Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi

Mehmet ADA[a*], Hüseyin ÇAKIR[b]

[a]*Adli Bilişim Anabilim Dalı, Gazi Üniversitesi,Bilişim Enstitüsü, Ankara, TÜRKİYE*

[b]*Bilgisayar ve Öğretim Teknolojisi Eğitimi, Eğitim Fakültesi, Gazi Üniversitesi, Ankara, TÜRKİYE*

** Sorumlu yazarın e-posta adresi: mehmetada@gazi.edu.tr*

ÖZET

Son yıllarda bilgi ve iletişim teknolojilerinde gerçekleşen gelişmeler ile coğrafik sınırların yerini sanal ortamda belirlenen dijital sınırlar almıştır. Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletlerin uluslararası anlaşmalar yapmasını kaçınılmaz hale getirmiştir. Bu çalışmada, küreselleşen dünyada ülkeleri aynı çatı altında birleştiren en büyük organizasyonlardan biri olan NATO'nun uyguladığı siber güvenlik stratejisi incelenerek, Türkiye'nin uyguladığı siber güvenlik stratejisine olumlu katkılar yapmak amaçlanmıştır.

***Anahtar Kelimeler*:** Siber güvenlik, NATO, strateji, siber saldırı, siber savaş.

Investigation Of Cyber Security Strategy Of North Atlantic Treaty Organisation (NATO)

ABSTRACT

Because of the fact that developments taking place in recent years in information and communication technology, digital boundaries has taken the place of the geographical boundaries. The challenges of protecting national interests against cyber attacks and ensuring the border security of cyberspace has made it inevitable for governments to make international agreements.In this study, it is aimed to make a positive contribution to the cyber security strategy implemented by Turkey by examining the cyber security strategy applied by NATO, one of the biggest organizations that unite countries under the same roof in the globalizing world.

***Keywords*:**Cyber security, NATO, strategy, cyber attack, cyber warfare.

Geliş: 31/10/2016, Düzeltme:26/03/2017, Kabul: 27/03/2017

I. GİRİŞ

Küresel çapta internetin hızla gelişmesi ve askeri, siyasi, ticari alanda yeni bir araç olarak kullanılması, devletlerin ulusal ve uluslararası güvenlik açısından siber güvenliği birinci önceliğe almasına neden olmuştur. Bilgisayar ağları üzerinde ortaya çıkan tehditler kişisel, kurumsal hatta küresel bakımdan önemli sonuçlar doğurmaktadır. İnternet bankacılığı yapmakta olan kişinin hesabında gerçekleşecek bir dolandırıcılık hadisesi, sadece o kişinin zarar görmesine sebep olurken; bir kurumun veri tabanına karşı yapılan saldırı tüm kurum çalışanlarının ve kurumla irtibatlı olan kişilerin kimlik bilgilerinin ele geçirilmesine, hatta kurumun milli güvenliğe yönelik önemli bilgilerinin yetkisiz insanların eline geçmesine sebep olmaktadır.

Bilgisayar güvenliği ve kriptografi üzerine önemli kitapları bulunan Bruce Schneier teknolojinin gelişmesiyle değişen güvenlik algısını şöyle özetlemiştir:

"Eğer teknolojinin güvenlik sorunlarını çözebileceğini düşünüyorsanız, teknolojiyi de sorunları da anlamamışsınız demektir." [1]

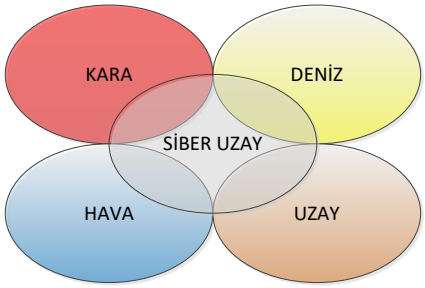
Bir devletin gizli bilgilerinin diğer devletler tarafından bilinmesi ve ya ele geçirilmesi, o devletin zayıf yanlarının ortaya çıkmasına dolayısıyla ülkenin itibar kaybetmesine neden olacaktır. Söz konusu tehditlerin yaygınlaşması, ülkelerin ulusal siber güvenlik tedbirleri almasına ve güvenlik stratejileri uygulamasına zemin hazırlamıştır. 11 Eylül saldırısının ardından ABD Hükümetinin kurduğu İç Güvenlik Bakanlığı (Department of Homeland Security) tarafından 2003 yılında hazırlanan "Siber Uzayın Güvenliği İçin Ulusal Strateji Belgesi (National Strategy to Secure Cyberspace)" dünya devletleri arasında yayınlanan ilk ulusal siber güvenlik yol haritası olma özelliğini taşımaktadır. Diğer ülkelere ilham kaynağı olan ilk ulusal siber güvenlik strateji planı aşağıda belirtilen temel amaçlar doğrultusunda hazırlanmıştır:

1. Ulusal kritik altyapılara karşı gerçekleştirilen siber saldırıları önlemek,
2. Siber saldırılara karşı ulusal güvenlik açığını azaltmak,
3. Siber saldırılar tarafından oluşacak hasarları ve hasarların iyileşme sürecini en aza indirmek. [2]

Sanal ortamda belirlenen dijital sınırlar ulusal sınırlarla örtüşmemektedir. Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletlerin uluslararası anlaşmalar yapmasını kaçınılmaz hale getirmiştir. NATO CCDCOE, ENISA ve ITU gibi uluslararası organizasyonlar aracılığıyla ülkeler siber saldırılara karşı dijital sınırlarını korumakta ve müşterek siber güvenlik stratejileri geliştirmektedir.

II.SİBER GÜVENLİK, SİBER SALDIRI VE SİBER SAVAŞ DENKLEMİ

"Siber Uzay" kavramı ilk olarak 1982 yılında bilim kurgu romanlarıyla bilinen William Gibson tarafından "Burning Chrome" adlı romanda kullanılmıştır. Ulusal Siber Güvenlik Stratejisinde "siber uzay" teriminin yerine "siber ortam" teriminin kullanılması tercih edilmiştir. Beşinci boyut olarak da tanımlanan siber uzay; şekil-1'de görüldüğü gibi yeryüzü, hava, deniz hatta uzaydan bağımsız ve iletişim altyapılarını kullanan sanal bir ortamdır [3].



Şekil 1 *- Siber Uzay*

Siber güvenlik; bütünlük, gizlilik ve erişilebilirlik prensipleri ışığında bilgi ve erişim güvenliğini sağlamak için kullanılan araç ve yöntemlerin birleşimi olarak tanımlanabilir [4].

Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır. Günümüzde oluşan tehditler ve bu tehditlerden bireylerin ve kurumların gördükleri zararlar göz önüne alındığında siber güvenliğin önemi daha iyi anlaşılacaktır. Eski ABD Başkanı Obama 29 Mayıs 2009 yılındaki sunduğu siber güvenlik yasası önerisinde siber güvenliğin önemini şöyle ifade etmiştir:

> *"Biz enerji dağıtımında, gaz dağıtımında ve su dağıtımında bilgisayar ağ altyapımıza güveniyoruz. Biz toplu taşıma ve hava trafik kontrolü için de ağ altyapımıza güveniyoruz. Ancak, bu altyapıların güvenliğine yatırım yapma konusunda başarısız olduk. Mevcut durum artık kabul edilemez. Tehdit altında birçok yatırımımız mevcut. Biz daha iyisini yapabiliriz ve yapmalıyız."*[5]

Siber güvenliğin birçok boyutu olmasına rağmen temel olarak aşağıdaki şekilde gösterilen yedi prensipten oluşmaktadır.

Şekil 2 *- Siber Güvenlik Prensipleri*

General James Cartwright siber saldırıyı; bilgisayar, bilgisayar ağları ve ya sistemler kullanılarak düşmanın kritik sistemleri, varlıklarını yok etmeyi ve görevlerini yapamaz hale getirmeyi amaçlayan düşmanca bir davranış olarak tanımlamıştır[6].

Virüs, Truva atı, solucan, casus yazılım, tuş kaydediciler, fidye yazılımları gibi zararlı yazılımlar kullanılarak yapılan saldırılar, oltalama saldırıları, istenmeyen e-posta saldırıları, trafiğin dinlenmesi, ortadaki adam saldırısı, zombi bilgisayarlar ve sosyal mühendislik saldırıları en yaygın kullanılan saldırı yöntemleridir.

Eski ABD Başkanı Bush'un Siber güvenlik danışmanı Richard A. Clarke "Cyber War" adlı kitabında siber savaşı, bir devletin, diğer bir devletin bilgisayar sistemlerine ve ya ağlarına hasar vermek ya da bozmak amacıyla gerçekleştirdiği faaliyetler olarak tanımlamıştır[7].

