T.C.

YALOVA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

DEVLETLERİN SİBER GÜVENLİK POLİTİKALARININ ŞEKİLLENDİRİLMESİ SÜRECİNDE KAMU-ÖZEL SEKTÖR İŞBİRLİĞİNİN ARTAN ÖNEMİ: İSRAİL VE YENİ ZELANDA ÖRNEKLERİ

YÜKSEK LİSANS TEZİ

Engin SAVÇIN

Enstitü Anabilim Dalı: Uluslararası İlişkiler

Enstitü Bilim Dalı: Uluslararası İlişkiler

Tez Danışmanı: Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK

TEMMUZ 2020

T.C.

YALOVA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

DEVLETLERİN SİBER GÜVENLİK POLİTİKALARININ ŞEKİLLENDİRİLMESİ SÜRECİNDE KAMU-ÖZEL SEKTÖR İŞBİRLİĞİNİN ARTAN ÖNEMİ: İSRAİL VE YENİ ZELANDA ÖRNEKLERİ

YÜKSEK LİSANS TEZİ

Engin SAVÇIN

Enstitü Anabilim Dalı: Uluslararası İlişkiler

Enstitü Bilim Dalı: Uluslararası İlişkiler

Bu tez 09/07/2020 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

	Adı SOYADI	**Kanaati**			**İmza**
Jüri Başkanı (***Danışman)***	Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK	☐ Kabul	☐ Düzeltme	☐ Ret	
Jüri Üyesi	Prof. Dr. Saadet Gülden AYMAN	☐ Kabul	☐ Düzeltme	☐ Ret	
Jüri Üyesi	Doç. Dr. Murat ALAKEL	☐ Kabul	☐ Düzeltme	☐ Ret	

SOSYAL BİLİMLER ENSTİTÜSÜ YÜKSEK LİSANS İNTİHAL YAZILIM RAPORU BEYAN BELGESİ

Tez Başlığı:

Devletlerin Siber Güvenlik Politikalarının Şekillendirilmesi Sürecinde, Kamu - Özel Sektör İşbirliğinin Artan Önemi: İsrail ve Yeni Zelanda Örnekleri

Yukarıda başlığı belirtilen tez çalışmamın toplam 92 sayfalık kısmına ilişkin aşağıda belirtilen filtrelemeler uygulanarak alınmış olan ve 21/ 06 / 2020 tarihinde aşağıda ismi yazılı öğretim görevlisi tarafından şahsıma iletilen Turnitin intihal tespit programı raporuna göre tezimin benzerlik oranı %1'dir

Uygulanan filtrelemeler:

1. Kaynakça hariç,
2. Alıntılar dâhil,
3. 5 kelimeden daha az örtüşme içeren metin kısımları hariç.

Bu bilgiler doğrultusunda tez çalışmamın herhangi bir intihal içermediğini; aksinin tespiti halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Adı Soyadı : Engin SAVÇIN

Öğrenci Numarası : 177207015

Ana Bilim Dalı : Uluslararası İlişkiler

Programı : Uluslararası İlişkiler

Türü : ( ) Proje (X) Yüksek Lisans Tezi ( ) Doktora Tezi

Danışman (Adı Soyadı, İmzası, Tarih)

Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK

ÖNSÖZ

Siber alanın gelişmesine olanak sağladığı asimetrik ve öngörülemeyen tehdit unsurları, güvenlik ortamını dönüştürmüş ve güvenlik stratejilerinin kapsayıcı yöntemler aracılığıyla ve ortak çıkarlar doğrultusunda yapılandırılmasının gerekliliğini ortaya koymuştur. Günümüzde kritik altyapı sistemlerinin tehdit unsurlarına karşı dayanıklı bir biçimde tesis edilmesi ve siber sistemler tarafından aktif ve pasif savunma yöntemleri ile korunmaları, ulusal güvenlik açısından elzemdir. Çok boyutlu ve çok aktörlü politikaların gerekliliği ve kapsamlı süreçler gerektirmeleri, siber güvenlik altyapılarını şekillendirirken devletleri özel sektör ile işbirliği kurmaya yöneltmiştir. Bu çalışmanın, Türkiye kapsamında bu alandaki çalışmaların gelişmesi açısından siber güvenlik stratejilerinin şekillendirilmesi sürecinde perspektif sağlaması ve farklı çerçevelerin çeşitli çözüm alternatifleri sunabileceğini göstermesi açısından faydalı olacağı düşünülmektedir.

Bu tez çalışmasının kaynak toplama, planlama ve yazım süreci boyunca desteğini ve katkısını hiçbir zaman esirgemeyen, her aşamada sabır ve anlayış ile yol gösteren danışman hocam Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK'a ve yüksek lisans eğitimim boyunca üzerimde emeği olan tüm hocalarıma teşekkürlerimi arz ederim.

Bu çalışma boyunca manevi destekleriyle her zaman yanımda olduklarını hissettiren aileme, tez yazım sürecim boyunca desteklerini esirgemeyen, aynı aşamalardan birlikte geçtiğimiz saygıdeğer dostlarım ve sınıf arkadaşlarım Abdullah YILDIZ ve Muaz TOK'a, değerli meslektaşım ve yakın dostum Meltem Damla ÇELİK YAVUZ'a ve beni her daim gülümseten tüm öğrencilerime teşekkürlerimi sunmayı bir borç bilirim.

Ayrıca araştırma ve yazım sürecimin başında fikirleri ve tecrübesiyle bana yol gösteren, Prof. Dr. Hakan Gürcan SICAKKAN'a, sonsuz teşekkürlerimi sunarım.

Engin SAVÇIN

İÇİNDEKİLER

KISALTMALAR LİSTESİ

AB: Avrupa Birliği
AR-GE: Araştırma-Geliştirme
CCIP: Kritik Altyapıları Koruma Merkezi
CERT: Siber Olaylara Müdahale Ekipleri
CICS: Siber Güvenlik İçin Sayısal Zeka
DDoS: Dağıtılmış Servis Hizmet Reddi Saldırısı
DoS: Servis Hizmet Reddi Saldırısı
FBI: Federal Soruşturma Bürosu
FVEY: Beş Gözlü İstihbarat Ağı
GCSB: Devlet Haberleşme Güvenliği Bürosu
GSYİH: Gayri Safi Yurtiçi Hâsıla
HAMAS: İslami Direniş Hareketi
IDF: İsrail Savunma Kuvvetleri
INCD: İsrail Ulusal Siber Direktörlüğü
INCB: İsrail Ulusal Siber Büro
IPCP: Bireysel Ortaklık ve İşbirliği Programı
NATO: Kuzey Atlantik Anlaşması Örgütü
NCSA: Ulusal Siber Güvenlik Ajansı
NCI: Ulusal Siber Girişim
NCSC: Ulusal Siber Güvenlik Merkezi
NISA: Ulusal İstihbarat ve Güvenlik Ajansı
NZCSC: Yeni Zelanda Siber Güvenlik Mücadeleleri
NZDF: Yeni Zelanda Savunma Kuvvetleri
OECD: İktisadi İşbirliği ve Gelişme Teşkilatı
SIS: Güvenlik ve İstihbarat Servisi
STK: Sivil Toplum Kuruluşu

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

ÖZET

Tezin Başlığı: Devletlerin Siber Güvenlik Politikalarının Şekillendirilmesi Sürecinde Kamu-Özel Sektör İşbirliğinin Artan Önemi: İsrail ve Yeni Zelanda Örnekleri	
Tezin Yazarı: Engin SAVÇIN	**Danışman:** Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK
Kabul Tarihi: 09.07.2020	**Sayfa Sayısı:** ix (ön kısım) + 103
Anabilim Dalı: Uluslararası İlişkiler	**Bilim Dalı:** Uluslararası İlişkiler

Güvenlik kavramı tarihsel süreç boyunca içinde bulunulan dönemin dinamikleri, aktörleri ve araçları kapsamında şekillendirilmiş ve askeri güvenlik geleneksel çerçeveyi oluşturan ana unsur olarak akademik yazında yer bulmuştur. Ancak, Soğuk Savaş sonrası dönemde güvenlik ajandasının genişleyerek bireysel, toplumsal, siyasi ve çevresel güvenlik politikalarını içerecek şekilde çeşitlendiği ve derinleştiği gözlemlenmektedir. Dönüşen güvenlik ajandasında siber güvenliğin önemli bir konu haline gelmesi, devletlerin uygulamakta oldukları güvenlik politikalarını ve bu politikaların uygulanma süreçlerinin siber alan üzerinden değerlendirilmesini elzem kılmıştır.

Siber uzayın beşinci operasyonel alan haline geldiği günümüzde, siber güvenlik stratejileri gittikçe önem kazanmaktadır. Uygulanmakta olan siber güvenlik politikalarının etkili ve verimli sonuçlar vermesi açısından devletlerin çok boyutlu bir şekilde politikalarını geliştirmeleri gerekmektedir. Bu çerçevede, devletlerin siber güvenlik politikalarını şekillendirmeleri sürecinde özel sektör ile işbirliği kurma ihtiyaçları ortaya çıkmaktadır. Bu tez çalışmasında, devletlerin siber güvenlik politikalarını şekillendirirken özel sektör ile işbirliğini elzem kılan faktörler incelenmiş ve çok paydaşlı, kapsamlı bir yaklaşımın siber güvenlik alanındaki önemine vurgu yapılmıştır. Kamu-özel sektör işbirlikleri çerçevesinde geliştirilen etkin siber güvenlik politikaları çerçevesinde İsrail ve Yeni Zelanda devletleri örnek olarak analiz edilmiştir. İsrail ve Yeni Zelanda devletlerinin siber güvenlik politikalarını şekillendirirken tüm paydaşların ortak çıkarları doğrultusunda, kapsayıcı politikalar oluşturabildikleri ve böylelikle siber güvenlik kapasitelerini arttırabildikleri görülmüştür.

Devletlerin siber alanda güvende olabilmelerini sağlamak amacıyla kritik altyapı sistemlerini güvence altına almaları gerekmektedir. Altyapı sistemlerinin tesis edilme süreçlerinin özel sektöre devredilmesi durumunda ortaya çıkan tehdit unsurları bağlamında devlet kurumlarını, kritik altyapıları, özel sektörü ve toplumu kapsayan siber güvenlik stratejilerine ihtiyaç duyulmaktadır. Sistem hassasiyetlerinin ve kırılganlıklarının yüksek olması nedeniyle kapsamlı yatırımlara ihtiyaç duyulması, devletleri özel sektör ile işbirlikleri kurmaya yöneltmektedir. Buna ek olarak siber güvenlik alanında istihdam edilecek personelin yetiştirilmesi amacıyla üniversiteler ile işbirlikleri yürütülmesi, askeri, siyasi ve ekonomik politikaların siber alan üzerinden etkisinin arttırılması ve siber alanın toplum tarafından aktif bir biçimde kullanılmakta olması nedeniyle siber alanda farkındalık sahibi olan bir toplum yaratma gereksinimi ortaya çıkmaktadır. Güvenlik aktörlerinin çeşitlendiği, güvenlik konularının çok boyutlu bir hal aldığı günümüzde, insan eliyle oluşturulmuş beşinci operasyonel alan halini alan siber alanda güvenliğin sağlanması çok paydaşlı politika uygulamalarına bağımlı hale gelmiştir. Bu kapsamda siber güvenlik politikalarının oluşturulmasında kamu-özel sektör işbirliği büyük bir önem arz etmektedir.

Bu çalışmada siber güvenlik politikalarının çok boyutlu ve çok paydaşlı politikalar aracılığıyla şekillendirilmesi süreci Kopenhag Ekolü ve Yönetişim kavramı çerçevesinde İsrail ve Yeni Zelanda örnekleri üzerinden değerlendirilerek, Türkiye'nin siber güvenlik politikalarının şekillendirilmesi sürecine perspektif sunulması amaçlanmıştır.

Anahtar Kelimeler: Güvenlik, güvenlik anlayışı, siber güvenlik, siber alan, kamu-özel sektör işbirliği

SUMMARY

Thesis Title: Rising Importance of Public-Private Partnership on Forming Cybersecurity Policies of States: Cases of Israel and New Zealand	
Thesis Author: Engin SAVÇIN	**Advisor:** Assistant Professor Övgü KALKAN KÜÇÜKSOLAK
Date of Acceptance: 09.07.2020	**Total Number of Pages:** ix (pre text) + 103
Department: International Relations	**Field of Study:** International Relations

The concept of security has been shaped by the actors of its era during the historical process and military security found a place in academic studies as the main conventional constituent that sets the perspective. However after the period followed by the Cold War, security issues became diversified and deepened when political, economic, societal and individual matters were added into the security issues. In the context of threat constituents which emerge through the interaction of the states via cyberspace, implementation of conventional security policies have to be utilized with the cybersecurity strategies.

Nowadays, cyberspace has become the fifth operational domain of the states and the cybersecurity strategies gain importance gradually. For cybersecurity policies to be efficient and forceful, they need to be integrated into the conventional security policies. In this context, states required to build partnerships with the private sector in order to shape their cybersecurity policies. For this study, the crucial reasons for these partnerships which require multi-stakeholder approach were analysed and emphasized the importance of an inclusive approach in the context regarding cybersecurity. The outcome is the states' efforts are insufficient to establish a durable cybersecurity on their own due to the multi-dimensional structure and diversification of actors as well as the threat constituents in cyberspace. The states of Israel and New Zealand were chosen as cases for this study due to their inclusive policy implementations to achieve common goals for all partners while forming the cybersecurity strategies and their achievements on increasing their capacity of cybersecurity with their policies.

For states to be secure in cyberspace, the critical infrastructure systems must be protected. When establishment processes of the critical infrastructures are delegated to private sector, due to the threat factors that emerge, cybersecurity strategies are required to involve; state agencies, critical infrastructures, private sector and society. Due to high sensitivities and vulnerabilities, requirement of inclusive investments steer states into forming public-private partnerships. In order to train personnel who will work on the field of cybersecurity, projects are needed to be conducted with universities so as to create high-skilled experts. The outcomes of military, political and economic strategies can be multiplied when they are implemented via cyberspace. Furthermore, creating an aware society in cyberspace because of the widespread use of technology by the citizens.

Nowadays that security actors diversify, security issues become multi-dimensional, cyberspace became the fifth operational domain which had been made by man is dependent on the implementations of multi-stakeholder policies to provide security. In this context, public-private partnerships have utmost importance on building cybersecurity. In this study, forming the cybersecurity policies via multi-dimensional and multi-stakeholder policies were evaluated through states of Israel and New Zealand cases by the frame of Copenhagen School and concept of Governance. Thus, offering a perspective on cybersecurity policies of Turkey has been aimed.

