nato.int/nato-welcome/index_tr.html Erişim Tarihi: 12.02.2019

Altınışık, H. Hibrit Savaş ve Siber Saldırılar. http://webcache.googleusercontent.com/search?q=cache:bHvUyQuekg4J:www.siberteror.org/siberteror2017/files/HalimAltinisik.pdf+&cd=5&hl=tr&ct=clnk&gl=tr Erişim Tarihi: 01.10.2019.

NATO. (2010). NATO'yu Keşfedin https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20111116_Discover_NATO_TUR.pdf. Erişim Tarihi: 12.02.2019.