2010 yılında yayınlanan "Clatham House Report" siber savaşı diğer savaşlardan ayıran en temel özellikleri aşağıdaki başlıklar altında sıralamıştır[8].

1. Silahlı çatışmaya gerek kalmadan siyasi ve stratejik hedeflere ulaşmayı mümkün kılar.
2. Küçük ve nispeten önemsiz aktörlere orantısız güç imkânı verir.
3. Sahte IP adresleri ve yabancı sunucuların arkasında faaliyet göstererek kısa süre anonimlik sağlayabilir.
4. Konvansiyonel harpten farklı olarak kara, deniz, hava, uzay haricinde siber uzay olarak tanımlanan beşinci boyutta icra edilir.
5. Klasik harp çatışma ve baskı rejimi gibi unsurlardan sonra ortaya çıkmasına rağmen siber savaş fiziksel baskı ve çatışma ortamından uzaktır.

Siber savaş ve siber saldırı birbirinden farklı hususlardır. Siber saldırılarda hedef kişi, şirket, kurumlar iken siber savaş ülkeleri hedef almaktadır. Siber savaş, siber saldırı ve siber savunmayı ihtiva eden daha genel bir kavramdır[9].

Şekil 3 – Siber Savaş Denklemi

III. NATO VE SİBER GÜVENLİK

A. NATO Tarihçesi

İkinci Dünya Savaşının sona ermesi ile birlikte güç dengeleri değişmiş ve savaşın yol açtığı yıkımla zayıflayan Batı Avrupa ülkelerinin aksine; Amerika Birleşik Devletleri ve Rusya iki süper güç olarak tarih sahnesine çıkmıştır. 1945-1949 yılları arasında Amerika Birleşik Devletleri ve Batı Avrupa ülkeleri savaş sonrası yaralarını sarmak için savunma yapılanmalarını küçültme ve savunma kuvvetlerini düşürme yolunu seçerken; Rusya, Doğu Avrupa'da yayılmacı politikayı izlemiş ve savunma yapılanmalarına hız kesmeden devam etmiştir. Rusya'nın yayılmacı politikası karşısında kendilerini tehlikede hisseden Batı Avrupa ülkeleri ve Kuzey Amerika ülkeleri tarafından 4 Nisan 1949 tarihinde imzalanan ve 14 maddeden oluşan Washington Antlaşması ile Kuzey Atlantik Antlaşma Örgütü (NATO) ittifakı kurulmuştur.

Kurulduğu tarihten itibaren günümüze kadar gelen süreçte ittifaka katılım durumu aşağıdaki çizelgede verilmiştir[10].

***Tablo 1**- NATO Ülkeleri*

KATILIM TARİHİ	ÜLKELER	GENİŞLEME
4 Nisan 1949	Belçika	Kurucu Üyeler
	Kanada	
	Danimarka	
	Fransa	
	İzlanda	
	İtalya	
	Lüksemburg	
	Hollanda	
	Norveç	
	Portekiz	
	Birleşik Krallık	
	Amerika Birleşik Devletleri	

18 Şubat 1952	Yunanistan	İlk Genişleme
	Türkiye	
9 Mayıs 1955	Almanya	İkinci Genişleme
30 Mayıs 1982	İspanya	Üçüncü Genişleme
12 Mart 1999	Çek Cumhuriyeti	Dördüncü Genişleme
	Macaristan	
	Polonya	
29 Mart 2004	Bulgaristan	Beşinci Genişleme
	Estonya	
	Letonya	
	Litvanya	
	Romanya	
	Slovakya	
	Slovenya	
1 Nisan 2009	Arnavutluk	Altıncı Genişleme
	Hırvatistan	

B. NATO Organizasyon Yapısı

NATO içerisinde oluşturulan yapılar, üye ülkelerin politikalarını temel görevleri yerine getirebilecek şekilde koordine etmelerine olanak sağlar. Bu yapılar politik, ekonomik ve askeri olmayan diğer konular üzerinde olduğu kadar, 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 sunarlar[11].

NATO bir demokrasiler ittifakıdır ve üyesi olan ülkelerin parlamentoları NATO ülkelerinin vatandaşları ile NATO liderleri arasındaki en önemli iletişim kanalıdır. Tüm NATO kararları üye ülkeler arasında tartışma ve istişare sonrasında, oy birliği ile alınır. Aşağıdaki şekil NATO'nun karar verme sürecini özetlemektedir.

Şekil 4 *– NATO Karar Verme Süreci*

C. NATO Siber Güvenlik Stratejisini Etkileyen Siber Savaşlar

NATO ittifakı uzun bir süredir söz konusu karmaşık tehdit ortamıyla karşı karşıyadır. NATO son yirmi yıl içerisinde siber saldırılara karşı savunmasını güçlendirmek, yeni tedbirler üretebilmek için bazı yöntemler ve stratejiler uygulamaktadır. Bu süreç içerisinde NATO'nun siber güvenlik tedbirleri üretmesine zemin hazırlayan üç önemli siber savaş gerçekleşmiştir.

1. NATO-Kosova Krizi (1999)

NATO uçakları Kosova Savaşı esnasında Sırbistan'ı bombalamaya başlayınca, "Black Hand" gibi Sırp yanlısı ve Batı karşıtı hacker grupları NATO'nun internet altyapısına saldırmaya başladı. Siber saldırıların, Yugoslavya Federal Cumhuriyeti'nin askeri kuvveti için gerçekleştirilip gerçekleştirilmediği tespit edilemese de, NATO'nun askeri operasyonlarını bozmayı hedeflediği ortadadır. "Black Hand" hacker grubu ismini, 1'inci Dünya Savaşı'nın başlamasına sebep olan Pan-Slav gizli bir topluluktan almıştır. Savaş sırasında "Black Hand" hacker grubunun NATO'ya ait en önemli bilgisayarları ele geçirdiği ve bilgisayarlar üzerindeki tüm verileri sildiği iddia edilmiştir[12].

NATO, Kosova Savaşı'nda amacına ulaşmış gibi görünse de siber saldırılar karşısında yetersiz kalmıştır. NATO'ya yapılan saldırıda, web sitelerine bırakılan mesajlar, saldırganların kim olduklarını; olayın evveliyatına bakıldığında ise neden bu saldırıyı yaptıklarını açıkça göstermektedir. Kosova'da maruz kalınan siber saldırılar NATO'yu yeni bir stratejik doküman hazırlamaya zorlamıştır.Bu dokümanda siber tehditlere çok az değinilmiş olsa da NATO'nun siber güvenlik alanında ilk adımı bu şekilde atılmıştır.

2. Estonya Siber Savaşı (2007)

Estonya siber savaşı Sovyetler Birliği'nin Estonya üzerinde baskıcı 50 yılının sonucu olarak ortaya çıkmıştır. Sovyetler Birliğinin 1989 yılında dağılması, Estonya'nın bağımsız bir devlet olarak yerini almasını sağlamıştır. Siber saldırılar, Estonya hükümetinin başkenti Talinn'de bulunan ve Estonyalıları

Nazi işgalinden kurtaran Rus askerlerinin hatırası için 1947 yılında dikilen Kızıl Ordu Anıtı'nın kaldırmasından hemen sonra başlamıştır[13].

Saldırıların başladığı 27 Nisan tarihinden itibaren Estonya Devlet sitelerinin internet trafiğinin yaklaşık 400 kat artış göstermesi saldırıların daha önceden planlandığını ve iyi koordine edildiğini göstermektedir. Saldırganlar dünya üzerinde dağıtık yapılandırılmış binlerce zombi bilgisayar kullanarak, kısa sürede Estonya Devlet sitelerine hizmet dışı bırakma (DDoS) saldırısı gerçekleştirmiş, Estonya Reform Partisi'nin web sitesini tahrif etmiş ve ülkenin DNS hizmetine müdahale etmek suretiyle ülkede kaos ortamına zemin hazırlamıştır[14].

Estonya siber savaşı, NATO'nun siber güvenlik çalışmalarında müttefik devletlerle müşterek hareket etme girişimlerinin başlaması açısından önemlidir. 2008 yılının Nisan ayında Bükreş'te gerçekleştirilen NATO Zirvesinde NATO Siber Savunma Birleşik Politikası kabul edilmiş ve ittifak çapında siber savunma operasyonel yeteneklerini merkezileştirmek için Brüksel merkezli Siber Savunma Yönetim Başkanlığı (CDMA) kurulmuştur. Aynı yılın Mayıs ayında yoğun siber saldırılara maruz kalan Talinn/Estonya'da NATO Siber Savunma Mükemmeliyet Merkezi (CCDCOE) kurulmuştur[15].