Keywords: Security, security understanding, cybersecurity, cyberspace, public-private partnership

GİRİŞ

Canlıların en temel gereksinimi olan güvenlik, içinde bulunulan döneme ve araçlara göre değişim geçirmekte ve aktörlerin bu çerçevede stratejiler geliştirmesi gerekliliğini beraberinde getirmektedir. İçinde bulunduğumuz süreçte siber güvenlik bireyden devlet düzeyine varan bir şekilde öncelikli güvenlik meselesi haline gelmektedir. Soğuk Savaş dönemi boyunca askeri güvenlik öncelikli gündem maddesi olmuş, Soğuk Savaş sonrası dönemde ise güvenlik konularının çeşitlenmesi siyasi, ekonomik, toplumsal, bireysel ve çevresel boyutların ön plana çıkmasına sebebiyet vermiştir. Soğuk Savaşın sonu itibariyle ortaya çıkmaya başlayan siber alanın tüm dünyayı birbirine bağlaması ve mesafelerin önemini ortadan kaldırmaya başlamasıyla aktör yelpazesinin hiç olmadığı kadar genişlediği görülmüştür.

Soğuk Savaş döneminin devlet ve askeri araçlar odaklı katı Realist yaklaşımının Soğuk Savaş sonrası dönemin genişleyen güvenlik ajandasını ve çeşitlenen güvenlik aktörlerini açıklamakta yetersiz kaldığı anlaşılmıştır. Bu dönemde bilişim teknolojilerinin kaydettiği gelişim çerçevesinde siber alan adı verilen insan yapımı, beşinci operasyonel alan ortaya çıkmış ve diğer alanları da kapsayacak şekilde önemli kullanım imkânları ortaya koymuştur. Siber alanın sahip olduğu manevra arttırma kapasitesi diğer operasyonel alanlara kıyasla oldukça yüksektir. Sunduğu imkânlar üzerinden asimetrik güç kazanan bireylerin devletlere zarar verebilecek kabiliyetlere ulaşmasına imkân tanıyan siber alan, birey güvenliğinden devlet bekasına uzanan son derece geniş bir çerçevede yeni bir güvenlik konusu haline gelmiştir.

Ortaya çıkan bu operasyonel alanın anlaşılması ve güvenlik politikalarının geliştirilmesinde klasik anlayışın yetersiz kalması, güvenliği daha geniş bir perspektifle inceleyen yaklaşımların üzerinden gidilmesini elzem kılmıştır. Bu çerçevede, çalışmada Kopenhag Ekolü'nün güvenliği daha geniş ve derin bir çerçeveden analiz eden yaklaşımından yararlanılmış ve aktör ve konu bazında çok boyutlu bir anlayış ortaya konulmaya çalışılmıştır. Zira siber alanın barındırdığı çok boyutlu ve belirsiz tehditler, devletlerin çok yönlü güvenlik politikalarını geliştirmesini ve bu anlamda kamu-özel sektör işbirliklerini geliştirmeleri gereğini gündeme getirmiştir.

Siber alanın gelmiş olduğu nokta itibariyle değerlendirildiğinde, devletlerin işlerlik kazandığı pek çok alanın buraya bağlandığı ve buradaki kırılganlıkların devletler için ciddi güvenlik açıkları haline geldiği görülmektedir. Devletlerin altyapı sistemlerinin siber saldırılar tarafından savunmasız bırakılması sonucunda devletin bütünlüğünü riske atabilecek unsurların ortaya çıkabildiği bir gerçektir. Bunun yanı sıra özel sektörün gerek bu alandaki yatırımları gerekse faaliyetlerinin devlet bekası anlamındaki önem itibariyle de siber alanın güvenliği konusunda önemli yer teşkil ettiğini söylemek mümkündür. Bu sebeplerden ötürü, ulusal düzeyde siber güvenlik politikalarının oluşturulması aşamasında devletlerin çok paydaşlı bir süreçte, özel sektör işbirliği ve vatandaşların bilinçlenmesine

yönelik girişimleriyle uzun dönemli, kapsamlı bir çerçeve inşa etmeleri gerektiği görülmektedir. Siber sistemlerin entegre edildiği tüm kritik altyapı sistemleri, sistemlere yüklenen yazılımlar, sistemlerin kullanıcıları, sistemlerin ve altyapıların sağladığı tüm hizmetlerden faydalanan ticari işletmeleri, özel sektörü ve devletin vatandaşlarını kapsayan güvenlik politikalarının geliştirilmesi önümüzdeki dönemin başlıca konusu haline gelmektedir.

Bu çalışmada devletlerin siber güvenlik politikalarının şekillendirilmesi sürecinde kamu – özel sektör işbirliğinin artan önemi, bu alanda öne çıkan devletler olan İsrail ve Yeni Zelanda örnekleri üzerinden açıklanmaktadır. Farklı coğrafyalardan seçilen bu iki örnekte de siber alan ulusal güvenlik meselesi haline getirilmiş ve bu anlamda kamu-özel sektör işbirliği çerçevesinde kapsamlı politikalar ortaya konmuştur. Önümüzdeki süreçte devlet bekası anlamında gittikçe daha fazla önem kazanması beklenen siber alana yönelik politikaların kapsamlı bir şekilde tartışılmasının Türkiye'nin bu alandaki politikalarına katkı sağlayacağı düşünülmektedir.

Çalışmanın Konusu

Bu tez çalışmasında, günümüz güvenlik ajandasının önde gelen konularından biri olan siber güvenliğin sağlanmasında, kamu-özel sektör işbirliğinin artan önemi İsrail ve Yeni Zelanda örnekleri üzerinden tartışılmaktadır. Güvenlik konularının çeşitlendiği ve hatta siber alanda tehditlerin yönünün ve kimliğinin belirsizleştiği bir ortamda devletlerin tek taraflı politika uygulamalarının yetersiz kaldığı gözlenmektedir. Bu kapsamda, bireyden devlete varan çok çeşitli düzeydeki aktörün yer aldığı ve tehdit arz etme kabiliyetine sahip olduğu siber alanda, güvenlik ihtiyacının karşılanması amacıyla çok paydaşlı bir yaklaşımın benimsenmesinin gerekliliği ve bu anlamda kamu – özel sektör işbirliklerinin öne çıkan unsurları üzerinde durulmuştur.

Günümüzde devlet ve özel sektör politikalarının ayrımı ve etkilediği kitle arasındaki makas oldukça daralmıştır. Aynı şekilde uygulanan politikaların yerel, bölgesel ve küresel etkileri için de aynı durum söz konusudur. Karşılıklı bağımlılıklar ve siber alanda artan kırılganlıklar uzun dönemli, entegre politikaların şekillendirilmesini ve uygulanmasını gerektirmektedir.

Bu çalışmada, güvenliğin gelmiş olduğu aşama geçirdiği dönüşüm ve siber alanın arz ettiği tehditler üzerinden ortaya konarak, bu çerçevedeki politikaların ve aktörlerin kapsamlı bir biçimde ele alınmasının öneminin altı çizilmektedir. Çalışmanın ilk bölümü güvenlik anlayışını klasik güvenlik anlayışından itibaren ele almakta ve Soğuk Savaş sonrası dönemin güvenlik ortamını Kopenhag Ekolü çerçevesinde inceleyerek güvenlik anlayışının dönüşümünü ortaya koymaktadır. Güvenlik ortamında yaşanan dönüşümün ulaşmış olduğu nokta itibariyle, Yönetişim anlayışının güvenlik sorunlarının çok paydaşlı bir çerçevede oluşturulması kapsamındaki önemi vurgulanmaktadır. İkinci bölümde siber güvenliğin içeriği, temel unsurları ve siber güvenlik politikalarının uygulanma biçimleri ve araçları, güvenlik anlayışını dönüştürmesi ve uluslararası ilişkiler dinamiklerine olan

yansımaları çerçevesinde tartışılmaktadır. Bu inceleme yapılırken kamu-özel sektör işbirliklerinin yapılandırılması kapsamında Yönetişim kavramının kapsayıcılığı ve entegre politikaların şekillendirilmesindeki önemi üzerinde durulmaktadır. Bu kapsamda, kritik altyapıları sistemlerinin oluşturulma yöntemleri ve araçları, insan kaynağının yetiştirilmesi ve devlet politikalarına entegre edilme yöntemleri incelenerek hem kamu hem de özel sektörden araçlar kullanan aktörler örneklendirilmektedir. Askeri, siyasi, ekonomik ve sosyal hayatı kapsayan entegre siber politikaların teşkil edilmesinde kullanılan yöntemler ve araçlar incelenmekte ve değerlendirilmektedir. Üçüncü bölümde ise, çalışmada örnek olarak ele alınan İsrail ve Yeni Zelanda devletlerinin bu aşamalarda izlemiş oldukları politikalar ve araçlar incelenmekte, kapsamlı ve uzun dönemli siber politikalarını hangi unsurlar üzerinden yapılandırdıkları irdelenmektedir. Ortadoğu'nun kalbinde yer alan İsrail ile bambaşka bir coğrafyada yer alan Yeni Zelanda'nın siber güvenlik anlayışında rol oynayan temel unsurlar, şekillendirdikleri araçlar ve siber güvenlik politikalarının dinamikleri detaylı bir şekilde analiz edilmektedir. Bu kapsamda, İsrail ve Yeni Zelanda'nın kamu – özel sektör işbirlikleri aracılığıyla siber güvenlik altyapısının inşası, geliştirilmesi ve dönüştürülmesi aşamalarında izledikleri yollar ileriye dönük perspektif sunması amacıyla tartışılmaktadır.

Çalışmanın Önemi

Bu çalışmanın konusunun şekillenmesinde, günümüz güvenlik ortamının en önemli konularından biri olan siber güvenlik konusunun önemli bir boyutunun derinlemesine incelenerek uzun dönemde geliştirilebilecek olan siber politikalara katkı sunulması düşünülmüştür. Siber güvenlik alanında son yıllarda kaydedilen gelişmeler konuya ilişkin olarak birey düzeyinden devlet düzeyine varan hemen her düzeyde farkındalık yaratılması gerekliliğini ortaya koymuştur. Özellikle de Türkiye'de ortaya konan çalışmaların büyük bir çoğunluğunun açıklayıcı ve tanımlayıcı özelliklere sahip olması, siber alanın belirli konularında derinlemesine yapılması gereken çalışmalar konusunda boşluk yaşanmasına sebebiyet vermiştir. Bu noktadan hareketle, uzun dönemli siber politikaların geliştirilmesi konusunda kamu-özel sektör işbirliklerinin arz ettiği önemin detaylı bir şekilde iki önemli örnek üzerinden tartışılarak farklı bir perspektif sunulması üzerinde durulmuştur.

Gerek artan karşılıklı bağımlılıklar, gerekse siber alanın diğer operasyonel alanlara nüfuz edecek şekilde ortaya koyduğu kırılganlıklar karşısında güvenliğin farklı boyutlarıyla, farklı işbirlikleri üzerinden ele alınması elzem hale gelmiştir. Türkiye'nin siber politikalarını yapılandırması sürecinde farklı perspektiflerin örneklerle ortaya konmasının devlet politikalarının gelişimine ve literatürün zenginleşmesine katkı sağlayacağı düşünülmektedir.

Çalışmanın Amacı

Bu çalışmada, siber güvenlik politikalarının şekillenmesinde kamu – özel sektör işbirliklerinin oynadıkları roller ile bu anlamda yapılandırılan politika uygulamaları ve araçlarının Yeni Zelanda ve İsrail örnekleri üzerinden tartışılması amaçlanmıştır. Bu amaç doğrultusunda aşağıdaki araştırma sorularına yanıt aranmıştır:

- Siber alanda yaşanan gelişmeler güvenlik kavramını ve konuya yönelik yaklaşımı hangi çerçevede dönüştürmüştür?

- Güvenlik ortamında yaşanan dönüşüm devletlerin güvenlik politikalarını nasıl etkilemektedir?

- Siber güvenlik politikalarının şekillenmesinde etkili olan başlıca unsurlar nelerdir?

- Siber güvenlik politikalarının uygulanması sürecinde aktörlerin rollerini hangi kapsamda değerlendirmek mümkündür?

- Siber güvenlik alanında kamu-özel sektör işbirliklerinin oluşumunda etkili olan faktörler nelerdir?

- Kamu-özel sektör işbirliği çerçevesinde şekillenen siber politika uygulamalarının temel unsurları nelerdir?

Çalışmanın Hipotezleri

Özellikle Soğuk Savaş sonrası dönemde güvenliğin yapısının, aktörler ve konular bazında dönüşüm geçirmesi ve bu anlamda siber alanın gittikçe önem kazanmaya başladığı noktasından hareketle, devletlerin tek başlarına bu çok boyutlu alanın güvenliğini sağlamada yeterli olmadıkları hipotezi temel olarak ortaya konmaktadır. Siber güvenlik alanında gelinen noktada, karşılıklı bağımlılıkların artışı ve siber alandaki kırılganlıkların farklı alanlarda ciddi sonuçlar doğurması, devletlerin tepeden inme politikalar yerine kapsayıcı ve çok paydaşlı güvenlik politikalarını benimsemesine sebebiyet vermiştir.

İsrail ve Yeni Zelanda örneklerinden de görüldüğü üzere, verimli ve başarılı siber güvenlik politikalarının devlet kurumlarını, özel sektörü ve vatandaşları kapsayan çok paydaşlı bir anlayışla şekillendiği ve bu çerçevede kamu-özel sektör işbirliklerinin önem kazandığı bir diğer temel hipotez olarak ortaya konulmaktadır.

Kamu-özel sektör işbirliklerinin altyapı tesislerinin kurulması esnasında üstlendiği roller, devlet ve özel sektör arasındaki güven bağını kuvvetlendirmektedir. Bu sayede devletin toplumu güvende tutma görevi gibi çeşitli sorumluluklarında da paydaşların öneminin arttığı ve bunun karşılıklı güveni olumlu yönde etkilediği görülmektedir.

Çalışmanın Yöntemi ve Teknikleri

Bu çalışmada siber güvenlik politikalarının artan önemi ve kamu-özel sektör işbirliklerinin bu süreçte hangi etkenler çerçevesinde önem kazandığı Kopenhag Ekolü ve Yönetişim perspektifinden incelenmektedir. Realist yaklaşımın devlet politikalarıyla sınırlı kalan güvenlik yaklaşımı karşısında Kopenhag Ekolünün güvenliğin değişen yapısının açıklanmasındaki işlevselliğinden yararlanılmaktadır. Kopenhag Ekolü'nün genişletilmiş güvenlik kavramı kapsamında siber alanda çeşitlenen güvenlik tehditleri ile aktörlerin önemi vurgulanmakta ve yönetişim kavramı çerçevesinde siber tehditlerin karşısında oluşturulması gereken çok paydaşlı yapının unsurlarının altı çizilmektedir. Araştırmanın konusunu teşkil eden kamu – özel sektör işbirliklerinin şekillenmesinde etkili olan faktörler siber güvenlik çerçevesinin bu çok boyutlu yapı kapsamında tartışılmakta ve bu anlamda kamu – özel sektör işbirliklerinin önemi vurgulanmaktadır.