3. Gürcistan Siber Savaşı (2008)

Gürcistan ve Rusya arasında 7 Ağustos 2008'te gerçekleşen ve Gürcistan kuvvetlerinin ayrılıkçı grubun provokasyonuna cevap vermesiyle hızla yükselen olaylar sıcak çatışmaya dönüştü. 8 Ağustos'ta Rus güçleri Gürcistan'a askeri operasyonla karşılık verdiler. Bu arada 7 Ağustos 2008 akşam saatlerinde Gürcistan'a karşı siber saldırılar başladı. Gürcistan enformasyon alt yapısının Estonya kadar gelişmiş olmaması saldırının verdiği zararın etkisini azalttı. Ama saldırı sırasında olayların gelişimi ve izlenen yöntemler neredeyse Estonya'dakinin aynısıydı[16].

Gürcistan'a yönelik olarak düzenlenen siber saldırılardan çıkartılabilecek en önemli sonuç bunun gerçek bir hibrit savaş niteliği taşımasıdır. Geleneksel savaş yöntemlerini kullanan Rusya, eş zamanlı olarak siber saldırıları da başlatmıştır. Rusya'nın uyguladığı bu savaş düzenini hibrit savaş olarak tanımlamak mümkündür. Olayın bu şekilde gerçekleşmesi, NATO'nun hibrit savaşa olan inancını kuvvetlendirmiştir[17].

Gürcistan siber saldırıları sonrasında, 2008 yılının Kasım ayında NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) tarafından "Gürcistan'a Karşı Gerçekleştirilen Siber Saldırılar: Belirlenen Yasal Dersler " isimli bir bildiri yayınlanmıştır. Bu bildiride, Rusya-Gürcistan Savaşı sırasında meydana gelen siber saldırılara karşı Silahlı Çatışma Hukuku'nun (Law of Armed Conflict-LOAC) uygulanabilirliği üzerinde görüşler yer almaktadır[18].

D. NATO Siber Güvenlik Stratejisi

1999 yılında Kosova Savaşı sırasında NATO ve NATO üyesi ülkelere yapılan siber saldırılar sonrasında NATO "siber savunma" konusunu gündem maddelerine almaya başladı. NATO merkezli yapılan ilk siber saldırıların ardından 2002 yılında icra edilen Prag Zirvesi ile NATO Siber Savunma Programı kabul edildi. Bu program kapsamında, aynı yıl siber olayları tespit etmek ve siber saldırıları önlemek maksadıyla NATO Bilgisayar Olaylarına Müdahale Birimi (NCIRC) kuruldu[19].
Estonya Siber Savaşı sonrasında 3 Nisan 2008 tarihinde Romanya'nın başkenti Bükreş'te gerçekleştirilen NATO zirvesinde NATO'nun siber savunma faaliyetleri ve kritik altyapıların

korunması konusunda gündem maddeleri görüşülmüştür. NATO'nun siber güvenlik uygulamalarına yön veren Bükreş Zirvesi Bildirisi'nin 47'nci maddesi şöyledir:

> *"NATO, siber saldırılara dayanıklılığını artırmak için ittifak bilgi sistemlerini güçlendirme kararlılığını sürdürecektir. Son zamanlarda NATO siber savunma politikası kabul edildi ve ilgili birimler tarafından geliştirilmeye devam edecektir. Siber savunma politikamız NATO ve müttefik devletlerin siber savunma ihtiyaçlarını karşılamak ve kritik bilgi sistemlerini korumak üzerine yoğunlaşmaktadır. Bu amaç doğrultusunda; faydalı uygulamalar paylaşılmalı ve siber saldırıya maruz kalan devletin talep etmesi durumunda siber savunma desteği sağlanmalıdır. Biz NATO olarak, siber savunma yeteneklerimizin güçlendirilmesi için müttefik devletler ve ulusal otoriteler ile ilişkilerin geliştirilmesi konusunda istekliyiz".*[20]

Bükreş Zirve'si sonrasında siber güvenlik alanında iki önemli gelişme yaşandı. İlk olarak, Brüksel'de bir NATO Siber Savunma Yönetimi Otoritesi'nin (Cyber Defense Management Authority-CDMA) kurulmasına karar verildi. İkinci olarak, siber savunma kapasitesini bir merkezde toplayarak harekât kabiliyetini arttırmak maksadıyla Tallinn/Estonya merkezli müşterek bir organizasyon kurulmasına karar verildi. Bu kapsamda, 14 Mayıs 2008 yılında Estonya, Almanya, İtalya, Letonya, Litvanya, Slovakya ve İspanya'nın katılımıyla Talinn/Estonya merkezli NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) kuruldu[21].

Estonya ve Gürcistan siber saldırıları sonrasında NATO ülkeleri tarafından NATO Siber Savunma Politikası onaylandı ve 2010 yılında gerçekleştirilen Lizbon Zirvesi ile siber savunma konusu NATO'nun savunma planlama sürecine dâhil edildi[22].

2010 NATO Strateji Konsepti; siber saldırıları tespit, önleme ve siber saldırılara karşı savunma yeteneğinin geliştirilmesine olan ihtiyacın altını çizdi. NATO siber savunma politikasının temelini oluşturan ve revize edilen NATO Siber Savunma Konsepti 2011 yılının Mart ayında NATO Savunma Bakanlarına sunulmak için hazırlandı. Söz konusu konsept süreç içerisinde genişletilmiş NATO Savunma Bakanları tarafından onaylanmıştır. Onaylanan doküman, NATO'nun kendi yapılanması ve Müttefik kuvvetlerin yapılanması için özel görevleri tanımlayan bir eylem planı da içermektedir[23].

Bu süreç içerisinde NATO'nun siber güvenlik politikasını formüle ederken dört temel zorluk ile karşılaşılmıştır[24]:

1. Standart tanımlarından farklı olarak; saldırı, savaş ve kuvvet kullanımı ifadelerinin siber uzayda kullanılmasının formüle edilmesi.
2. Krizleri zamanında çözmek için oluşturulan stratejik çerçeve ile yönetimlerin desteklenmesi. Bu konu, siber savaş konusunda ulusal ve uluslararası düzeyde sorumlulukların belirlenmesi ve ortaya çıkan yeni çatışma ortamına göre yasaların tekrar düzenlenmesini içermektedir.
3. Siber uzay konusunda gerçekleştirilecek düzenlemelerin kolaylaştırılması için davranış normlarının formüle edilmesi. Bu konu, ulusal stratejilerin arasında artan uyumu içeren çok taraflı bir yaklaşım gerektirir.
4. Kolektif güvenlik ve bireysel özgürlüklerin korunması arasındaki dengenin sağlanması.

NATO tarafından yürütülen her türlü müşterek siber savunma harekâtı Kuzey Atlantik Konseyi'nin (NAC) kararlarına tabidir. Bu kapsamda NATO siber savunma harekatı konusunda tepe nokta Kuzey Atlantik Konseyi'dir. NATO Siber Savunma Konseptine göre NATO siber savunma yönetim hiyerarşisi aşağıdaki gibi tanımlanmıştır[25].

Şekil 5 *– NATO Siber Savunma Yönetim Yapılanması*

NATO Siber Savunma Konseptine göre NATO Siber Savunma Politikasının odak noktası; NATO ağlarının korunmasının sağlanması ile birlikte toplu savunma ve kriz yönetimi kapsamında ulusal ağların temel görevlerini yürütebilmesi için siber savunma ihtiyaçlarının karşılanmasıdır[25].

NATO'nun Talinn'de bulunan Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE) tarafından 2012 yılında yayınlanan "National Cyber Security Framework Manual" dokümanı NATO bünyesinde bulunan müttefik devletlerin uygulaması gereken siber savunma yöntemlerini 10 adımda tanımlamaktadır[26]:

1. Siber saldırılardan etkilenen devletin kritik altyapılarını korumaya yardımcı olmak için sivil ve ya askeri yapıyı kullanmak
2. Siber saldırılardan etkilenen devletin kriz yönetim görevlerini yerine getirmesine yardımcı olmak için sivil ve ya askeri yapıyı kullanmak
3. İncelemelerde yardımcı olmak için adli müfettişlerin görevlendirilmesi
4. Uzman ekipler görevlendirerek siber saldırılara maruz kalan devlet ile NATO ve özel sektör arasında eşgüdümlü çalışmaya yardımcı olmak
5. İnternet Servis Sağlayıcılara (ISP) verilen talimatlar aracılığıyla saldırıya uğrayan devletin saldırı trafiğini engellemek
6. İnternet Servis Sağlayıcılara (ISP) verilen talimatlar aracılığıyla saldırıya uğrayan devletin saldırıları destekleyen ve arkasında olduğundan şüphelenilen devletlerin erişimini engellemek
7. Saldırıların arkasında olduğu tespit edilen komuta-kontrol altyapısını bozmaya yönelik aktif savunma tedbirlerini uygulamak
8. Savunmaya yönelik harekât tarzlarını artırmaya yardımcı olmak için ilave İnternet Değişim Noktaları (IXP) oluşturmak ve yerel internet altyapısını güçlendirmeye yönelik tedbirler üretmek
9. Bilgisayar ve ağ cihazları üreticileri ile yapılacak koordineler sonrasında bölgeye yapacakları sevkiyatlara öncelik verilmesinin temin edilmesi
10. Müttefik ülkeler, saldırıya uğraya devleti rahatlamak ve saldırı yapan unsurları durdurmak maksadıyla bünyesinde bulundurdukları siber saldırı kuvvetlerini saldırganlar üzerine karşı saldırı yapmak suretiyle kullanabilir. Müttefik devlet bu karşı saldırıyı kendi namına değil bizzat İttifak (NATO) adına gerçekleştirir.

NATO siber savunma politikasının gelişmesi ve gerçekleştirilen siber saldırılara karşı uygulanması ile birlikte uluslararası yasalar ve silahlı çatışma yasalarına ilişkin sorunlar NATO toplantılarının

gündeminde yer almaya başlamıştır. NATO CCDCOE koordinatörlüğünde ve Uluslararası Bağımsız Uzmanlar Grubu'nun katılımıyla siber harekâtın karmaşık hukuk problemleri ile ilgili konularınaaçıklık getirmek maksadıyla, "Siber Savaşta Uygulanacak Hukuk Hakkında Tallinn El Kitabı" adıyla hazırlanan doküman, 2013 yılının Mart ayında Cambridge Üniversitesi tarafından yayımlanmıştır. Bu doküman aşağıdaki iki temel soruya cevap aramaktadır:

1. Savaşa girmenin haklı nedenleri nelerdir?
2. Savaş sırasında uyulması gereken kurallar nelerdir?

Tallinn El Kitabı; "Uluslararası Siber Güvenlik Hukuku" ve "Siber Silahlı Çatışma Hukuku" başlıklı iki ana bölümden ve 95 adet kuraldan oluşmaktadır. Birinci bölümde, "Devletler ve Siber Uzay" (Egemenlik, Yargılama Yetkisi, Kontrol ve Devlet sorumluluğu) alt konuları ele alınırken, ikinci bölümde ise, "Genel Siber Silahlı Çatışma Hukuku", "Düşmanca Davranışlar", "Belirli Kişiler, Nesneler ve Faaliyetler", "İşgal" ve "Tarafsızlık" alt konularına açıklık getirilmiştir[27].

IV. ULUSAL SİBER GÜVENLİK STRATEJİLERİNİN HAZIRLANMASI

Siber tehditlerin yaygınlaştığı günümüzde, kritik altyapılar üzerinde akan bilgilerin bütünlüğü ve gizliliği büyük önem arz etmektedir. Toplumun bilgi teknolojilerine gittikçe daha fazla bağımlı hale gelmesi, bu kritik altyapıların korunmasını ve kullanılabilirliğini ulusal çıkar haline getirmektedir. Böylece siber güvenlik, toplumun her seviyesini etkileyen yatay ve stratejik bir ulusal mesele olarak kabul edilmektedir.

Ulusal Siber Güvenlik Stratejisi gelişen teknoloji, değişen koşullar ve gereksinimler göz önünde bulundurularak, kamu ve özel sektörden gelecek talepler doğrultusunda, ulusal düzeyde sağlanmalı ve eşgüdüm ile güncellenmelidir.Ulusal siber güvenliğin sağlanmasına yönelik olarak yürütülecek çalışmalarda esas alınması gereken temel ilkeler şunlardır[28]:

1. Uluslararası sözleşmelerle teminat altına alınmış temel insan hak ve hürriyetlerinin korunması,
2. Demokratik toplum düzeninin gereklerine uyulması,
3. Alınacak tedbirlerin Ölçülülük İlkesine göre belirlenmesi,
4. Karar alma süreçlerine tüm paydaşların katılımını sağlayacak kapsayıcı bir yaklaşımın benimsenmesi,
5. Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile ele alan bütüncül bir yaklaşımın benimsenmesi,
6. Geliştirilecek çözümlerde güvenlik ile kullanılabilirlik arasında denge kurulması,
7. Diğer ülke mevzuatlarının göz önünde bulundurulması ve mümkün olabildiğince uyumluluğun sağlanması,
8. Uluslararası işbirliğinin sağlanması.

İlk olarak ABD tarafından 2003 yılında yayımlanan ulusal siber güvenlik planının ardından tüm dünya ülkeleri ulusal güvenliğini artırmak ve bu bağlamda siber güvenlik vizyonunu belirlemek maksadıyla ulusal siber güvenlik strateji dokümanları hazırlamaya başlamışlardır. Ulusal siber güvenlik stratejileri, ulus devletlerin stratejik ilkelerini, yönergelerini, hedeflerini belirleyen ve siber güvenlikle ilgili riskleri azaltmak için özel tedbirler içeren ana belgeleridir.

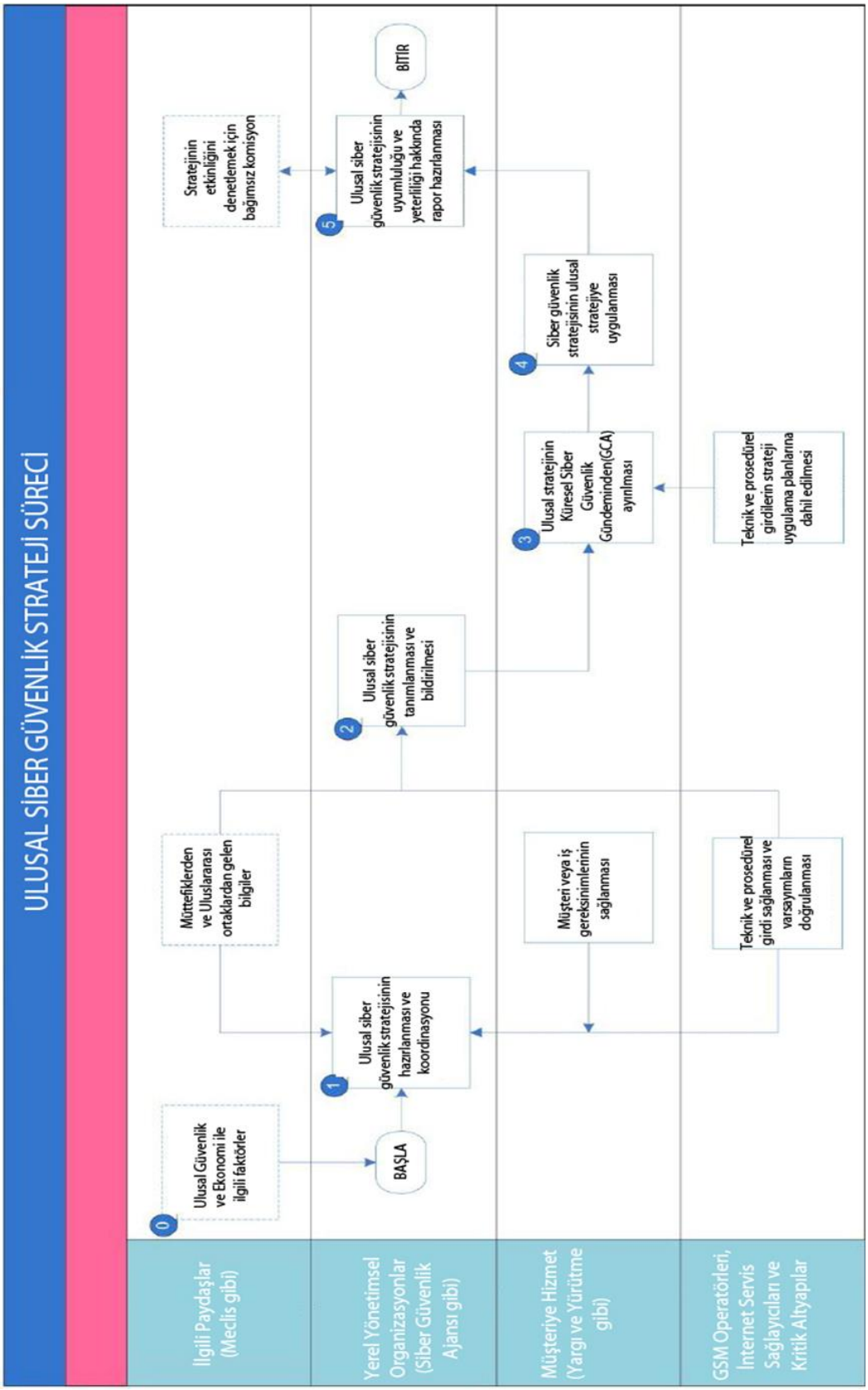
Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletleri siber güvenlik konusunda aynı çatı altında toplanmasına

neden olmuştur. Ulusal Siber Güvenlik Stratejisinin belirlenmesi ve uygulanması her devletin kendi sorumluluğundadır. Ancak, bazı uluslararası organizasyonlar Ulusal Siber Güvenlik Stratejisinin hazırlanması ve uygulanması konusunda devletlere rehberlik yapmak ve bu konuda standart oluşturmak maksadıyla modeller önermektedir.
Şekil 6'daki akış şeması, 1865 yılında kurulan ve 1947 yılında Birleşmiş Milletler bünyesine katılan Uluslararası Telekomünikasyon Birliği (ITU)tarafından önerilen ulusal siber güvenlik strateji sürecini tasvir etmektedir. Ulusların yönetim yapıları, yetenekleri ve ihtiyaçları değiştikçe strateji süreçleri de değişebilmektedir. Bu açıdan, şekilde gösterilen akış şeması sadece örnek niteliğindedir ancak NATO, siber güvenlik stratejisi hazırlama sürecince ITU modelini referans olarak göstermektedir. Ayrıca, bir ulusun ulusal siber güvenlik çerçevesini nasıl kuracağı, uygulayacağı, işleteceği ve izleyeceği Şekil 6'da tarif edilmektedir.