Bu çalışmanın yazımı sırasında birincil ve ikincil kaynaklardan bilgi toplama tekniği uygulanmış, analitik yorumlar yapılarak iki devletin siber alanda şekillendirdikleri güvenlik politikaları kamu-özel sektör işbirliği modelleri kapsamında incelenmeye çalışılmıştır. Bu amaç doğrultusunda, üniversite kütüphanelerinde bulunan eserler ile birçok Yüksek Lisans ve Doktora Tezi taranmıştır. Konuya ilişkin kitaplar, internet siteleri, ulusal ve uluslararası hakemli dergilerdeki makaleler ile alanında uzman kişilerin çeşitli platformlardaki çalışmaları incelenmiştir. İsrail ve Yeni Zelanda örneklerinin incelenmesi aşamasında bu ülkelerin resmi internet sitelerinde yer alan yıllık raporlardan ve stratejik planlamalardan yararlanılmıştır. Çalışma yapılırken İngilizce ve Türkçe eserlerden faydalanılmıştır. İsrail örneğinin incelenmesi sırasında İbranice bilinmemesi bu dilde yazılan bazı kaynakların incelenmesini imkânsız kılmış ve bu konu da çalışmanın sınırlılıklarından birini teşkil etmiştir.

Literatür İncelemesi

Tarihsel süreç boyunca dönüşen güvenlik tehditleri, devletlerin güvenlik politikalarının dinamik bir yapıda olmasını gerektirmiştir. Tarihsel anlamda güvenlik politikaları devletlerin savaşa hazırlanmak, savaşa girmek ve savaşı engellemek üzerine geliştirdikleri askeri odaklı yol haritaları olmuştur (Çetinkaya, 2012-13: 242). John Baylis, devletlerin kendi kendine yetmenin esas olduğu dünyada, varlıklarını sürdürmek için çıkar odaklı politikalar uygulamaktan başka şanslarının olmadığını belirtmektedir. Hobbes ve Machiavelli gibi realist kuramın öncü düşünürleri devletlerin kendi varlıklarını komşuları pahasına koruyacaklarını ve devletlerarası ilişkilerin güç ve çıkar odaklı mücadelelere dayandığını belirtmektedirler (Baylis, 2008: 71-72). Bilhassa Soğuk Savaş dönemine kadar gerçekleşen güvenlik ortamını yorumlamak amacıyla Realist yaklaşımların kullanılması, devlet tabanlı politikalar üzerinden güvenlik anlayışının şekillendirilmesi süreçlerini analiz etmekte ve tek boyutlu anlayış çerçevesinde güvenlik ortamını açıklamakla yetinmektedirler (Hansen ve Nissenbaum, 2009: 1161).

Soğuk Savaş yıllarında nükleer stratejiler üzerinden şekillendirilen güvenlik yaklaşımı çerçevesinde caydırıcılık politikalarının devletler arası savaşı engellemede etkili olabileceği görülmüştür (Powell, 2003: 107). Soğuk Savaş yıllarının sonuna doğru küreselleşmenin ve ekonomik karşılıklı bağımlığın artan şekilde gündemdeki yerini alması güvenliğin siyasi, ekonomik, toplumsal ve bireysel boyutlarının önem kazanmaya başladığını göstermiştir (Buzan, 1983: 216-235). Gelişen bilgi ve iletişim teknolojileri, devletler arasındaki mesafelerin öneminin azalmasına sebep olmaya başlamış ve yeni tehdit unsurları ortaya çıkmaya başlamıştır. Soğuk Savaş sonrası dönemin dinamikleri doğrultusunda şekillenen güvenlik ortamı bağlamında devletler güvenlik anlayışlarını yeniden yapılandırmak durumunda kalmışlardır (Ağır, 2011: 104). Soğuk Savaş sonrası dönemde siber alanın güvenliğin konusu haline gelmesi devletlerin güvenlik politikalarını şekillendirme süreçlerinde etkili olmasına sebebiyet vermiştir. Ortaya çıkan her risk, gerekli önlem alınmadığı takdirde tehdide dönüşmektedir (Küçükşahin, 2006: 18).

İnsan eliyle yapılan beşinci operasyonel alan olan siber alanı güvenli hale getirmek için yapılan çalışmalar günden güne artmaktadır. Bu alandan kaynaklı tehditlerin diğer fiziki operasyonel alanlarda etkili olduğu ve bireyden devlet düzeyine varan geniş bir yelpazede tehdit arz ettiği görülmektedir (Kramer, Starr ve Wentz, 2009: 348). Estonya ekonomisinin Rusya tarafından uygulandığı iddia edilen siber saldırılarla sekteye uğratılması, İran'ın uranyum zenginleştirme tesislerinin Çernobil benzeri bir felakete yol açabilecek STUXNET virüsü tarafından saldırıya uğraması en bariz örneklerdendir (Clayton, 2010: 2). Bu süreçte devlet veri tabanlarına çok katmanlı güvenlik sistemlerinin yerleştirilmesi, bilginin depolandığı sunuculara erişimin sadece özel izinler ile mümkün olması ve izinli veya izinsiz her türlü erişimin sıkı bir takipte tutulması önem kazanmıştır (Carr, 2016: 48). Siber saldırılar devlet kurumlarının işleyişini, özel sektörün operasyonlarını ve toplumun günlük aktivitelerini sekteye uğratabilecek tehditler içermektedir.

Aktörlerin kolaylıkla kimliklerini gizleyebildikleri siber alanda, siber tehditlerin öngörülemez olması ve siber alanın belirsizlikler içinde amorf bir yapıya sahip olması, bu alandaki aktörleri risk ve tehditler karşısında sürekli olarak aktif olmaya itmektedir (Cavelty, 2013: 107). Ayrıca, bankacılık, elektrik, su, gaz, kanalizasyon gibi kritik altyapı sistemlerinin zaman içerisinde siber alana daha fazla entegre olması bu alanların siber tehditlerden korunmasını öncelikli hale getirmiştir (Warfield, 2012: 128). Bu sistemlerin zaman zaman devletler tarafından özelleştirilerek şirketlere devredilebilmesi veya işbirliği kapsamında ortak yönetilmesi, bu sistemlerin güvenliğini sağlama aşamasında şirketlerin ve devletlerin ortak sorumluluk ve ortak çıkarlar doğrultusunda politikalar geliştirebilmelerine vesile olmuştur (Singer ve Friedman, 2014: 196). Bu gelişme, siber güvenlik uzmanlarının yetişmesine ve iş alanlarının çeşitlenmesine vesile olmuştur (Cornish, 2015: 157). Bu gelişmeler ışığında altyapı ağlarını özel sektörün

profesyonelliğinde geliştirmek ve işletmek isteyen devletler özel şirketlerle işbirliğine girerek özel şirketleri de siber alanda birer aktör haline getirmişlerdir (Carr, 2016: 49).

Siber alan, yapısı gereği mesafeleri önemsizleştirmiş ve kimi sınırlılıkların geleneksel kapasitelerle mümkün olmayan yöntemler aracılığıyla aşılabilmesini sağlamıştır. Örneklendirmek gerekirse; Yeni Zelanda coğrafi izolasyonuna rağmen operasyonlarını siber alana kamu-özel sektör işbirliği aracılığıyla entegre ederek daha etkili ve daha geniş çapta sürdürebilmeyi başarmıştır (Burton, 2013: 219). Diğer taraftan İsrail sahip olduğu iklimin ektisine rağmen yüksek teknoloji alanına yaptığı yatırımlar aracılığıyla ihracat kapasitesini önce tarım, ilerleyen yıllarda yüksek teknoloji alanında arttırmayı başarmış ve siber alanda aktif bir özel sektör yaratarak, küresel aktörler ile stratejik ortaklıklar kurmayı başarmış ve siber alana entegre bir devlet haline gelmiştir (Tabansky ve Israel, 2015: 22).

1.BÖLÜM: GÜVENLİK ANLAYIŞINDA YAŞANAN DÖNÜŞÜM

Geçen yüzyıl, dünya tarihinde en çok yıkımın yaşandığı yüzyıllardan biri olarak görülmektedir. İki dünya savaşı ve Soğuk Savaşın yaşanmış olduğu bu yüzyılda güvenlik alanındaki çalışmalar genel olarak Realist perspektif tarafından yorumlanmış ve devletler arasındaki ilişkileri askeri odaklı bir anlayış doğrultusunda açıklama çabası içerisinde bulunmuştur (Sandıklı ve Emeklier, 2011: 3). Soğuk Savaşın sona erdiği yıllarda güvenlik konularının siyasi, ekonomik, toplumsal ve çevresel güvenlik kapsamlarında çeşitlenmesi Kopenhag Ekolü tarafından ortaya konmuş, çeşitlenen ve derinleşen güvenlik konularının ve ortamının çok boyutlu yaklaşımlar tarafından incelenmesinin gerekliliği belirtilerek Realist politikaların tek boyutluluğu ortaya konmuştur. 1990'lar itibariyle siber alanın bir operasyon alanı haline gelmesi ile birlikte güvenlik konularına bir yenisi eklenmiş ve dönüşen güvenlik ortamı, aktör sayılarının çeşitlenmesine vesile olmuştur. Siber güvenlik politikaları kritik altyapıların korunması, siber alanda çalışacak insan kaynağı yetiştirilmesi, devletin geleneksel güvenlik politikalarına entegre edilmesi gibi çok çeşitli politikalar uygulanmasını gerektirmektedir. Bu çerçevede, çok taraflı ve kapsayıcı yöntemler ile uygulanan siber güvenlik polititkalarının en verimli ve en etkili sonuçları ortaya çıkaracağı öngörülmektedir.

1.1 Geleneksel Güvenlik Anlayışı

Devlet bekasının temelini teşkil eden güvenliğin tesis edilmesinin amacı; varlığını tehdit eden oluşumları ortadan kaldırmak, çıkarları doğrultusunda politikalar geliştirmek ve uygulamaktır. Bu amaçlar doğrultusunda, insan ve devlet yapısı benzer özellikler göstermektedir. Var olduğu alanın sınırlarını belirlemek, bu sınırları korumak ve karşısına çıkan tehdit unsurları uyarınca tedbir almak, insan ve devlet doğasını ilk çağlardan beri şekillendirmeye devam etmektedir. İçinde bulunulan dönemin koşullarına göre tehdit unsurları da güncellenmekte ve güvenlik ihtiyaçları da bu doğrultuda çeşitlenmektedir. Diğer bir tabirle, güvenlik anlayışı önceki dönemin herkes tarafından kabul edilen güvende olma şartlarını yerine getirmek ve diğer aktörlerin yaşıyor olduğu tehlikelere karşı zamanında tedbir alabilecek politikalar geliştirebilmektir (Buzan, 1991). Şehir devletlerinin dönemin aktörlerine ve güncel konjonktüre göre yapılanması ve hayatta kalma mücadelesi, ulus devletlerin kontrol ettikleri alanları koruma, genişletme ve halkını vergilendirerek gelir akışını sağlama arzusu güvenlik parametrelerini belirlemekte ve güvenlik anlayışını şekillendirmektedir.

Dönem değiştikçe, güvenlik konularının da güncellendiği ve fiziksel gücün yanı sıra, ekonomik güvenlik, ideolojik üstünlük, birey, bilgi ve altyapı güvenliği gibi konuların güvenlik anlayışı içine dâhil edilerek çok yönlü, birbiri içine geçmiş bir güvenlik anlayışını inşa ettiği görülmektedir (Demir, 2009). Dahası, tehditlerin öngörülemeyen bir şekilde ortaya çıktığı siber alanda güvenlik anlayışı devletlerin ve diğer büyük çaplı aktörlerin yanı sıra birey güvenliğini de yeniden şekillendirerek dönüştürmektedir.

Tarihsel süreç içerisinde, güvenlik anlayışının aktör bazında devletten bireye varan bir düzlemde derinleştiği, askeri güvenlikten çevresel güvenliğe varan bir düzlemde de genişlediği gözlenmektedir. Gelişen teknolojinin artan ağırlığının etkisiyle aktörler çeşitlenmekte, karşılıklı bağımlılıklar ve hassasiyetler artmakta, güç unsurları sert güç, yumuşak güç ve akıllı güç kapsamında tartışılmaktadır. Özellikle de siber alanın sağlamış olduğu imkânlar üzerinden artan etkileşim aktörlere kazandırdığı kapasite ve yarattığı kırılganlıklar üzerinden güvenlik çevresini, aktörleri ve araçları dönüştürmektedir. Hem birey hem de devlet seviyesinde gerçekleşen yeni kazanımlar kaybetme endişesini ortaya çıkarmakta ve güvenlik anlayışının dönüşümünde önemli bir paya sahip olmaktadır.

Güvenliğin unsurları tarihsel süreçte farklılık arz etmişse de güvenlik konusunun temelini oluşturan güvenlik ikileminin aşılamadığı ve farklı şekillerde, farklı araçlar ve aktörler üzerinden tezahür etmeye devam ettiği görülmektedir. M.Ö. 5. yüzyılda yaşanan Peloponezya Savaşlarından Soğuk Savaşa uzanan yüzlerce yıllık süreçte tehditler karşısında güvenlik sağlanması kapsamında uygulanan dengeleme politikalarının diğer taraftan güvenlik ikilemini beslediği görülmektedir. Örneğin, M.Ö. 5. yüzyılın Grek şehir devletlerinin, aşırı güçlenen Atina devleti karşısında dengeleyici bir Sparta ittifakı kurduğu görülmüşse de ittifakın karşısında yapılanan Atina devleti ve kendi ittifakı bloklaşarak çözüm bulmak tehdit unsurunu yok etmede etkili olmuştur (Korab-Karpowicz, 2006: 47). İlk bakışta, çatışma ortamının oluşumunun sebebinin aktörlerin güvenlik endişesi olduğu görülmekle beraber güçlenen Atina devletinin ve karşısında kurulan ittifakın temel sebebinin tam anlamıyla salt askeri güce bağlanması yetersiz kalmaktadır. Zira Thucydides 'Pelaponez Savaşları' adlı çalışmasında çatışmanın sebebini bir aktörün asimetrik olarak güçlenmesinden kaynaklı korku ve endişe faktörlerine de dayandırmaktadır (Strassler, 1996: 128). Ancak, çatışmanın uzun yıllar sürmesi sonucunda Atina ve Sparta'nın askeri ve ekonomik olarak yıpranmış olduğu ve bir güç boşluğu oluştuğu anlaşılmaktadır. Bu güç boşluğu ise, M.Ö 359-336 yılları arasında hüküm süren II. Philip doldurmuş ve Grek yarım adasını egemenliği altına almıştır. Fakat kısa bir süre sonra düzenlenen bir suikast girişimi sonrasında yaşamını yitirmiştir. Ardından, Aristotales tarafından eğitilen oğlu Büyük İskender tahta geçtiğinde, ileri dünya görüşlü olması ve almış olduğu felsefi eğitimin getirisi ile üstün askeri teknikler geliştirerek Asya kıtasında Pers İmparatorluğu kontrolünde bulunan Yunan şehir devletlerini de ele geçirmiş ve akabinde M.Ö 326 yılında Pers İmparatorluğu'na son vermiştir (Worthington, 2014: 93). Asya kıtasında bugünkü Hindistan'a, Kuzey Afrika'da bugünkü Libya'ya kadar ulaşan sınırlarıyla, Büyük İskender'in ulaşmış olduğu sınırlar zamanının en genişini teşkil etmiştir. Buna ek olarak, Yunan kültürünün yayılmasına olanak sağlaması bakımından da oldukça önemli görülmektedir. Ortak değerlere sahip olan ancak farklı coğrafyalarda hüküm süren devletler küreselleşme sürecinin ilk aktörleri olarak karşımıza çıkmaktadır (Martin, 1996).

Tarihsel süreçte egemen devletler, 1618-1648 yılları arasında cereyan eden ve kilise ile krallıkların mutlak güç mücadelesine sahne olan Otuz Yıl Savaşları'nın sonucunda Vestfalya düzeninin teşkil edilmesiyle, uluslararası ilişkilerdeki yerlerini almışlardır. Kilise baskısından kurtulan ve egemen haline gelen devletlerin yürüttüğü ilişkiler, güvenlik anlayışının dönüşümünde önemli bir yere sahiptir. Askeri ve ticari ortaklıkların artması, büyük yıkım kapasiteli ateşli silahların yaygınlaşması ve gelecek on yıllar içerisinde ordu kapasitesinin genişlemesiyle yeni caydırıcılık mekanizmaları ortaya çıkmıştır. Ardından gelen Napolyon dönemi ile birlikte milliyetçilik ideolojisi inşa edilmiş ve egemen devletlerin ordu kapasitelerini hiç olmadığı kadar genişletmelerine olanak tanımıştır. Devletlerin sahip olduğu bu fiziksel güç unsurunun güvenlik anlayışını tabanından dönüştürerek karşılaşılan güvenlik stratejilerini ve ortaya çıkan ikilemleri farklı boyutlara taşımıştır. Örnek olarak, Napolyon hakimiyetindeki Fransa'nın yarattığı tehdit unsuru karşısında 5 farklı koalisyon kurulmuş ve her biri siyasi başarısızlıkla sonuçlanmıştır. Bu başarısızlıkların temel sebebi; karşılıklı güvensizliğin hakim olduğu koalisyon yapılanmalarında her devletin kendi çıkarlarını ortak çıkarların üzerinde tutmalarından kaynaklanmaktadır. Ordu emir komuta zinciri, finansal yönetim, stratejik planlama gibi bir çok hususta anlaşmazlığa düşen koalisyon kuvvetleri ta ki, ortak bir strateji planı oluşturmayı başardıkları 1813'e dek her denemede başarısız olmuştur (Thompson, 1990: 57). Diğer yandan Napolyon'un orduları tek bir merkezden yönetilmekte ve istikrarlı bir stratejik plan takip etmekte olduğu için rakipleri karşısında üstünlük sağlamıştır. Ortak kazançlar doğrultusunda ortaya çıkan kısa süreli koalisyon yapılanmalarının zaman içerisinde Avrupa Ahengi'ne evrilmesi ve bugünkü Avrupa'nın temellerini atması; karşılıklı işbirliği ve taviz verme sürecini iyi yöneten, ortak askeri, siyasi ve ekonomik stratejiler oluşturmayı başarabilen devletlerin kalıcı işbirlikleri oluşturacağını ve daha verimli sonuçlar elde edeceğini göstermektedir.

Yirminci yüzyıla gelindiğinde, Birinci Dünya Savaşı'nın ertesinde oluşturulan Milletler Cemiyeti, aktörlerin işbirlikleri kurarak ve uluslararası bir örgüt çatısı altında birleşerek savaşın sebep olduğu yıkımın onarılması, olası bir savaşın önüne geçilmesi ve savaş sonrası düzenin tesisini amaçlamıştır. Savaştan sonraki on yıllık süreç boyunca işbirlikleri ve ortak kazanç politikalarıyla sürdürülen ilişkiler fiziksel ve ekonomik güç odaklı politikaları ikinci planda bırakmıştır. Ancak, kaybeden tarafta bulunan devletlerin kabul ettiği şartlar yıllar boyunca ekonomilerini güçlendirmelerinin önüne geçmiş ve ardından patlak veren Büyük Buhranın yarattığı ekonomik kriz askeri güç odaklı politikaları yeniden ön plana çıkarmıştır. Buna ek olarak, ağır şartlar içeren antlaşmalar yoluyla galip devletler politikalarını mağlup devletlerin tekrar toparlanmasını güçleştirmek ve yeniden tehdit oluşturmalarını engellemek amacıyla oluşturmuşlardır. Ortaya çıkan durum itibariyle düşünüldüğünde de Milletler Cemiyeti politikalarının İkinci Dünya Savaşı'nı engellemekte yetersiz kaldığı ve hatta birçok açıdan körüklediği gözlenmektedir.

İkinci Dünya Savaşı sonrası dönemde bölgesel, kıtasal işbirlikleri ve bloklaşmanın artmasıyla iki kutuplu uluslararası sistemin temelleri atılmıştır. Hegemonik mücadelelere

evrilen küresel ölçekli rekabet, askeri ittifaklar üzerinden kıtalar arası ortaklıkları arttırmış ve güvenlik politikalarının küresel güvenlik çerçevesinde değerlendirilmesine vesile olmuştur. Özellikle Soğuk Savaş döneminde nükleer silahlar üzerinden dikte edilen askeri caydırıcılık stratejileri, olası bir çatışma durumunda aktörlerin birbirlerinin varlığına son verebilecekleri ve kazananı olmayan bir seviyeye tırmanmıştır. Bu denli yüksek seviyedeki caydırıcılık, çatışma ortamını sonlandırmak yerine aktörlerin vekâlet savaşlarına yönelmesine neden olmuş ve çatışma ortamının farklı alanlarda sürmesine sebebiyet vermiştir. Ayrıca tarafların kendi toplumlarını ve diğer kutuptaki toplumu medya organları aracılığıyla kendi tezleri doğrultusunda manipüle etmeye çalışması, toplum güvenliği ve birey güvenliği unsurlarını ilgilendiren bir durum arz etmiştir. Küreselleşme kavramının 1970'lerden itibaren ortaya çıkmasıyla; karşılıklı bağımlılık ve aktörler arası etkileşimin artması neticesinde güvenlik konuları çeşitlenmeye başlayarak içine bilim, teknoloji, kültür, medya, kamuoyu algısı gibi daha önce güvenliğin konusu olmayan kavramların da dâhil edilerek genişlemeye ve derinleşmeye başladığı görülmüştür (Erdoğan, 2013: 5).

Diğer taraftan, gerek Avrupa Topluluğu kapsamında ortaya konan işbirliği alanları, gerek yumuşak güç unsurlarının artan önemi, gerekse 1970'lerden itibaren altı çizilen karşılıklı bağımlılık unsuru kapsamında ekonomi ve çevre konularının güvenlik çerçevesinde değerlendirilmeye başlanmasıyla birlikte güvenlik yaklaşımında konu ve aktör bazında dönüşüm gözlenmeye başlanmıştır. Askeri olmayan unsurların güvenlik kapsamında ele alınmasıyla genişleyen güvenlik çalışmaları, realizmin devlet odaklı dar kapsamının dışına çıkılarak birey güvenliğinin konu edinilmesiyle derinleşen bir içeriğe yönelinmiştir. Devlet güvenliğinin yanı sıra, insani güvenliğin de güvenlik çalışmalarına konu edilmeye başlanmasıyla derinlik kazanmaya başlayan güvenlik yaklaşımı, askeri olmayan unsurların tartışılmasıyla da genişleyen bir nitelik kazanmıştır. İnsani güvenlik, bireylerin yaşadıkları coğrafyada güvensizlik hissetmelerine sebep olabilecek doğal veya insani felaketler sonrasında, can güvenliğini tehdit eden veya yaşam kalitesini olumsuz yönde etkileyen olaylar sonucunda ortaya çıkmaktadır. Örnek olarak, doğal afetler, kıtlık, ayrımcılık, çatışma vb. durumlar en temel sebepler arasında gösterilmektedir (Özdemir ve Özdemir, 2018: 9).

Çeşitlenen ajandasıyla da güvenlik anlayışına dâhil etmeye başlayan güvenlik yaklaşımı, devlet odağından birey odağına doğru derinleşmiştir. Aktörlerin çeşitliği ve sayısı arttıkça uluslararası ilişkiler klasik anlamda devlet ilişkilerinin ötesinde boyut kazanan bir yapıya doğru evrilmektedir. Derinleşen ve karmaşıklaşan ilişkiler ağı, güvenlik anlayışının sadece askeri güç kaynağı ile sınırlanamayacağını göstermekte ve birey güvenliğini tehdit eden konuların da ulusal güvenliği tehdit edebilecek boyutta olduğunu ortaya koymaktadır (Buzan, 2004).

Soğuk Savaş sonrası dönemde, salt askeri gücün güvenlik sağlanmasında ne derece başarılı olduğunu sorgulatan savaşlar ve gerek küreselleşme, gerekse teknolojide yaşanan

gelişmeler neticesinde farklılaşan güvenlik unsurlarına cevap verebilecek politika arayışlarına girildiği görülmektedir. Neo-liberal kurumsalcı bir yaklaşımla, Avrupa Birliği'ne giden yollar adım adım inşa edilirken ekonomiden dış politikaya varan farklı alanlarda çeşitlenen ve derinleşen işbirlikleri kurumsal bir yapıya dönüşmüştür. Güvenlik ikileminin karşılıklı bağımlılık ve fonksiyonalist bir kurumsal yaklaşımla aşılmaya çalışıldığı AB örneğinin yanı sıra küresel bağlamda yönetişim kavramı ortaya konmuş ve farklı konular üzerinden küresel yönetişim yaklaşımları tartışılmaya başlanmıştır (Thomas, 2000: 13). Bu bağlamda, karşılıklı bağımlılığın önde gelen dinamiklerden birini teşkil ettiği küresel düzlemde, güvenlik yapılanmasında kamu-özel işbirliğinin önemli bir noktayı oluşturduğu anlaşılmaktadır.

1.2 Soğuk Savaş Sonrası Dönemin Güvenlik Ortamının Kopenhag Ekolü ve Yönetişim Kavramı Çerçevesinde İncelenmesi

Soğuk Savaş döneminin iki kutuplu dünya görüşü tarafından inşa edilen güvenlik ortamında, büyük güçlerin sahip oldukları yıkım gücü, tüm dünyayı yaşanılmayacak hale getirme potansiyeli barındırmıştır. Ancak, silahlanma yarışının ve dolayısıyla kitle imha silahlarının kullanılma potansiyelinin zirvede olduğu bu dönemde, aktörler Dehşet Dengesi üzerinden caydırıcılık kavramına odaklanmışlardır. Realist anlayış çerçevesinde şekillenen bir güvensizlik ortamının mevcut oluşu, askeri güç odaklı bir anlayışın güvenlik sağlamada yeterli olmadığını göstermektedir (Sandıklı ve Emeklier, 2011: 4).

1.2.1 Geleneksel Güvenlik Anlayışının Şekillenmesi

Fiziksel güç odaklı güvenlik anlayışı olarak Realist teori merkezine temel aktör olarak devleti yerleştirerek güç odaklı bir paradigma meydana getirmiştir ve bu hususta devletler arası ilişkilerde, güvenlik anlayışı devletler arası rekabet ve çatışma ortamındaki dengenin değişme süreci içerisinde şekillenmektedir. Askeri konular ve ulusal sınırların güvenliği temel endişeleri oluşturmaktadır (Buzan, Weaver, ve De Wilde, 1998: 21). Bu yaklaşımın merkezinde güç unsurunun bulunması ve sistemin rekabet ve çatışma ortamları üzerinden şekillenmesinin temel sebebi, insan doğasının benmerkezci, çıkarcı ve değişmez olarak tanımlanmasından kaynaklanmaktadır (Küçüksolak, 2012: 203). Bu doğrultuda güvenlik politikaları, güç – tehdit – güvensizlik üçgeni kullanılarak şekillendirilmektedir. Devletler üstü bir otoritenin yokluğu anarşik bir sistem yaratmaktadır ve gücü elinde bulunduran aktör, uyguladığı politikaları tehdit unsuru belirtmesi halinde meşrulaştırabilmektedir (Sandıklı ve Emeklier, 2011: 6). Realist kuramın kurucuları olarak kabul edilen Thomas Hobbes, Niccolo Machiavelli ve Carl von Clausewitz gibi realist kuramın ana yazarlarının yaşamları göz önüne alındığında dünya görüşleri daha iyi anlaşılmaktadır. 1588-1679 yılları arasında yaşayan Hobbes, küçük yaşlarda İspanyol yağmalarına, gençliğinde İngiltere'deki iç karışıklıklara tanık olmuş ve entelektüel birikimini seyahatlerinde zenginleştirerek kuramını şekillendirmiştir. Realist kuramda, kaos ortamı içerisinde kendi çıkarını korumak için herkesin herkese karşı

olduğu bir dünya düzeninin varlığının ve hayatta kalmak için daimi mücadelenin şart olmasının temel sebebi Hobbes'un hayatının kargaşa içerisinde geçmiş olması gösterilmektedir (Yücel, 2016).

Machiavelli'ye göre de, hayatta kalma şansını maksimize etmek isteyen tüm devletler sürekli bir savaş hazırlığı içerisinde olmalı ve askeri gücü en önemli araç haline getirmelidir. İtalya'nın Floransa kentinde 1469 – 1527 yılları arasında yaşayan ve devlet yönetimi konusunda kendisini son derece iyi yetiştirmiş olan Niccolo Machiavelli'nin, şehir devletleri ile Papalık arasındaki siyasi rekabet ortamında hayatını sürdürdüğü görülmektedir. Oligarşik bir yönetim anlayışı benimsemiş olan İtalyan şehir devletlerinde Roma geleneğine bağlı ve kilise karşıtı bir görüş benimsenmiştir. Machiavelli, iyi ordular olmadan iyi yasaların var olamayacağını, halkın hükümdarını iyi bilmesinin şart olduğunu ancak hükümdarın iktidarını sağlamlaştırmak ve hükmünü meşru kılmak için tüm araçları kullanmasının da makul olduğunu savunmaktadır (Atkinson, 2008).