Şekil 6'daki akış şemasında tanımlanan süreçlerin tamamı Ulusal Siber Güvenlik Otoritesi tarafından yürütülmeli ve koordine edilmelidir. Ulusal Siber Güvenlik Otoritesi, ulusal siber güvenlik politikasının yönetiminin ve bölgesel ve uluslararası işbirliğinin tek elden koordine edilmesini sağlamalıdır. Ulusal Siber Güvenlik Otoritesi müdahalelerden uzak, bağımsız bir konumda bulunmalıdır. ITU tarafından kurulması önerilen Ulusal Siber Güvenlik Otoritesinin görevleri şunlardır[30]:

1. Ulusal siber güvenlik politikasının tanımlanması,
2. Ulusal siber güvenlik girişimleri için önceliklerin belirlenmesi,
3. Siber güvenlik faaliyetlerinin ulusal seviyede koordine edilmesi,
4. Siber güvenlik sorunlarını ele almak üzere paydaşların ve kamu-özel sektör ilişkilerinin belirlenmesi,
5. Bölgesel ve uluslararası taraf, kurum ve kuruluşlarla işbirliği yapılması,
6. Siber güvenlik ile ilgili uluslararası standartların uygulanması,
7. Bilgi ve iletişim altyapılarının, hizmetlerinin veya işletmecilerinin sertifikasyonu,
8. Sayısal kimlik sistemlerinin işletilmesi, geliştirilmesi ve yönetilmesi.

ITU modeline göre, Ulusal Siber Güvenlik Otoritesi tarafından stratejik seviyede yürütülen faaliyetler operatif seviyede Bilgisayar Olaylarına Müdahale Ekipleri (CERT, CSIRT, BOME) tarafından icra edilmelidir. Bilgisayar Olaylarına Müdahale Ekipleri, bilgisayar ve şebeke güvenliğini izleyen ve siber saldırı mağdurlarına olaylara müdahale hizmeti sunan teknik birimlerdir. ITU Dünya Telekomünikasyon Standartları Teşkilatı Meclisi (WTSA) 2008 yılında yayınlanan karar ile ulusal çerçevede BOME teşkilatlarının kurulmasını önermektedir.



Şekil 6 *- Ulusal Siber Güvenlik Strateji Süreci[29]*

V. YÖNTEM

Bu çalışmada teorik düzeyde literatür taraması yapılmış olup, belirlenen sorunun cevabı aranmıştır. Bu kapsamda, araştırma yöntemi olarak doküman incelemesi yöntemi benimsenmiştir. Bu kapsamda özellikle; NATO CCDCOE, ENISA, BSA, ITU organizasyonlarının yayımladıkları dokümanlar detaylı bir şekilde incelenmiştir.
Makalede belirlenen alt amaçların tespit edilmesi aşamasında aşağıda belirtilen yöntemler kullanılmıştır.

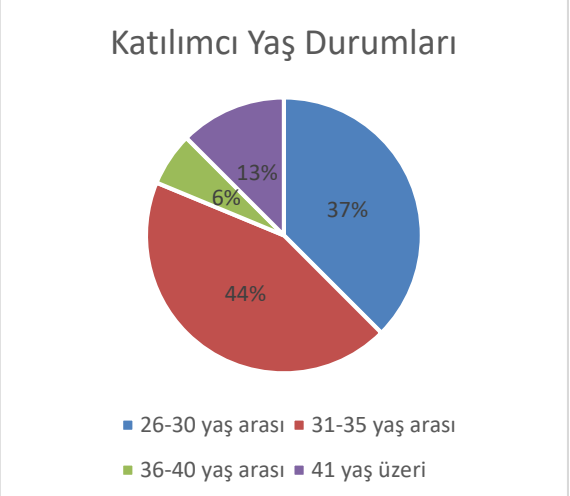
1. Siber güvenlik konusunda uzman olan 16 kişiden oluşan heyete sunum yapılmış ve görüşleri alınmıştır.
2. ENISA Raporlarında ülke temsilcilerinin tespitleri göz önünde bulundurulmuştur.
3. CCDCOE Raporlarında ülke temsilcilerinin tespitleri göz önünde bulundurulmuştur.

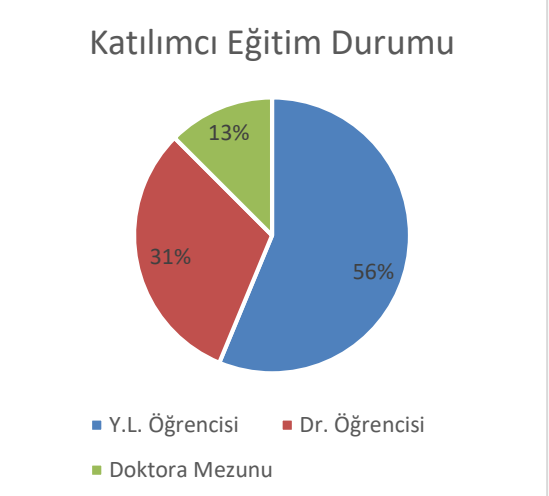
Görüşmeler ve ilgili içeriklerin incelenmesi sonucu belirlenen 4 alt başlık altında NATO çatısı altında bulunan ülkelerin siber güvenlik stratejileri sonraki bölümde karşılaştırma yapılarak değerlendirilmiştir. Araştırmanın evrenini, NATO üyesi olan 28 ülke oluşturmaktadır.

VI. ARAŞTIRMA BULGULARI

Bu çalışma ile; mevcut bulunan akademik çalışmalardan farklı olarak NATO çatısı altında bulunan ulusların uyguladıkları siber güvenlik stratejileri mukayeseli olarak incelenecektir. Bu çalışmanın, 28 farklı devletin siber güvenlik altyapılarını, siber güvenlik stratejilerini, siber güvenlik faaliyetlerini ortaya koymak suretiyle, ulusal çapta icra edilecek siber güvenlik çalışmalarına yeni bir bakış açısı sunması ve bu konuda farkındalık yaratması açısından önemli bir katkı sağlayacağı düşünülmektedir.

Çalışma başlıklarının belirlenmesi esnasında, önceki bölümde ifade edildiği üzere siber güvenlik konusunda tecrübe sahibi 16 kişi ile mülakat yapılmıştır. Katılımcıların yaşlarının dağılımı Şekil 7'de, eğitim durumlarının dağılımı ise Şekil 8'de gösterilmiştir.





***Şekil 7** - Katılımcıların Yaş Durumları*

***Şekil 8** - Katılımcıların Eğitim Durumları*

Araştırma, aşağıdaki tabloda gösterilen 2 farklı aşamada gerçekleştirilmiştir.

***Tablo 2** – Alt Amaçlar*

Aşama 1	1. Ulusal Siber Güvenlik Stratejisi ve Koordinatör Makamı Açısından İncelenmesi
Aşama 2	2. Bilgisayar Olaylarına Müdahale Ekipleri (CERT) Açısından İncelenmesi 3. Uluslararası İşbirliği Açısından İncelenmesi 4. Avrupa Birliği Konseyi Siber Suç Sözleşmesi Açısından İncelenmesi

Birinci aşamada; belirlenen bir tane alt amaç doğrultusunda 28 NATO üyesi ülkenin tamamı incelenecektir.
İkinci aşamada; günümüz itibariyle onaylı Ulusal Siber Güvenlik Stratejisi bulunmayan 8 NATO üyesi ülke ve onaylanmış Ulusal Siber Güvenlik Stratejisi bulunan ancak bu kapsamda icra ettikleri faaliyetleri, planları kısıtlı olan Lüksemburg araştırma dışında bırakılacaktır. Bu safhada; belirlenen üç adet alt amaç doğrultusunda onaylanmış Ulusal Siber Güvenlik Stratejisi bulunan 19 adet ülke incelenecektir.
Müteakip maddelerdeki tablolar, NATO üyesi ülkelerin yayınladıkları ulusal siber güvenlik strateji belgelerinden ve NATO Müşterek Siber Savunma Mükemmeliyet Merkezi'nin (CCDCOE) yayınladığı dokümanlardan faydalanılarak oluşturulmuştur.