Realist kuramın önemli düşünürlerinden Carl von Clausewitz ise, savaş kavramını hasmı isteğimizi yerine getirmeye zorlayan bir şiddet eylemi olarak nitelendirmektedir (Howard ve Paret, 1984). Hasmın yarattığı güvenlik endişesini ortadan kaldırmanın tek yolunun karşı tarafı silahsızlandırmak olduğunu ve bu amaç doğrultusunda hasmı ortadan kaldırmanın meşru olduğunu savunmaktadır. Üstünlük kurulmayan ve boyun eğdirilmeyen düşmanın kendisine boyun eğdirebilme potansiyelinin endişesindedir. 1780-1831 yılları arasında yaşayan ve Prusya Ordusu'nda tümgeneralliğe kadar yükselen Clausewitz, Prusya monarkına ve prenslerine askeri danışmanlık görevi yapmış ve hem Prusya hem de Rus ordusunda Napolyon'a karşı savaşmıştır. Tüm hayatı savaş alanlarında geçmiş olan Clausewitz'in 'Savaş Üzerine' adlı eserinde politik hedeflerin savaş sürecinde değişebileceği, savaşın da devlet politikalarının bir uzantısı niteliğinde olduğu vurgulanmaktadır (Howard ve Paret, 1984: 80). Güvenlik anlayışı içinde bulunulan dönemin doğasına ve dinamiklerine göre şekillenmekte ve bu çerçevede güvenlik uygulamaları ortaya konmaktadır. Fiziksel güç odaklı Hobbesiyan teorisyenler, insanın kötücül doğasının ve çakışan çıkarlarının şiddeti kaçınılmaz kıldığını ve bundan uzaklaşmanın zorluğu üzerinde durmaktadırlar. Zira doğası gereği kusurlu olan insanın kurmuş olduğu devlet yapısı da kusurlu olmakta ve dolayısıyla bu problemli yapıda çatışma ve savaş kaçınılmaz hale gelmektedir.

Devletleri tek sesli konuşan, beka odaklı kara kutular şeklinde ele alan realist yaklaşımın sunmuş olduğu askeri unsurlarla kısıtlanmış güvenlik anlayışı, günümüzün çok boyutlu ve iç içe geçen güvenlik sorunlarının çözümünde yetersiz kalmaktadır. Kantçı görüş ise anlaşmazlıkları çatışma ve şiddetle çözmeye odaklanan tek taraflı bir yaklaşımdan ziyade barışçıl yöntemlerin uygulanabileceğini savunmaktadır. Modern dünyada sadece fiziksel güç odaklı bir uluslararası ilişkilerden bahsetmek mümkün değildir ve genişleyen, derinleşen ticaret ağı, ülkelerin çıkarları doğrultusunda fiziksel güç kullanımını sınırlandırmakta ve kurmuş oldukları ticari bağları zedelemeye cesaret etmelerini oldukça

zorlaştırmaktadır. Dahası, insan hakları, çevre güvenliği, uluslararası hukuk gibi konuların önem kazanmasıyla ve dünyanın özellikle yirminci yüzyıl sonrasında küresel bir köy haline gelmiş olması da bu savı destekler niteliktedir. Üçüncü bir görüş görüş olarak Grotiusçu düşünürler, anlaşmazlıkları çözmek için şiddet ve çatışma ortamının ortadan kalkmasının oldukça zor bir süreç olduğunu ancak fiziksel gücün yıkıcılığını azaltmak amacıyla birtakım norm ve kurallar geliştirilebileceğini öne sürmektedir (Baylis, 2008: 70). Bu doğrultuda ortaya konan kurallar, çatışma ortamını minimuma indirerek uluslararası anlaşmazlıkları çözmede medeni yollar bulunabileceğini göstermektedir. Hatta çatışmanın kaçınılmaz olduğu durumlarda da aşırı ve gereksiz olarak kullanılan fiziksel gücün kınanması, sistemin onanmasında büyük bir etkiye sahiptir.

1.2.2 Kopenhag Ekolünün Açıklanması

Soğuk Savaş sonrası güvenlik çalışmaları, güvenliğin çok boyutlu yapısını vurgulamakta ve konuları genişleyen bir çerçevede incelemektedir. Kopenhag Okulu'nun önemli teorisyenlerinden Barry Buzan güvenlik kavramına yönelik bakış açısını genişletmiş ve klasik fiziksel güvenliğin yanı sıra ekonomik, siyasi, toplumsal ve çevresel güvenliği de güvenliğin konusu haline getirmiştir. Ancak, 21. yüzyılda bu çok boyutlu güvenlik anlayışı da teknolojik gelişmeler doğrultusunda yetersiz kalmaya başlamış ve değişmesi zorunlu hale gelmiştir. Bu teknolojik gelişmeler göz önüne alındığında, yukarıda bahsedilen boyutlara siber güvenlik adında yeni bir boyut kazandırılmıştır (Hensen ve Nissenbaum, 2009: 1163). Daha kapsamlı ve açıklayıcı bir güvenlik anlayışına ihtiyaç olduğunu öngören Barry Buzan güvenliğin içerisine siyasi, ekonomik, çevresel ve sosyal konuları dâhil ederek geniş bir uluslararası çerçeve oluşturmuştur. Devletlerin, kendi çıkarları doğrultusunda geliştirdikleri politikalarını terk etmelerini ve komşu devletlerin çıkarlarını da gözetmelerini tavsiye etmektedir. Hem ulusal hem de uluslararası güvenlik endişelerinin giderilmesi amacıyla devletlerin işbirliği odaklı güvenlik yaklaşımlarını benimsemeleri durumunda güvenlik kaygısının azalacağı ve çatışma ortamından kaçınılabileceğini belirtmektedir (Buzan, 1983: 97).

Günümüzün dünya sisteminde aktör sayısı, aksiyon düzeyi, hedef kitlesi ve eylem amacı muğlaklaşmış ve tedbir kavramını anlamsızlaştırmıştır. Siber alanın güvenli hale getirilmesi hem bireysel seviyede hem de devlet seviyesinde büyük önem taşımaktadır. Yapılan tüm çalışmalara rağmen, siber güvenlik çalışmalarının verimliliği; tehditlerin muğlaklığı, tedbir almanın mümkün olmaması, yetişmiş personel azlığı ve politikaların teknolojik gelişimden yavaş ilerlemesi sebebiyle yetersiz kalmaktadır. Politikacıların siber tehditlerin farkında olmasına rağmen internet teknolojisinin devletlerin savunma politikasına dâhil olması uzun zaman almıştır. Bunun sebebi siber alana erişimi yasaklamanın güvenli hale getirmekten çok daha kolay olmasıdır. Çünkü tam anlamıyla güvenli bir siber alana erişmenin tek yolu kendi ülke içi siber ağını (intranet) kurarak (ör. Kuzey Kore) içeriden dışarıya veya dışarıdan içeriye erişimi engellemektir. Ancak bu

sistemin kişisel hak ve özgürlüklere ve batı medeniyetinin desteklediği hemen hemen tüm 'batı' değerlerine karşı olduğunu belirtmek gerekmektedir. Diğer yandan, batı değerlerini benimsemiş devletlerde geniş bir özel sektör yelpazesi bulunmakta ve devletler kendi görevlerinin de önemli bir kısmını özel şirketlere devretmek suretiyle hem maliyetleri azaltmakta, hem de serbest piyasanın gelişmesine ve genişlemesine olanak tanımaktadır. Böylece, devlet kasasından masraf etmeden işletme kârı karşılığında ülkenin altyapı hizmetlerinin oluşturulması, geliştirilmesi ve işletilmesi şirketlerin kendi sermayesiyle yürütülmektedir. Ancak yalnızca enerji, su, atık vb. hizmetleri gibi altyapı hizmetlerinin kamu-özel sektör işbirlikleri tarafından yürütülmesi beraberinde ciddi güvenlik tehditleri yaratmaktadır (Shore, Du, ve Zeadally, 2011: 19). İlerleyen teknoloji tüm altyapı hizmetlerinin otomatikleşmesine ve insan gücüne daha az ihtiyaç duyulmasına sebep olmakta ve otomatik olan her bilgisayar sistemi düzenli kontrol edilebilmesi amacıyla internete bağlı olmak zorundadır. Elektrik veya su şebekesine yapılabilecek herhangi bir saldırı toplumu haftalarca mağdur etmeye yeteceği gibi nükleer santrallere yapılabilecek bir saldırı çok daha ciddi sonuçlara sebep olabilmektedir veya bankacılık ve borsa gibi ciddi kâr payı sağlanan piyasalara yapılacak herhangi bir saldırının vereceği hasar oldukça büyük olacaktır. Estonya'da para piyasalarına, İran'da nükleer santrale daha önce saldırılar düzenlenmiş ve kimin gerçekleştirdiği bilinmesine rağmen kanıt gösterilemediği için sadece spekülasyon olarak kalmıştır. Büyük veya küçük her devlet kendi siber güvenlik altyapısını kurmak için kendi kaynakları ile veya özel şirketlerden destek alarak bu yapıyı oluşturmak zorundadır. Her devlet vatandaşlarının kimlik bilgilerini, şahsi kazançlarını ve gelecek güvencelerini tahsis etmekle yükümlüdür.

Geleneksel anlayışta, güvenlik politikaları oluşturulurken her devletin kendi güvenlik öncelikleri jeopolitik konumuna göre belirlenmektedir. Ancak siber alanda ülkelerin konumu önemsizleşmekte ve bu sebeple siber güvenlik politikaları belirlenirken mevcut veya öngörülebilir tehditlere göre değil, çağın gerektirdiği tüm önlemler alınarak politika izlenilmesi gerekmektedir.

1.2.3 Yönetişim Kavramının Açıklanması

Yönetişim; yönetimi çok boyutlu ve parçalara ayrılmış kontrol mekanizmalarının hibritleştirilmesi çerçevesinde düzen ve düzensizlik, verimlilik ve meşruiyet üzerine devlet içinde, devlet tarafından, devlet olmaksızın ve devlet ötesinde gerçekleştirilen disiplinler arası bir araştırma gündemi olarak tanımlanmaktadır (Levi-Faur, 2012: 28). Kontrol mekanizmalarının sayıca çokluğu politikaların çeşitlenmesine imkân sağlayarak karar verme sürecinin demokratik bir şekilde yürütülmesini teşvik etmekte ve devlet dışı aktörleri karar alma sürecinde devlet ile eşit konuma getirmektedir. Bu sayede, devlet ve devlet dışı kurumlarının haiz olduğu risk unsurlarının kontrol altında tutulabilmesi için yeni yöntemler geliştirilmesini teşvik etmektedir. Yönetim, hiyerarşik olarak inşa edilmiş devlet kurumlarının eylemi olarak tanımlanmakta iken, yönetişim ortak çalışmaya dayalı gayriresmi sistemler arasında gücün dağıtılması olarak düşünülebilmektedir (Barkay,

2009: 368). Her ne kadar devlet hâlâ yerel, ulusal ve devletler arası politikalarda karar verici konumunda yer alsada artık toplumun refahını sağlamak hususunda tekel rol oynamamaktadır. Egemen devletin, koymuş olduğu yasalar doğrultusunda toplumu 'tepeden inme' yönetme anlayışı geçerliliğini yitirmiş ve yerini karşılıklı bağımlılığa, müzakereye ve güvene dayalı yönetişim anlayışına bırakmıştır (Sørsensen ve Torfing, 2005: 198).

Hedef belirleme ve belirlenen hedef doğrultusunda politikalarının planlanması başarılı bir yönetişim mekanizması inşa etmenin ilk adımlarını meydana getirmektedir. Hedef koyma aşaması esas olarak devlet tarafından karar verilebildiği gibi, devlet dışı aktörlerin de karar alma sürecine dahil edilmesini de içerebilmektedir. Bilhassa paydaşlar ile birlikte alınan kararların akabinde uygulanan politikaların, devlet merkezli olanlardan daha etkili olacağı öngörülmektedir. Zira, koyulacak hedef konusunda paydaşların uzlaşması ve koordineli hareket etmesi önceliklerin belirlenmesinde kilit rol oynamaktadır. Alınan kararların yürürlüğe konması sürecinde rol alacak mekanizmaların da bu süreç içerisinde belirleneceği hesaba katıldığında müzakere aşaması sistem dahilinde rol alan tüm aktörlerin katılması gereken bir süreç olarak öne çıkmaktadır. Uygulama sürecinde karşılaşılma ihtimali olan problemlerin bu süreçte tartışılması ve önleyici tedbirlerin alınması, hesap verilebilirlik ve geri bildirim mekanizmalarının etkili çalışmasının sağlanması için önem taşımaktadır (Peters, 2012: 45). İnşa edilen yönetişim mekanizmaları devletler, devlet kurumları, özel şirketler, bireyler, sivil toplum kuruluşları, uluslararası örgütler gibi çeşitli boyutta ve güçte aktörleri içerebilmektedir.

Yönetişim anlayışının hangi aktörler arasında ve ne şekillerde meydana geldiğinin daha açık bir şekilde anlaşılması açısından Börzel ve Risse'nin oluşturmuş olduğu 'Yönetişim Alanı' tablosu oldukça faydalı bulunmaktadır.

Tablo 1. Yönetişim Alanı

Yönlendirme Modlarında Mevcut Olan Aktörler	Yalnızca Devlet Kurumları	Devlet ve Özel Sektör Ortaklıkları	Yalnızca Özel Sektör
Hiyerarşik: Tepeden İnme; Yaptırım (Tehditleri)	- Geleneksel ulus-devlet; - Ulus-üstü kurumlar (AB, kısmen DTÖ)		
Hiyerarşik Olmayan 1: Teşvikler; Pazarlık	- Devletlerarası pazarlık	- Kamu faaliyetlerinin özel sektöre devredilmesi - Korporatizm - Kamu-özel sektör	- Şahsi çıkar amaçlayan devlet/özel sektör rejimleri
Hiyerarşik Olmayan 2: Manipülatif Olmayan İkna (öğrenme, tartışma vb.)	- Kurumsal problem çözme	- Şebekeler ve ortaklıklar - Kıyaslama	- Kamu-özel sektör ortaklıkları (STK'lar-özel şirketler)

(Taralı alan: Yönetişimin kullanıldığı alanları; koyu taralı alan: kamu-özel sektör işbirliklerinin kullanıldığı alanları göstermektedir)

Kaynak: Börzel, T. A., ve Risse, T. (2002: 3) Public-Private Partnerships: Effective and Legitimate Tools of International Governance *The Reconstitution of Political Authority in the 21st Century* (s. 1-23). Florence: University of Toronto.

Tabloda da görüldüğü üzere, yönetişim biçimlerinden biri olarak kamu-özel sektör işbirlikleri devlet, STK'lar ve özel şirketlerin belirli bir amacı veya amaçları gerçekleştirmek üzere bir araya geldikleri işbirliği oluşumu olarak ortaya çıkmıştır. Bilhassa belirli konularda karar verme sürecinde uzmanlıklarına danışılması gereken bir altküme olarak uluslararası ilişkilere dâhil olmuştur.

Küreselleşme, sosyal ve politik hayatın sadece devlet kurumları tarafından yönetilemeyecek kadar çok parçaya ayrılmasına sebebiyet vermektedir. Esas olarak tek bir aktörün tüm toplumun ve ekonominin işleyişini tek başına yönetmeye yetecek bilgisi, kapasitesi ve otoritesi bulunmamaktadır. Bu süreç, yönetimden yönetişime geçiş aşaması olarak gösterilmekte ve tepeden inme yönetim anlayışının yerini işbirlikleri çerçevesinde çözüm amaçlı bir araya gelmekte olan resmi kurumların ve gayri resmi olarak STK'ların, özel şirketlerin ve bireylerin oluşturduğu, kendi kendini yöneten mekanizmalara bırakacağı öngörülmektedir. Bilhassa, siber alanın çeşitli aktörler tarafından ticari ve politik amaçlar doğrultusunda aktif bir biçimde kullanılmakta olması, ulusal güvenlik politikalarının da çok boyutlu perspektifler aracılığıyla geliştirilmesinin gerekliliğini beraberinde getirmektedir. Bu bağlamda ulusal ve küresel çapta yürütülmesi gereken yönetişim politikaları, tüm aktörlerin ortak çıkarlarının korunmasına ve daha etkili stratejiler oluşturulmasına önemli katkılar sağlamaktadır. Örneklendirmek gerekirse, ulusal yönetişim kavramı, ulusal sınırlar içerisinde politik faaliyet gösteren devletin, ticari faaliyet içerisinde olan özel sektörün ve toplumsal fayda amaçlı kurulmuş olan STK'ların ortak çıkarlar çerçevesinde şekillenen çok paydaşlı politikalar geliştirmelerine imkân sağlamaktadır. Yürütülen faaliyetlerin birçoğunun siber alana entegre olması, ortak

güvenlik politikalarının şekillenmesine vesile olmakta ve çok paydaşlı stratejiler oluşturulmasına ortam hazırlamaktadır. Ayrıca, siber alanın uluslararası aktörler tarafından aktif bir şekilde kullanılmasının, uluslararası işbirliklerinde küresel yönetişim kavramının da önemini arttırıcı bir etkiye sahip olduğu düşünülmektedir. Küresel karşılıklı bağımlılığın siber alan üzerinden yürütülmekte olan faaliyetler sonucu artmasıyla, aktör sayıları devletler ile sınırlı kalmayarak çeşitlenmekte ve devlet-dışı aktörlerin hareket kabiliyetini arttırarak küresel problemler üzerine yürütmekte oldukları faaliyetlerin etki alanının derinleşmesine ve kamu-özel sektör işbirliğinin kullanım alanlarının genişlemesine olanak tanımaktadır.

1.2.4 Soğuk Savaş Sonrası Dönemin Güvenlik Ortamının Temel Dinamikleri

Soğuk Savaş sonrası dönemde küreselleşmenin de artan etkisiyle aktörler ve konular hiç olmadığı kadar genişlemiştir. İnsan güvenliği, toplumsal güvenlik ve çevre güvenliği akademik yazınlarda yer bulmaya başlamıştır. Güvenlik anlayışı, hem normatif hem de rasyonel değişkenleri hesaba katarak yeniden tanımlanmakta ve askeri olmayan tehditleri de içine alacak kapsama ulaşmaktadır (Ağır, 2011). İlerleyen teknolojinin sağladığı olanaklar ve tehditler, sistemdeki aktörlerin çeşitlenmesine yol açmakta ve bu sebeple, güvenlik tehditleri de dönüşmekte ve muğlaklaşmaktadır. Yirminci yüzyılın sonlarında bilişim teknolojilerinde yaşanan gelişmeler, siber saldırı örneklerinde de görüldüğü üzere yeterli bilgi ve beceriye sahip bireylerin devletlerle aynı düzlemde hareket edebilmesine olanak vermiştir.

Özellikle yirminci yüzyılda yaşanan dünya savaşları ve Soğuk Savaş süreci, fiziksel çatışmanın dünyanın en modern devletleri için bile ağır sonuçlar doğuracağı ve hiçbir yönden kazananı olmayan çatışmalara yol açacağını işaret etmektedir. Savaşların yarattığı ekonomik krizler sadece savaşa giren devletlerin değil, aynı zamanda ticari ortaklarının da yıllar boyunca ekonomilerini düzeltememesine sebep olmuştur (Baylis, 2008). İdeolojik bloklaşmalar, kitle imha silahları ve soykırımlar, geniş çaptaki bilimsel ve teknolojik ilerlemenin önündeki engel haline gelmiş ve savaş teknolojisi üzerine yoğunlaşarak bu alanlarda ulaşılabilecek potansiyelin gerisinde kalınmasına sebep olmuştur.

Güvenlik anlayışının yeni bir boyut kazandığı Soğuk Savaş sonrasında yapılan çalışmalar dönemindeki sistemin yapısı, aktörleri ve aktörlerin sayı ve çeşitliğinden etkilenerek gelişmiş ve çok çeşitli görüşler ortaya çıkartmıştır (Hensen ve Nissenbaum, 2009). Bilhassa 1990'lardan başlayarak küreselleşmenin artması değişimin oldukça hızlı gerçekleşmesine sebep olmuştur. Güvenliğin kimin için ya da neyin için sağlanması gerektiği tartışmalarıyla birlikte güvenliğin edilgen boyutu önem kazanmaya başlamıştır. Askeri tehditler hala önemini korurken, aynı zamanda ideolojik, sosyal, toplumsal, dini, kültürel ve çevresel tehditler de güvenliğin konusu haline gelmiştir. Geleneksel devlet temelli güvenlik anlayışının yeni tehditleri ortadan kaldırma girişimleri bireysel olarak elimine etmelerinden ziyade, işbirlikleri kapsamında dünyanın ortak problemi olarak

görülen tehdit unsurlarına karşı mücadele hız kazanmaya başlamıştır. Bunun yanında, çeşitlenen ve artan aktör sayıları asimetrikleşmeye ve dolayısıyla tedbir imkânlarının kısıtlanmasına yol açmıştır (Erdoğan, 2013: 5).

1.3 Devlet Dışı Aktörlerin Güvenlik Ajandasındaki Yeri

20. yüzyılın çeşitlenen aktör sayıları kapsamında devlet dışı aktörler, hem ulusal hem uluslararası güvenlik konularının ana unsurlardan biri olmaya başlamışlardır. Zira haiz oldukları tehdit unsurları devletlerin hassasiyet göstermesi gereken noktaları arttırmakta ve kırılganlıkları büyük ölçüde çeşitlendirmektedir. Sonuçta, güvenlik tedbirlerinin etkili bir biçimde alınması için aktörlerin ilk önce güvenlik ortamını analiz etmeleri, ardından bu ortam içerisindeki hangi unsurların tehdit algıları ile örtüştüğünü belirlemeleri gerekmektedir. Daimi bir değişim ve dönüşüm süreci içerisinde güvenlik ortamı Soğuk Savaşın sona ermesiyle birlikte devlet seviyesinden birey seviyesine doğru inerek derinleşmeye başlamıştır (Küçükşahin ve Akkan, 2007: 44).

1.3.1 Bireyin Güvenlik Aktörü Haline Gelmesi

Birey güvenliği kavramı özellikle teknolojinin ilerlemesi ve küreselleşmenin gelmiş olduğu aşamalar sonucunda önem kazanmaya, akademik yazınlarda yer bulmaya başlamıştır (Tangör, 2012: 63). Yirminci yüzyılın sonundan itibaren, birey güvenliğine yönelik tehditler büyük çoğunlukla diğer bir devletin askeri gücünden ziyade, ekonomik kriz, yükselen suç oranları, insan kaçakçılığı, etnik çatışmalar, terör, hastalık, siyasi baskı gibi sebepler üzerinden değerlendirilmektedir. Özellikle, gelişmekte olan ve geri kalmış devletlerin kendi halklarına yönelik tehditleri önlemede yetersiz kalmaları, devlete olan güveni sarsmakta ve mevcut durumun kötüleşme hızını arttırmaktadır (Booth, 1991: 318).

Soğuk Savaşın sona ermesinden itibaren geniş bir çerçevede tartışılmaya başlanan güvenliğin kimin için tesis edilmesi gerektiği sorusu birey güvenliği üzerine yapılan çalışmaların sayısını arttırmış, aynı zamanda güvenlik kavramının çeşitlenmesine ve derinlemesine incelenmesine olanak sağlamıştır (Krause ve Williams, 1997: 228-232). Geleneksel güvenlik anlayışı çerçevesinde devlet merkezli olarak inşa edilen güvenlik algısı askeri gücü en önemli araç olarak benisemekte ve kullanımını Clausewitz'in de belirttiği üzere diplomasinin bir uzantısı olarak meşrulaştırmaktadır (Howard ve Paret, 1984: 97). Diğer yandan, genişletilmiş güvenlik anlayışı içine aldığı konular ve içerdiği aktör çeşitliliği sebebiyle güvenliğin tahsis edilmesini bir sorumluluk olarak tanımlayarak devletlerden uluslararası örgütlere, sivil toplum örgütlerinden kamuoyuna uzanan bir aktör yelpazesine dağıtmaktadır (Thomas, 2000: 113).

Soğuk Savaş sonrası döneme kadar, uluslararası ilişkiler disiplininde güvenlik yaklaşımlarından bahsederken kastedilen güvenlik anlayışı ulusal güvenlik politikalarını ve stratejilerini ifade etmektedir (Booth, 1991: 318). Özellikle İkinci Dünya Savaşı ve

Soğuk Savaş dönemlerinde gerçekleştirilen toplu idamlar[1], işkence[2] ve soykırım suçları[3] ulusal güvenlik çerçevesinde meşrulaştırılabilmiştir. Devlet merkezli güvenlik anlayışı, ulusal güvenliğe tehdit yaratan her türlü durumun bertaraf edilmesi gerektiği üzerine yoğunlaşmaktadır. Ayrıca, devlet bekası odaklı klasik güvenlik yaklaşımını benimseyen aktörler insani güvenliğe yönelik mülahazaları bu çerçevede göz ardı edebilmekte ve sivil zayiat önemsenmeyebilmektedir. Geleneksel güvenlik anlayışının önemli temsilcilerinden Niccolo Machiavelli'nin de 'Prens' adlı eserinde bir prensin tek meşguliyetinin savaş olması gerektiğini ve barışın yalnızca savaş planları yapmaya yetecek kadar nefeslenecek bir vakit olarak düşünülmesi gerektiğini belirtmektedir (Atkinson, 2008: 249). Geleneksel güvenlik anlayışı çerçevesinde, devlet güvenliğinin sağlanması amacıyla alınacak tedbirlerin sınırlanması mümkün görülmemektedir ve aynı zamanda kendi halkına zulmeden devlet, kendi bekası için bunu meşrulaştırabilmektedir. Yakın tarihe bakıldığında, devletler arasında gerçekleşen savaşlar sonucunda hayatını kaybeden bireylerin sayısı[4] özellikle Soğuk Savaş döneminin son bulmasıyla kaydadeğer bir azalma göstermiştir. Ancak kendi devleti tarafından doğrudan veya dolaylı şekilde zarara uğrayan ve bunun sonucunda intihar, hastalık, kıtlık, ayrımcılık vb. durumlar sonucu yaşamını yitiren veya göç etmek zorunda kalan bireylerin sayısı[5] savaş esnasında ölenlere kıyasla daha yüksek seyretmeye devam etmektedir (Simon Fraser University, 2013: 24-25).

Doksanlı yıllarda iki kutuplu dünya sisteminin son bulmasıyla güvenlik meselelerini meydana getiren şartlar değişmeye başlamıştır (Çetinkaya, 2012-13: 244). Özellikle siber alanın terör ve suç örgütlerine sağladığı imkanlar çerçevesinde küresel bir güvenlik

[1] 1930-1953 yılları arasında Stalin Rusyasında en aktif şekilde uygulanan toplu idamlar devlet düşmanları ve vatana ihanet suçundan hüküm giymiş mahkûmların, Sibirya'da konuşlanan kamplarda ağır şartlarda çalıştırılarak veya kurşuna dizilerek idam edildiği hapishane sistemidir. Toplamda 12.000.000 kişinin çalışma şartları, işkence ve soğuk gibi çeşitli sebeplerden yaşamını yitirdiği Gulag Kampları örnek olarak verilebilir (Özakın, 2019 "Kötülüğün Sıradanlığı": Aleksandr Soljenitsin'in Sovyet Çalışma Kampı İzlenimlerini Hannah Arendt'in Kavramlarıyla Okumak. *RumeliDE Dil ve Edebiyat Araştırmaları Dergisi,* (15), 431-468. DOI: 10.29000/rumelide.580703).

[2] 13. yüzyıldan 16. yüzyılın sonlarına kadar Avrupa ve Amerika'da kilise önderliğinde kurulan mahkemelerde masum insanlar işkence ile konuşturularak idam edilmiştir. İdam edilen ve işkence sonucu yaşamını yitiren insanların %90'ını kadınlar oluşturmaktadır (Aksan, Yücel *'1450 – 1750 Yılları Arasında Avrupa'da Cadılık, Tarih İncelemeleri Dergisi'* XXVIIII' 2, 2013: 355-368).

[3] Nazi Almanyası ve Mussolini İtalyasının güdümünde Avrupa Yahudileri için oluşturulan ve toplu kıyımların gerçekleştirildiği toplama kampları kapsamında tüm Avrupa'da toplam 5,846,032 kişi zalimce katledilmiştir (Dominick LaCapra 1994, Representing the Holocaust: History, Theory, Trauma Cornell University Press).

[4] 1946'dan 2011'e kadar ölçülen devletlerarası savaş sırasında ölüm oranları 1951'de ±550.000 ile en yüksek değer olarak kaydedilirken, Soğuk Savaş süresince ±50.000 (1977) ile en düşük ve ±320.000 (1971) en yüksek değer arasında dalgalanma göstermektedir (Human Security Report, 2013: 18).

[5] 1950 – 2011 yılları arasında iki devlet arasındaki savaşlardan dolayı yaşamını kaybeden insan sayısı gittikçe azalmış ve 2000'lerin ilk on yılında en alt seviyelere ulaşmıştır. Diğer yandan, iç savaşlar, kıtlık, intihar, hastalık vb. sebeplerden yaşamını yitiren bireylerin sayısı Soğuk Savaşın sona erdiği 1990 yılına kadar katlanarak artmaya devam etmiş ve 2000'lerin ilk on yılında istikrarını korumuştur. En büyük kıyım 1980-1989 yılları arasında gerçekleşmiş olup yıllık ölüm oranı ±2900 olarak verilmiştir (Human Security Report, 2013: 24).

yaklaşımı ortaya çıkmaya ve devletin güvenliğin sağlanmasındaki yegane aktör olduğu yaklaşım yetersiz kalmaya başlamıştır. Güvenliğin tesis edildiği alanlara beşinci alan olarak siber alan dahil edilerek bu yapı çerçevesinde kollektif bir güvenlik anlayışı geliştirilmeye başlanmıştır. Kopenhag Ekolü güvenlik dışı herhangi bir konunun politik söylemler aracılığıyla güvenliğin konusu haline getirilebileceğini, bir diğer deyişle güvenlikleştirilebileceğini savunmaktadır (Buzan, Weaver, ve De Wilde, 1998: 25).