A. Ulusal Siber Güvenlik Stratejisi ve Koordinatör Makamı Açısından İncelenmesi

Çeşitli ülkelerin siber güvenlik yapılanmaları incelendiğinde, siber güvenliği sağlamak amacıyla bazılarının yeni kurumlar oluşturduğu, bazılarının ise mevcut kurumların görev alanını genişlettiği görülmektedir. Oluşturulan veya görev alanı genişletilen kurumlar daimî komiteler, çalışma grupları, danışma kurulları, disiplinler arası merkezler gibi çok çeşitli yapılara sahiptirler.

Siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla ülkelerde "Siber Güvenlik Konseyleri" oluşturulmaktadır. Ülkemizde 1 Başkan ve 11 üyeden oluşan "Siber Güvenlik Kurulu" ulusal çapta bu görevi yürütmektedir.
Ulusal çapta oluşturulan Siber Güvenlik Konseyi, Ulusal Siber Güvenlik Koordinatörü başkanlığında toplanmaktadır. Ulusal Siber Güvenlik Koordinatörü; ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonu konularında Hükümetin Başkanı/Başbakanına karşı sorumludur. Ülkemizde bu görev; "Ulaştırma, Denizcilik ve Haberleşme Bakanlığı" tarafından yürütülmektedir. Tablo 3'te NATO üyesi 28 ülke Ulusal Siber Güvenlik Strateji Planı ve Koordinatör Makamı açısından incelenmesi gösterilmektedir.

***Tablo 3** – Ulusal Siber Güvenlik Stratejisi ve Koordinatör Makamı Açısından İncelenmesi*

ÜLKELER	ULUSAL SİBER GÜVENLİK STRATEJİSİ MEVCUT MU?	KOORDİNATÖR MAKAM	TARİH ARALIĞI
AL	✗	✗	✗
BE	✓	İçişleri Bakanlığı	2012-…

	BG	✗	✗	✗
	CA	✓	Kamu Güvenliği Bakanlığı	2010-…
	CZ	✓	İçişleri Bakanlığı	2011-…
	DE	✓	İçişleri Bakanlığı	2011-…
	DK	✗	✗	✗
	EE	✓	Savunma Bakanlığı Ekonomik İşler ve Haberleşme Bakanlığı	2009-2011 2011-…
	ES	✓	İçişleri Bakanlığı	2011-…
	FR	✓	Dışişleri ve Uluslararası Kalkınma Bakanlığı	2011- …
	GR	✓	Altyapı, Ulaştırma ve Ağlar Bakanlığı	2015-…
	HR	✗	✗	✗
	HU	✓	İçişleri Bakanlığı	2013-…
	IS	✗	✗	✗
	IT	✓	Başbakanlık Askeri Müşavirliğinde Kurulan Siber Güvenlik Birimi	2013-…
	LT	✓	Savunma Bakanlığı	2011-…
	LU	✓	Ekonomi ve Dış Ticaret Bakanlığı	2013
	LV	✓	Savunma Bakanlığı	2014-…
	NL	✓	Güvenlik ve Adalet Bakanlığı	2011-…
	NO	✗	✗	✗
	PL	✓	İdare ve Dijitalleştirme Bakanlığı	2013-…
	PT	✗	✗	✗
	RO	✓	İletişim ve Bilgi Toplumu Bakanlığı	2013-…
	SK	✓	Maliye Bakanlığı	2009-…

	SL	✗	✗	✗
	TR	✓	Ulaştırma, Denizcilik ve Haberleşme Bakanlığı	2013-…
	UK	✓	Başbakanlığa bağlı Milli Güvenlik Sekreterliği	2011
	US	✓	İç Güvenlik Bakanlığı	2003-…

Tablo3'te NATO üyesi olan 28 ülke; ulusal siber güvenlik stratejisinin mevcudiyeti ve bakanlık seviyesindeki koordinatör makamı açısından incelenmiştir. Tablodaki veriler ışığında aşağıdaki bulgulara rastlanmıştır:

Onaylanmış Ulusal Siber Güvenlik Stratejisi bulunan ülke sayısı :20
Onaylanmış Ulusal Siber Güvenlik Stratejisi bulunmayan ülke sayısı :7
Ulusal Siber Güvenlik Strateji Planı taslak halinde olan ülke sayısı :1 (Portekiz)
Ulusal Siber Güvenlik Strateji Planı ilk olarak Amerika Birleşik Devletleri tarafından 2003 yılında hazırlanmıştır.

Şekil 9 *- Ulusal Siber Güvenlik Strateji Planı*

Şekil 9'da gösterildiği gibi, 28 ülke arasında yapılan incelemede ülkelerin %71'inin onaylanmış Ulusal Siber Güvenlik Strateji Planının olduğu tespit edilmiştir.

Onaylanmış Siber Güvenlik Stratejisi bulunan ancak planları ve faaliyetleri kısıtlı olan Lüksemburg sonraki safhalarda araştırmamızın dışında yer alacaktır.

Araştırmanın sonraki safhasına onaylanmış Ulusal Siber Güvenlik Strateji Belgesi bulunan 19 ülke ile devam edilecektir.

B. Bilgisayar Olaylarına Müdahale Ekipleri (CERT) Açısından İncelenmesi

Uluslararası camiada siber saldırılara karşı ortak tepkilerin gerçekleştirilebilmesi maksadıyla bölgesel BOME'ler arasında koordinasyonu sağlayan organizasyonlar mevcuttur. FISRT (Forum of Incident Response and Security Teams), bilgisayar güvenlik olaylarını kooperatif olarak ele alan, olay önleme programlarını teşvik eden ve güvenilir bilgisayar olayları müdahale ekipleri arasında koordinasyonu sağlayan uluslararası bir konfederasyonudur. FIRST temel olarak [31];

1. Teknik bilgi, araçlar, yöntemler ve süreçler geliştirir ve paylaşır,
2. Kaliteli güvenlik ürünlerinin, politikalarının ve hizmetlerinin geliştirilmesini teşvik eder,
3. Bilgisayar güvenlik uygulamaları geliştirir ve ilan eder,
4. BOME ekiplerinin oluşturulmasını ve yaygınlaştırılmasını teşvik eder,
5. Müşterek bilgi, beceri ve deneyimleri kullanarak güvenli ortamlar oluşturulmasına yardımcı olur.

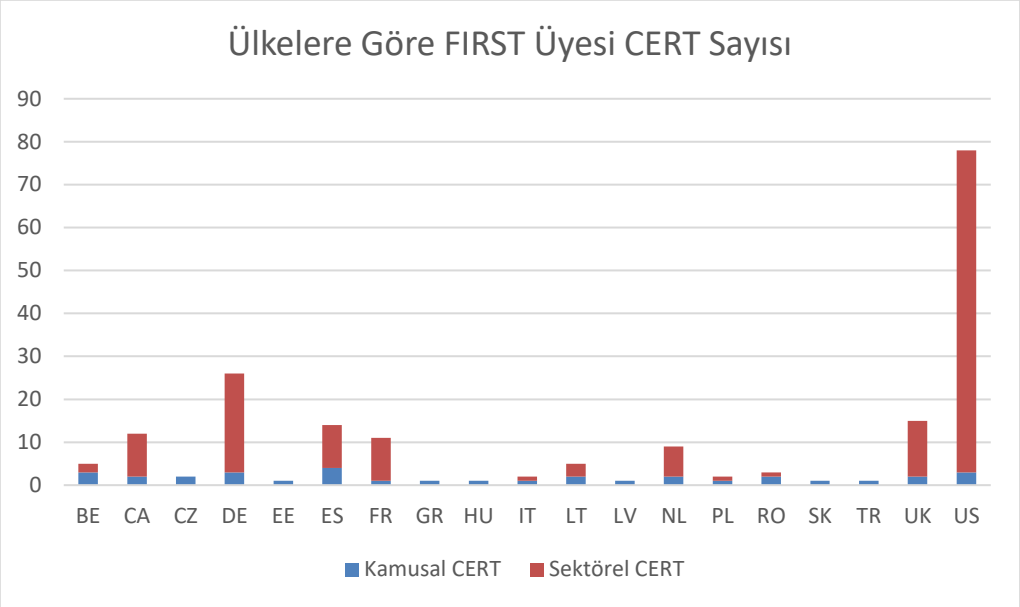
Tablo 4'te Onaylanmış Ulusal Siber Güvenlik Strateji Belgesi bulunan 19 NATO ülkesinin Bilgisayar Olaylarına Müdahale Ekipleri FIRST üyelikleri açısından incelenmesi gösterilmektedir.