1.3.2 Birey ve Kurum Güvenliğinin Devlet Güvenliğine Etkisi

İlerleyen teknoloji, suç ve terör örgütlerinin mevcut üyelerine, aralarına katmak istedikleri bireylere ve hedefleri olan nüfuz sahibi bireylere ulaşımalarını kolaylaştırmakta ve kırılganlıkları arttırmaktadır. Ayrıca, fon toplama, plan yapma, bilgi aktarma faaliyetlerinin de siber alanın mümkün kıldığı gizlilik sayesinde kolaylaştığı görülmektedir. Dahası, siyasi bir amaç veya herhangi bir sebepten doğmuş olan mağduriyetler doğrultusunda kimi bireyler bu tip örgütlere daha kolay ulaşabilmekte ve aralarına katılabilmektedir (Nye, 2010: 12-13). Siber alanda kendini yetiştirmiş bireyler kendi başlarına bu alan içerisinde oldukça aktif olabilmekte ve hem devletin kritik altyapı sistemlerine hem de özel sektöre ciddi zararlar verebilmektedirler. Özellikle kriz anlarında faydalı olabilecek bireylerin yetiştirilmesi ve kritik pozisyonlarda görevlendirilmesi, mevcut tehditlere karşı savunma stratejilerinin geliştirilmesi ve güvende olma hissinin sağlanmasında önemli rol oynamaktadır. Kendini yetiştirmiş olan ancak beyin göçü yoluyla kaybedilen bireyler güvenlik açığı yaratmaktadırlar. Ayrıca, faaliyetlerin toplumda yaratacağı korku ve panik devletin, toplumun güvenini kaybetmesine ve kaos ortamının oluşmasına zemin hazırlamaktadır. Bu faaliyetlerin önüne geçilmesi hem devlet güvenliği hem de birey güvenliği açısından ciddi önem taşımakta ve bu hususta kollektif güvenlik stratejilerine ihtiyaç duyulmaktadır. Çünkü, pekçok durumda saldırıya uğrayan devlet kurumları[6] veya özel şirketler siber saldırı gerçekleştirildiğini reddetmekte veya savuşturulmuş bir girişim olarak adlandırarak kırılgan bir durumda olmadıklarını ilan etmektedirler. 2003 yılındaki FBI verilerine göre, siber saldırılara maruz kalan özel şirketlerin yalnızca %30'u durumu polise bildirmiş, %21'i yaşadıkları saldırıdan ötürü maddi kayıp belirtmiş ve endüstriyel casusluk şüphesi ile hukuki yollara başvurmuştur (CSI/FBI, 2003: 18).

Siber alan içerisinde faaliyet gösteren tüm aktörlere, amaçları çerçevesinde yöntemler geliştirmeleri için olanaklar sağlamaktadır. Aktörler devlet, uluslararası örgüt, çokuluslu şirket, organize suç örgütü, terör örgütü veya birey formunda karşımıza çıkmakta ve her aktörün kendi çıkarlarına yönelik aktivitede bulunması farklı türden aktörleri karşı karşıya getirmektedir. Siber alanı çıkarları doğrultusunda kullanan her aktör devletin

[6] İran'ın Natanz'da bulunan nükleer materyal zenginleştirme tesisine Stuxnet virüsü ile yapılan saldırı kabul edilmemiş ve yaşanılan gecikmenin teknik bir arıza sebebiyle kaynaklandığı belirtilmiştir (Brown, 2011: 70-73).

kritik altyapı sistemlerine müdahelede bulunabileceği gibi aynı zamanda vatandaşların kimlik bilgilerine, kişisel verilerine ve gelir kaynaklarına karşı da bir tehdit yöneltmektedir. Kurumlar açısından değerlendirildiğinde ise, hassas bilgilere dışarıdan erişilebilme ihtimali, ticari ortaklara ve müşteri bilgilerine yönelik bir tehdit arz ederek kurumları çok daha kırılgan hale getirmektedir (Carr, 2016: 48). Söz konusu kurumların devlet ile su, enerji veya internet gibi bir altyapı oluşturulması ve dağıtımı hususunda işbirliği içerisinde olan bir kurum olması devlet güvenliğini de doğrudan tehdit eden bir nitelik ihtiva etmektedir (Carr, 2016: 46).

Devletler, siber güvenlik altyapısının oluşturulması ve personelinin yetiştirilmesi amacıyla mali kaynak ayırabilmektedir. Aynı zamanda, sahip oldukları imkanlar dahilinde bilgi toplama faaliyetleri gerçekleştirebilmekte ve pazar kontrolünü sağlayarak hem siber hem geleneksel operasyonel alanlar üzerinden politika yürütebilmektedir. Devlet, otoritesini ve kontrolündeki kolluk kuvvetlerini kullanarak veya vergilendirme uygulayarak bireyler ve kurumlar üzerinde baskı kurabilmektedir. Bunlara ek olarak, aktif oldukları piyasa üzerinde kontrol sağlayarak avantaj sağlayabilmektedir. Dahası, devlet imajı oluşturmak ve yumuşak güç aracı olarak siber alandan faydalanabilmektedir. Ancak, sahip olunan kritik altyapı sistemleri hem yüksek mali giderler yaratmakta hem de siber saldırılara karşı yüksek kırılganlıklara sebep olmaktadır. Ayrıca siyasi istikrara sahip olmayan devletlerde hükümet değiştikçe izlenen poltikalar değişebimekte ve farklı politikalar yürürlüğe konabilmektedir ve bu da mali kaynakların hızla tükenmesine yol açmaktadır.

Kurumlar siber alandaki güvenlik altyapılarını oluştururken birincil amaçları şirket verileri ve çalışanların kişisel bilgilerin korunması yönünde stratejiler geliştirmektedir. Sahip oldukları bütçe birçok farklı kaynaktan beslendiği takdirde gelişmekte olan bir veya birkaç ülkeden fazla yıllık gelire sahip oldukları görülmektedir. Etkinlik alanlarını farklı coğrafyalara yayabilme kapasitesine sahip olmaları esneklik sağlamakta ve global bir etki yaratma imkanı sunmaktadır. Çeşitli ülkelerden alanında uzman kişileri istihdam ederek etkin bir insan gücü toplayabilmektedir. Geliştirilen stratejilerin ve uygulamaların patentleri kuruma ait olduğu sürece etkin bir güvenlik politikası izlenebilmektedir. Ancak, bu tip yüksek yapılanmalı kurumlar özellikle endüstriyel casusluk amacıyla siber saldırıların hedefi olmaktadır. Ayrıca, herhangi bir alandaki itibar kaybı tüm kurum imajına yansımakta ve mali kayıplara sebep olmaktadır.

Bireylerin siber alanda aktif olabilmeleri için sahip olmaları gereken donanım maliyeti devletlere ve kurumlara kıyasla oldukça düşüktür. Çünkü, bireyler siber alanda anonim olarak var olabilmekte ve bu sayede savunma stratejileri daha çok ikinci planda kalmaktadır. Ayrıca bireyler belli bir süre sonra siber alanda aktif olmamayı seçtiklerinde geçmiş faaliyetlerinin tespit edilmesi oldukça güç olmaktadır. Dahası, gerekli ekipmana ve bilgiye sahip oldukları takdirde herhangi bir kuruma, bireye veya devlete tehdit oluşturabilecek kapasiteye erişebilmektedirler. Ortaya çıkan bu asimetrik tehdit tüm

aktörler nezdinde kabul görmektedir. Bu tehdit unsuru sebebiyle diğer aktör grupları bireylerin siber alandaki faaliyetleri konusunda hassas davranmaktadır ve aktif bireyleri istihdam etmekte veya yasal veya yasal olmayan baskı araçlarıyla sindirmektedir.

Siber alanda aktif olan tüm aktörler kendi güvenliklerini maksimize etmeye çalışmaktadır. Fakat, saldırı imkanlarının savunma yöntemlerinden daha düşük maaliyetli olması sebebiyle kollektif bir çalışma olmadan güvenlik tam olarak sağlanamamaktadır. Devletler, kurumlar ve bireylerin siber güvenliklerinin sağlanması amacıyla triumvirate[7] bir yöntem uygulanması gerekmektedir.

1.3.3 Geleneksel Tedbirler, Modern Tehditler ve Yönetişim

Küreselleşmenin geldiği nokta ve teknolojideki ilerleme ile birlikte tehdit içeriğinin dönüşümü güvenlik kavramının sadece devlet tabanlı bir yaklaşım çerçevesinde incelenmesini yetersiz kılmaktadır. Geçmişte bir tehdit algısının oluşması için bir devletin başka bir devletin toprak bütünlüğünü tehdit etmesi yegâne tehdit unsuru olarak değerlendirilirken, gelmiş olduğumuz noktada çevre tahribatına sebep olan, terör faaliyetlerini destekleyen, uluslararası hukuka uymayan veya kitle imha silahlarına[8] sahip olan aktörler de güvenlik tehdidi oluşturmaktadır (Kibaroğlu, 2014: 7-16). Endüstriyel faaliyetleri doğrultusunda çevre hukukunu hiçe sayan, siyasi amaçları gerçekleştirmek için isyancı gruplara, terör örgütlerine destek veren, yasal ve yasadışı baskı araçlarıyla bireyleri sindiren devletler, artık beka odaklı söylemlerle eylemlerini meşrulaştıramamaktadır. Yerel veya bölgesel tehditler varlığını devam ettirmekle beraber artan küresel güvenlik tehditlerinin mevcudiyeti bütüncül tedbirler gerektirmektedir. Özellikle de birey güvenliği ve bireylerin sebep olduğu güvenlik tehditleri siber alan çerçevesinde şekilllenen güvenlik ortamında karşımıza çıkmaktadır. Günümüzde, özellikle siber alanın sağlamış olduğu imkanlar dahilinde bireyler ciddi güvenlik tehditleri oluşturabilmekte, hem etken hem edilgen hale gelebilmekte ve devletlere önemli ekonomik veya siyasi kayıplar yaşatabilmektedirler.

Güvenlik alanı tüm aktörlerin devamlı rekabet içerisinde olduğu fakat devletin aktör olarak sahip olduğu geniş imkanlar ve elverişli yapılanmaları sayesinde tarihsel olarak ayrıcalıklı kabul edildiği subektif bir fenomendir (Buzan, Weaver, ve De Wilde, Security, 1998: 36). Buna rağmen, tehditlerin gelişen teknoloji ile birlikte asimetrik hale gelmesiyle devletin güvenliğini sağlaması için sadece resmi kurumları değil, aynı zamanda özel kurumları ve bireyleri de kapsayacak bir güvenlik stratejisi oluşturması gerekmektedir.

[7] Bir operasyon veya aktivitenin yönetiminin üç ayrı merci tarafından gerçekleştirilmesidir (Cambridge University Press, 2020).

[8] Kitle imha silahları; nükleer, kimyasal ve biyolojik yıkım gerçekleştirme potansiyeli olan, kullanıldığı bölge ve bölgede yaşayanlar üzerinde geri döndürülemeyecek hasarlara yol açan araçlardır. Orantısız güç kullanımının en önemli örneği olmakla beraber, kitle imha silahlarına sahip olan iki aktörün bu silahları kullanarak çatışmaya girmesi durumunda çevresel ve insani felaketlerin yaşanması kaçınılmazdır.

Siber güvenlik altyapılarının oluşturulması, özel kurumların finansal temelli veya devletlerin beka odaklı politikalarına terk edilemeyecek kadar kritik bir alan olarak görülmekte ve kollektif bir çabayla kamu-özel sektör işbirlikleri aracılığıyla oluşturulduğu takdirde ortak faydaya ve amaca hizmet etmesi mümkün olabilmektedir (Hensen ve Nissenbaum, 2009: 1162). Siber alan çerçevesinde güvenlik ihtiyacı tek bir aktöre veya alana odaklanmamakta, bireye, devlete veya tüm topluma yönelik tehditler bütüncül bir çerçevede değerlendirilmektedir. Tehditler siber alanda mevcut olan kırılganlıklardan faydalanarak ortaya çıkmakta ve tehdit oluşturduğu kesim kapsamında kollektif tedbirler gerektirmektedir (Sarbu, 2017: 132). Siber alanın güvenlik tehditleri her ne kadar öngörülemez ve önlenemez gibi görünse de kollektif bir çalışma ile bariz kırılgan noktalar aşılabilmektedir.

Siber alanda yalnızca devleti, kurumları veya bireyleri koruyacak yaklaşımlar diğer aktörleri savunmasız bırakarak yeni güvenlik tehditleri yaratmakta ve bu sebeple tek bir aktöre yönelik güvenlik anlayışı yetersiz kalmaktadır. Tüm aktörlerin kendi koşullarından kaynaklanan güçlü ve zayıf noktaları bulunsa da sistemin istikrarını sağlayacak kapsamlı bir güvenlik yaklaşımı oluşturmak mümkündür. Örnek olarak, kapsamlı bir devlet güvenliği sağlamak devletin kurumlarını, işbirliği gerçekleştirdiği özel kurumları, altyapı sistemlerini ve tüm vatandaşların güvenliğini sağlamak anlamına gelmektedir. Zira, herhangi bir altyapı sistemine, bireye veya kurumlara gelecek saldırı tüm sistemi etkilemektedir. Özellikle kritik altyapı sistemlerinin korunması kamu-özel sektör ortak çalışmasını gerektirmektedir. Çünkü, günümüzde serbest piyasa ekonomisinin hakim olduğu birçok ülkede enerji ve internet hizmetlerinin sağlanması ve geliştirilmesi özel kurumlar tarafından gerçekleştirilmektedir. Bu kritik altyapı sistemlerine gerçekleştirilecek bir siber saldırı tüm devleti savunmasız bırakacak etkilere yol açabilmektedir (Carr, 2016: 54). Bu kapsamda, alanında uzman bireylerin yetiştirilmesi ve istihdam edilmesi, muhtemel tehditlerin belirlenmesi ve önlenmesi hususunda hem devletlerin hem de özel kurumların siber güvenlik algısını sağlamlaştıracaktır (Shackelford, 2013: 1280-1281). Buna ek olarak, siber güvenlik için oluşturulacak küresel bir kültür olası çatışma ortamlarının oluşmasını engelleyerek yapıcı bir çerçeve oluşmasına imkan tanıyacaktır (Shackelford, 2020: 178).

Hak ve özgürlüklere yönelik söz konusu yaklaşım bireyin devletten uzaklaşmasına ve hatta siber alanın sağladığı imkânlar doğrultusunda terör ve suç örgütleri tarafından kullanılmasına yol açmaktadır. Hâlbuki bütüncül ve birleştirici politikalar doğrultusunda bireyler ile kurulan ilişkiler güçlendirilebilmekte ve kamu yararına katkıda bulunan bireyler üretken bir hayat sürebilmektedir (Betz ve Stevens, 2011: 64). Bu bağlamda, bireylere ve kurumlara yönelik tehditler devleti de dolaylı olarak tehdit etmekte ve ortak bir güvenlik anlayışı çerçevesinde tedbirler alınmasını gerekmektedir. Aksi halde, kapsamlı bir güvenlikten bahsedilmesi mümkün olmayacaktır. Bu doğrultuda, kamu-özel sektör işbirlikleri yüksek oranda sanayileşmiş ülkelerde yaygın bir yönetişim aracı olarak

kullanılmakta ve son yıllarda kollektif güvenlik çalışmaları kapsamında devletlerarası ortak eylem planları oluşturulmaktadır.