Tablo 4 *- Bilgisayar Olaylarına Müdahale Ekipleri (CERT) Açısından İncelenmesi*

ÜLKELER	FIRST Üyesi Kurumsal CERT Durumu				FIRST Üyesi Sektörel CERT Sayısı	FIRST Üyesi Toplam CERT Sayısı
	Sayı	İsim	Açıklama	Kuruluş Tarihi		
BE	3	BELNET CERT CERT-EU NCIRC-CC	Ulusal BOME (Belçika Araştırma ve Eğitim Ağı) AB BOME NATO BOME	2004 2011 2004	2	5
CA	2	CCIRC CANCERT	Kanada Siber Olay Tepki Merkezi Kanada Ulusal BOME	2003 1998	10	12
CZ	2	CSIRT.CZ GovCERT.CZ	Çek Cumhuriyeti Ulusal BOME Çek Cumhuriyeti Hükümeti BOME	2008 2012	0	2
DE	3	CERT-Bund KIT-CERT RUS-CERT	Bilgi Güvenliği Federal Dairesi BOME Karlsruhe Teknoloji Enstitüsü BOME Stuttgart Üniversitesi BOME	2012 2008 1998	23	26
EE	1	CERT-EE	Ulusal BOME (Estonya Bilişim Merkezi)	2006	0	1
ES	4	CCN-CERT CERTSI CESISAT-CERT esCERT-UPC	Hükümet Ulusal Kripto Merkezi BOME Ulusal Güvenlik ve Sanayi BOME Katalonya Bilgi Güvenliği Merkezi CERT Katalonya Politeknik Üniversitesi BOME	2006 2007 2010 1994	10	14
FR	1	CERT-FR	Ulusal BOME	2004	10	11
GR	1	FORTHcert	Araştırma ve Teknoloji Vakfı BOME	2007	0	1
HU	1	CERT-Hungary	Ulusal BOME	2013	0	1
IT	1	PI-CERT	İtalyan Posta İdaresi BOME	2013	1	2
LT	2	CERT-LT LTU MOD CIRT	Ulusal BOME (İletişim Düzenleme Kurumu) Savunma Bakanlığı BOME	2006 2009	3	5
LV	1	CERT.LV	Ulusal BOME (Mat. Ve Bilg. Bil. Enst.)	2006	0	1
NL	2	DefCERT NCSC-NL	Savunma Bakanlığı BOME Ulusal Siber Güvenlik Merkezi BOME	2010 2002	7	9
PL	1	CERT POLSKA	Ulusal BOME (Akademik Bilgi Ağı)	1996	1	2
RO	2	CERT-RO RoCSIRT	Ulusal BOME Ulusal Eğitim Ajansı BOME	2011 2008	1	3

	SK	1	CSIRT.SK	Ulusal BOME (Maliye Bakanlığı)	2009	0	1
	TR	1	TR-CERT	Ulusal BOME (Bilgi Teknolojileri Kurumu)	2013	0	1
	UK	2	CERT.UK WAR-CSIIRT	Ulusal Siber Güvenlik Merkezi BOME Warwick Üniversitesi BOME	2007 2009	13	15
	US	3	CERT/CC JC3-CIRC US_CERT	BOME Koordinasyon Merkezi Enerji Dep. Siber Güv. Koor.Merkezi Ulusal BOME	1984 2008 2003	75	78

Yukarıdaki tabloda yer alan veriler ışığında NATO Üyesi 19 ülkenin FIRST üyesi BOME sayıları Şekil 10'da gösterilmektedir (Ülkelerin farklı sayılarda BOME ekipleri mevcut olabilir ancak küresel bir organizasyon olarak FIRST üyelik sayılarını ifade etmektedir).



Şekil 10 *- Ülkelere Göre FIRST Üyesi CERT Sayısı*

Yaygın uygulama olarak ülkelerin, Siber Güvenlik Otorite Makamları (Ülkemiz için USOM-TR CERT) Ulusal BOME olarak FIRST üyesidir. FIRST üyesi ulusal BOME'ler uluslararası BOME'ler ile koordinasyon halinde hareket ederek yerel BOME'leri yönlendirir. Ancak A.B.D., Almanya, Birleşik Krallık ve Fransa gibi teknoloji açısında gelişmiş ülkelerde sektörel BOME'ler etkin rol oynamaktadır. Özellikle Apple, Microsoft, Oracle, Siemens, AT&T gibi küresel çapta faaliyet gösteren kuruluşlar kendi bulundukları ülkelerde de gelişmiş birer sektörel BOME olarak görev yapmaktadır.

C. Uluslararası İşbirliği Açısından İncelenmesi

Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletlerin uluslararası anlaşmalar yapmasını kaçınılmaz hale getirmiştir. NATO CCDCOE, ENISA ve ITU gibi uluslararası organizasyonlar aracılığıyla ülkeler siber saldırılara karşı dijital sınırlarını korumakta ve müşterek siber güvenlik stratejileri geliştirmektedir. Bu uluslararası organizasyonlar hakkında bilgi Tablo 5'te gösterilmektedir.

Tablo 5 *– Uluslararası Organizasyonlar*

Uluslararası Organizasyonlar	**Kuruluş Tarihi**	**Merkezi**
NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCDCOE)	14 Mays 2008	Talinn/Estonya
Avrupa Birliği Ağ Ve Bilgi Güvenliği Ajansı (ENISA)	1 Eylül 2005	Crete/Yunanistan
Birleşmiş MilletlerUluslararası Telekomünikasyon Birliği (ITU)	17 Mayıs 1865	Geneva/İsviçre

Tablo 6'da Onaylanmış Ulusal Siber Güvenlik Strateji Belgesi bulunan 19 NATO ülkesinin yukarıda belirtilen uluslararası organizasyonlara üyelikleri açısından incelenmesi gösterilmektedir.

Tablo 6 *– Uluslararası İşbirliği Açısından İncelenmesi*

ÜLKELER	**CCDCOE**		**ENISA**		**ITU**	
	Katılım Durumu	**Katılım Tarihi**	**Katılım Durumu**	**Katılım Tarihi**	**Katılım Durumu**	**Katılım Tarihi**
BE	✗	✗	✓	01.09.2005	✓	01.01.1866
CA	✗	✗	✗	✗	✓	01.07.1908
CZ	✓	03.06.2014	✓	01.09.2005	✓	01.01.1993
DE	✓	14.05.2008	✓	01.09.2005	✓	01.01.1866
EE	✓	14.05.2008	✓	01.09.2005	✓	22.04.1992
ES	✓	14.05.2008	✓	01.09.2005	✓	01.01.1866
FR	✓	03.06.2014	✓	01.09.2005	✓	01.01.1866
GR	✓	03.11.2015	✓	01.09.2005	✓	01.01.1866
HU	✓	23.06.2010	✓	01.09.2005	✓	01.01.1866
IT	✓	14.05.2008	✓	01.09.2005	✓	01.01.1866
LT	✓	14.05.2008	✓	01.09.2005	✓	12.10.1991
LV	✓	14.05.2008	✓	01.09.2005	✓	11.11.1991
NL	✗	✗	✓	01.09.2005	✓	01.01.1866

	PL	✓	16.11.2011	✓	01.09.2005	✓	01.01.1921
	RO	✗	✗	✓	01.01.2007	✓	09.02.1866
	SK	✓	14.05.2008	✓	01.09.2005	✓	23.02.1993
	TR	✓	03.11.2015	✗	✗	✓	01.01.1866
	UK	✓	03.06.2014	✓	01.09.2005	✓	24.02.1871
	US	✓	16.11.2011	✗	✗	✓	01.07.1908

NATO üyesi 19 ülke arasında yapılan ve Tablo 6'da gösterilen veriler ışığında aşağıdaki bulgulara rastlanmıştır:

1. Ülkelerin %79'u CCDCOE üyesidir.
2. Ülkelerin %84'ü ENISA üyesidir.
3. Ülkelerin tamamı ITU üyesidir.
4. Ülkelerin %68'i üç organizasyona da üyedir.

D. Avrupa Birliği Konseyi Siber Suç Sözleşmesi Açısından İncelenmesi

İnternet ve bulut ortamlarında tutulan verilerin birçoğu organize suç örgütleri tarafından hedef halinde bulunmaktadır. Ülkeler, sürekli gelişen siber tehditlere karşı hukuki düzenlemeler yapar ve uygularlar.

Avrupa Birliği Konseyi tarafından 23 Kasım 2001 tarihinde imzaya açılıp 1 Temmuz 2004 tarihinde yürürlüğe giren Siber Suç Sözleşmesi, bilgisayar ve internet suçlarını kapsayan ilk uluslararası sözleşmedir. Sözleşmenin amacı, ulusal kanunların arasında ortak nokta sağlayarak, araştırma tekniklerini geliştirerek ve ülkeler arası işbirliğini arttırarak siber suçlara karşı ortak mücadeleyi sağlamaktır.

Tablo 7'de Onaylanmış Ulusal Siber Güvenlik Strateji Belgesi bulunan 19 NATO ülkesinin Avrupa Birliği Konseyi Siber Suç Sözleşmesine göre incelenmesi gösterilmektedir.

***Tablo 7** - Avrupa Birliği Konseyi Siber Suç Sözleşmesi Açısından İncelenmesi*

ÜLKELER	İMZALAMA TARİHİ	ONAY TARİHİ	YÜRÜRLÜĞE GİRME TARİHİ
BE	23.11.2001	20.08.2012	01.12.2012
CA	23.11.2001	08.07.2015	01.11.2015
CZ	09.02.2005	22.08.2013	01.12.2013
DE	23.11.2001	09.03.2009	01.07.2009

	EE	23.11.2001	12.05.2003	01.07.2004
	ES	23.11.2001	03.06.2010	01.10.2010
	FR	23.11.2001	10.01.2006	01.05.2006
	GR	23.11.2001	✖	✖
	HU	23.11.2001	04.12.2003	01.07.2004
	IT	23.11.2001	05.06.2008	01.10.2008
	LT	23.06.2003	18.03.2004	01.07.2004
	LV	05.05.2004	14.02.2007	01.06.2007
	NL	23.11.2001	16.11.2006	01.03.2007
	PL	23.11.2001	20.02.2015	01.06.2015
	RO	23.11.2001	12.05.2004	01.09.2004
	SK	04.02.2005	08.01.2008	01.05.2008
	TR	10.11.2010	29.09.2014	01.01.2015
	UK	23.11.2001	25.05.2011	01.09.2011
	US	23.11.2001	29.09.2006	01.01.2007

VII. SONUÇ

Ulusal bilgi güvenliğinin sağlanması; birey, kurum ve kuruluşlarınkatılımıyla stratejik seviyede planlama yapılması planın sağlıklı uygulanması ile gerçekleştirilebilecektir. Siber saldırılara karşı ulusal çıkarların korunması ve siber uzayın sınır güvenliğinin sağlanması hususunda karşılaşılan zorluklar, devletlerin uluslararası anlaşmalar yapmasını kaçınılmaz hale getirmiştir. Bu çalışma kapsamında, küreselleşen dünyada ülkeleri aynı çatı altında birleştiren en büyük organizasyonlardan biri olan NATO'nun ve NATO üyesi ülkelerin uyguladıkları siber güvenlik stratejileri mukayeseli olarak incelenmiştir.

Bu çalışma ile söz konusu ülkeler;

1. Ulusal siber güvenlik stratejisi ve koordinatör makamı
2. Bilgisayar Olaylarına Müdahale Ekipleri (CERT)

3. Uluslararası işbirliği
4. Avrupa Birliği Konseyi Siber Suç Sözleşmesi açısından incelenmiştir.

Bu çalışma kapsamında yapılan incelemeler sonucunda aşağıda belirtilen sonuçlara ulaşılmıştır:

1. Ulusal siber güvenlik stratejisi hazırlanırken uluslararası koordinasyon sağlanmalı ve ülkeler aynı görüş etrafında toplanmalıdır. Siber ortam sorunları, uluslararası şeffaflık sağlanarak ve belirlenecek kurallar çerçevesinde kontrol altına alınmalıdır.
2. Uluslararası bir organizasyon çatısı altında ulusal siber güvenliğin değerlendirilmesi gerekmektedir.
3. Ülkemizde siber suçlar konusunda hukuki düzenlemelerin yeterli olmadığı değerlendirilerek farklı ülkelerin bu konudaki başarılı uygulamaları doğrultusunda eksiklikler giderilmelidir.
4. Ülkemizde siber güvenlik tehditlerinin önceden tespit edilebilmesi ve en kısa sürede tepkinin verilebilmesi için sektörel çerçevede Bilgisayar Olaylarına Müdahale Ekipleri (CERT) yaygınlaştırılmalıdır.

VIII. KAYNAKLAR

[1] B. Schneier, *Secrets and Lies, Digital Security In A Networked World*, Indiana, Wiley Publishing, 2000.

[2] "The National Strategy to Secure Cyberspace", The White House, Washington, 2007.

[3] M.C. Libicki, *Cyberdeterrence and Cyberwar*, USA, RAND Corporation, 2009, Sf.12-13.

[4] R. Hill, "Dealing With Cyber Security Threats: International Coorporation, ITU and WCIT", *7th International Conference on Cyber Conflict*, sf.119-134, 2015.

[5] FACT SHEET: Cybersecurity Legislative Proposal, (29 Nisan 2016). Erişim: https://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative proposal.

[6] General James Cartwright, "Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5", Depatment of Defense, Washington DC, 2011

[7] R. Clarke, R.Knake, *Cyber War*. HarperCollins e-books. Sf 11.

[8] P.Cornish, D.Livingstone, D.Clemente, C.Yorke, "On Cyber Warfare" A Clatham House Report, Sf.1, 2010.

[9] C. Stallard, C. (2011). "At The Crossroads of Cyber Warfare: Signposts For The Royal Australian Air Force" Yüksek Lisans Tezi, School of Advanced Air and Space Studies, Maxwell Air Force Base, Alabama, USA, 2011, Sf 47.

[10] Anonim, (20 Haziran 2016). [Online]. Erişim: http://www.nato.int/cps/en/natohq/natocountries.htm

[11] Anonim, (25 Haziran 2016). [Online]. Erişim: http://www.nato.int/cps/en/natohq/structure.htm

[12] J.Arquilla, D.Ronfeldt, *Networks and Netwars The Future of Terror, Crime, and Militancy*. USA, RAND Corporation, 2001, Sf.240-248.

[13] R.Kaiser, "The birth of cyberwar", *Political Geography* 46, Sf.11-20, 2015

[14] P.Shakarian, J.Shakarian, A.Ruef, *Introduction To Cyber-Warfare: A Multidisciplinary Approach*, USA, Elsevier, 2013, Sf.16-20.

[15] S.Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security*, Number 2, Volume 4, Sf.54-55, 2011.

[16] S.Bıçakcı, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler Akademik Dergi*, Cilt 10, Sayı 40, Sf.101-130, 2014.

[17] S.Bıçakcı, "Yeni Savaş Ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", *Uluslararası İlişkiler Akademik Dergi*, Cilt 9, Sayı 34, Sf.205-226, 2012.

[18] J.Carr, (2010). *Inside Cyber Warfare*, O'Reilly Media, Second Edition, USA, 2012, Sf.31.

[19] T.Check, "Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict: A NATO-Centric Approach", *Cleveland State University Law Journals*, Sf.495-512, 2015.

[20] NATO CCDCOE, (2016, 10 Temmuz), 2008 NATO Bucharest Summit Declaration, Erişim: https://ccdcoe.org/sites/default/files/documents/NATO-080403BucharestSummitDeclaration.pdf

[21] Anonim, (10 Temmuz 2016) [Online]. Erişim: https://ccdcoe.org/history.html

[22] NATO CCDCOE, (2016, 8 Temmuz), Lisbon Summit Declaration, Erişim: http://www.nato.int/cps/en/natolive/official_ texts_68828.htm

[23] Anonim, (8 Temmuz 2016) [Online]. Erişim: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

[24] Rapporteur R.Noshiravani, "NATO and Cyber Security: Building on the Strategic Concept", Chatham House Report, 2011.

[25] NATO Document, "Defending the Networks: The NATO Policy on Cyber Defence", Brüksel, 2011.

[26] A.Klimburg, *National Cyber Security Framework Manual*, NATO CCDCOE Publication, Talinn, Sf.180-188, 2012.

[27] International Group of Experts at the Invitation of The NATO Cooparative Cyber Defence Centre of Excellence, *Talinn Manual On The International Law Applicable to Cyber Warfare*, Cambridge University Press. 2013.

[28] M.Ünver, C.Canbay, A.G.Mirzaoğlu, "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler", *Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı*, Sf.22-52, 2009.

[29] F.Wamala, *ITU National Cybersecurity Strategy Guide*, Sf.25-65, 2011.

[30] H.I.Toure, "ITU Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG) Global Strategic Report", Sf.92-101, 2008.

[31] Anonim, (10 Şubat 2017) [Online]. Erişim: https://www.first.org/about/mission