2. BÖLÜM: SİBER GÜVENLİĞİN ARTAN ÖNEMİ KAPSAMINDA SİBER GÜVENLİK POLİTİKALARININ İNŞASI

İletişim ve bilişim sektörlerindeki gelişmeler siber alanın yaratılmasına vesile olmuştur. Aynı kara, deniz, hava ve uzay operasyonel alanlarına benzer şekilde, siber alanda etkili olan aktörler amaçlarını gerçekleştirmek için çeşitlenen unsurlar üzerinden güç elde etmeye çalışmaktadırlar. Ayrıca diğer etkinlik alanlarındaki aktörlerin varlığı fiziki saldırılar ile son bulabilirken siber alandaki siber unsurlar üzerinden varlık kolaylıkla yeniden yaratılabilmektedir. Diğer operasyonel alanlarda mevcut olan askeri birimlerin yok edilmesi mümkün olmakla beraber yerlerine yenilerini yerleştirmek ekstra zaman ve maliyet gerektirmektedir. Örnek olarak, dünyanın yörüngesine çeşitli maksatlar ile yerleştirilen uydular farklı sebeplerden dolayı arızalanabilmekte ve yeni bir uydunun eskisinin yerini alması büyük bir bütçe ve uzun bir süreç gerektirmektedir (Betz ve Stevens, 2011: 35).

Günümüz teknolojileri kapsamında güvenlik, devlet düzeyinden birey düzeyine varacak şekilde derinleşmiştir. Modern dünyada tehdit unsurlarının tek başına diğer devletlerin politikalarından oluşmadığı da göz önüne alındığında ortaya çıkan asimetrik tehdit unsurları, güvenlik anlayışın çeşitlendirilmesi ihtiyacını göstermektedir. Devletler, uluslararası örgütler, özel şirketler, sivil toplum kuruluşları, terör ve organize suç örgütleri ve gerekli teçhizata sahip olan her birey siber alanda amaçları doğrultusunda var olabilmektedir.

2.1 Siber Güvenlik Kavramının Gelişimi

Bilişim teknolojilerinde yaşanan gelişmelerin hayatın her alanını etkilemesi nedeniyle içinde bulunduğumuz dönem ‘Dijital Çağ’ olarak adlandırılmaktadır. Sanal bir operasyonel etkinlik alanı olan siber alan yapısı gereği aktörlerin sahip oldukları politika araçlarını çeşitlendirirken, aynı zamanda da öngörülemeyen tehdit unsurları yaratmaktadır. Kritik altyapı sistemlerinin siber alana olan bağımlılıklarının yaratmış olduğu hassasiyetler, devletlerin siber güvenlik yaklaşımlarını planlarken çok boyutlu ve kapsayıcı politikalar şekillendirmelerini gerektirmektedir. Zira siber alan üzerinden gerçekleştirilmekte olan geleneksel güvenlik stratejilerine eklenerek yürütülen politikaların geleneksel etki boyutlarından kat be kat yüksek etki yaratabilmesi, siber tehditler ve fırsatlar ekseninde siber güvenlik politikalarının şekillendirilmesinin gerekliliğini ortaya koymaktadır.

2.1.1 Siber Uzay

Siber uzay internet erişimine sahip olan herhangi bir aktörün kolaylıkla ve düşük maliyetlerle eylemde bulunmasına imkân sağlayan bir platform niteliği taşımaktadır. Bugünün uluslararası aktörleri, siber alanı kullanarak amaçlarını

gerçekleştirmeye çalışmaktadırlar. Siber alanın kesintisiz bir sanal ortam olarak sürdürülebilmesi için ilk gerçekleştirilen süreçler fiziksel altyapıların inşa edilmesi ve korunaklı hale getirilmesidir. Ardından altyapı sistemlerinin idare edilmesi ve kullanılacakları alanlarda yardımcı olacak yazılımlar ile donatılmaları gerekmektedir. Donanım ve yazılım süreçleri tamamlandığında ortaya çıkan mevcut sistemlerin her iki yönden de analiz edilmesi ve kırılganlıklarının belirlenmesi gerekmektedir. Zira donanımların veya yazılımların zarar görmesi tehdit unsurlarının ortaya çıkmasına yol açmaktadır. Donanımlar yazılımların işleyebilmesine, yazılımlarda siber alana bilginin depolanabilmesini, aktarılabilmesini ve aktörün amacına yönelik olarak kullanılabilmesini sağlamaktadır. Siber alan yapısı gereği farklı türden aktörleri içerebilme potansiyeline sahiptir ve aktörlerin amaçları doğrultusunda çeşitli operasyonlar yürütmek için kullanılabilmektedir. Devlet perspektifinden bakılacak olursa, siber alan üzerinden gerçekleştirilen operasyonların istihbarat toplanılması ve ekonomik faaliyet kapasitesinin arttırılması amacıyla kullanılabildiği gibi, konvansiyonel yöntemler ile desteklenebilmekte ve hibrit saldırılar gerçekleştirilmektedir. Bu sayede saldırıların yıkıcılık potansiyeli arttırılabilmektedir. Diğer taraftan, terörist örgütler toplumda panik ve korku yaratmak amacıyla bir bomba kullanmak yerine siber saldırı yöntemlerini tercih edebilmekte ve bu sayede yerel veya bölgesel değil, küresel bir yankı uyandırabilmektedirler (Hensen ve Nissenbaum, 2009: 1159). Çeşitlenen aktör sayısı risk unsurlarının öngörülemez biçimde tehditlere dönüşmesine sebebiyet vermekte ve siber güvenlik politikalarının uygulanma süreçlerinin günden güne yenilenmesi ve iyileştirilmesi ihtiyacını doğurmaktadır (Choucri ve Clark, 2012: 2-3).

Choucri ve Clark'a göre siber uzay dört katmandan oluşmaktadır:

1. Fiziksel altyapılar (fiber-optik kablolar, bilgisayar donanımları, baz istasyonları, sunucular vb.),

2. Yazılım katmanı, altyapıların yönetiminde kullanılan ve altyapıları birbirine bağlayan yazılım programları (internet protokolleri, www (world wide web), tarayıcılar, internet siteleri, donanımların kullanımını sağlayan tüm yazılımlar),

3. İçerik/Bilgi katmanı, donanımlar tarafından depolanan ve yazılımlar aracılığıyla aktarılan kritik bilgiler (siber alanda depolanan, aktarılan ve dönüştürülen tüm kodlanmış metinler, fotoğraflar, videolar ve diğer materyaller),

4. Kullanıcı katmanı (birey veya kurum), sistemleri kontrol eden, sistemler aracılığıyla iletişim kuran, çalışan veya sistemlere bağlı bir operasyon yürüten bireyleri ve kurumları içermektedir.

İlk iki teknik katman sistem güvenliğinin sağlanması için kritik rol oynamaktadır. Gelişen teknoloji doğrultusunda düzenli yatırımlar gerektirmekte, içerik ve kullanıcı katmanlarının güvenliğini tesis etmektedir. Ancak ilk iki katmanın güvenliği sağlansa dahi, dördüncü katmanda yer alan kullanıcıların yeterli farkındalığa sahip olmamaları

durumunda ortaya çıkabilecek olan ihmalkâr davranışlar, kritik bilgilerin sızmasına sebep olabilmektedir.

Tablo 2. Siber Alanda Aktörlerin Göreli Güç Kaynakları

A. Devletler
1. Altyapı gelişimi ve desteği, eğitim, fikri haklar.
2. Bireylere ve aracı kurumlara ülkenin sınırları içerisinde yasal ve fiziki baskı.
3. Pazarın boyutu ve erişim kontrolü; örnek olarak AB, Çin, ABD
4. Siber saldırı ve savunma kaynakları: bürokrasi, bütçe, istihbarat teşkilatı
5. Kamu mallarının tedariği; örnek olarak ticaret için gerekli düzenlemeler
6. Meşruiyet için itibar, merhamet, yumuşak güç üretme kabiliyeti
Ana Kırılganlıklar: Kolayca kesintiye uğratılabilen karmaşık sistemlere yüksek bağımlılık, siyasi istikrar, itibar kaybı
B. Kurumlar ve yüksek yapılanmalı ağlar
1. Geniş bütçe ve insan kaynağı; ölçek ekonomisi
2. Ulusaşırı esneklik
3. Kod kontrolü ve ürün gelişimi, uygulama üretkenliği
4. Markalar ve itibar
Ana Kırılganlıklar: Yasal , fikri hakların çalınması, sistemin bozulması, itibar kaybı
C. Bireyler ve zayıf yapılanmalı ağlar
1. Giriş için düşük yatırım maliyeti
2. Sanal anonimlik ve çıkış kolaylığı
3. Devletler ve büyük örgütlere kıyasla asimetrik kırılganlık
Ana Kırılganlıklar: Yakalanılması durumunda devletler ve örgütler tarafından yasal ve yasal olmayan baskı

Kaynak: Nye Jr., J. S. (2010: 15). *Cyber Power.* Harvard Kennedy School. Cambridge, MA: Belfer Center for Science and International Affairs.

Tablo 2'de görüldüğü üzere aktörlerin siber alandaki güç ve kırılganlık kaynakları farklılık göstermektedir. Siber alanın sağladığı imkanlar doğrultusunda her aktör güçlü yanlarını mümkün olduğunca öne çıkarmaya ve kırılgan olduğu alanlarda tedbir almaya çabalamaktadır. Aktörlerin farklı avantajları ve dezavantajları göz önüne alındığında siber alanın mevcut operasyonların etkisini arttırmak veya kırılganlıkların giderilmesi amacıyla kullanılabileceği söylenebilmektedir. Aktörün teknik, mali ve insan kapasitesi genişledikçe siber alanın imkanları ve tehditleri de bu doğrultuda çeşitlenmektedir. Her ne kadar kapasite büyüklüğü önem arz etse de arrtırdığı kırılganlık da aynı şekilde paralellik göstermektedir. Tabloda farklı aktörlerin güç kaynakları ve kırılganlık ögeleri ayrı ayrı verilmiştir ve bu sayede aktörlerin siber alandaki avantajları ve dezavantajları açıkça görülebilmektedir. Siber alanda; devletler, uluslarası kurumlar, bireyler ve küçük ölçekli yapılanmalar arasında, hem aynı grup içerisindeki aktörlerin birbirleriyle etkileşimi hem de gruplar arası etkileşimler gerçekleşmektedir. Siber alan teknolojinin geldiği nokta itibariyle hem devletlerin hem de devlet dışı aktörlerin aktif olabileceği bir operasyonel alan olarak karşımıza çıkmaktadır. Siber güvenlik; kişisel çevrimiçi

güvenlik, kritik altyapı ve elektronik ticaret güvenliği, askeri tehditler ve bilgi güvenliğini kapsamaktadır (Carr, 2016: 49). Bunun yanında, siber alanda yer alan aktörler hedeflerine ulaşma yolunda bir taraftan yeni imkanlara sahip olurken diğer taraftan da yeni tehdit unsurlarıyla karşı karşıya kalmaktadırlar. Devletlerin ve diğer aktörlerin güvenlik anlayışları her alanda artan güvenlik artan kırılganlıkları doğrultusunda dönüşüm geçirmekte ve tehdit unsurlarının evrilmesine sebebiyet vermektedir. Örneğin, siber imkanlardan yararlanan terör örgütleri mesajlarını daha geniş kitlelere iletebilmekte ve eylemlerini dünya toplumu önünde sergileyerek çok daha geniş bir tabanda korku uyandırabilmektedirler.

Siber alan gelişimine paralel şekilde bir yandan içinde bulunan aktörlerin operasyonel yeteneklerini güçlendirmiş, diğer yandan da tehditlerin çeşitlenmesine sebebiyet vermiştir. Siber alanda devletler, uluslararası örgütler, terörist gruplar, aktivistler ve bireyler aktif bir şekilde yer almaktadırlar. Sürekli gelişen teknoloji ve bu teknolojinin sağladığı imkânlar devlet birey güvenliği arasında yeni bir güvenlik açmazı yaratmaktadır. Siber alana entegre devletlerin, gerekli ekipmana ve bilgi birikimine sahip bireyler tarafından gerçekleştirilebilecek saldırılara açık oldukları gibi, devletler tarafından tehdit olarak görülen bireyler de saldırı tehditleri karşısında daha kırılgan hale gelmişlerdir. Tehdit olgusunun belirsiz hale gelmesi, devletlerin konvansiyonel araçlar ile karşılık vermesini yetersiz kılmakta ve geleneksel güvenlik anlayışının sınırlılığını ortaya koymaktadır (Shaheen, 2014: 81-83). Bu sınırlılığı gidermek amacıyla daha geniş kapsamlı güvenlik politikalarına ihtiyaç duyulmaktadır.

Siber alanın beşinci operasyonel güvenlik alanı halini aldığı bir ortamda güvenliğin katılımcı bir yaklaşımla temin edilebileceği öngörülmektedir. Güvenliğin evrilen yapısı, devletin güvenlik sağlamadaki rolünün de sorgulanmasına neden olmaktadır. Temel sorumlulukları arasında bireylerin hak ve özgürlüklerinin korunması bulunan devlet aygıtlarının siber suçlarla mücadele kapsamında bireyin özel hayatını ihlal etmesi güvenlik-özgürlük ikilemini beraberinde getirmektedir. Bu güç unsurları fiziksel olabildiği gibi bireyin özel hayatının ihlal edilmesini de kapsamaktadır.

Yirminci yüzyılın sonuna yaklaşırken, siber alanda aktif bireylerin hem kamu hem de özel sektöre kişisel amaçları doğrultusunda katkı sağlamaları veya zarar vermeleri özellikle kişisel verilerin korunması alanını güvenliğin konusu haline getirmede önemli bir rol oynamıştır. Bireyin güvenlik tehdidi altında olması doğrudan veya dolaylı olarak çalıştığı devlet veya özel kurum için yeni bir güvenlik açığı meydana getirmektedir. Bilişim suçları doğaları gereği *sui generis*[9] bir niteliğe sahiptir. Örneği görülmemiş suçların yarattığı belirsizlik ortamı hem bireysel suçlarda hem de devlete karşı işlenen suçlarda verilecek cezaların muğlaklığına sebep olmaktadır (Walden, 2005: 52) Siber

[9] Sui generis: Latinceden kendine özgü, nevi şahsına münhasır vb. şeklinde dilimize çevrilmektedir. Başka bir örneği veya benzeri bulunmayan durumları ve nesneleri açıklamak için kullanılmaktadır (Cambridge University Press, 2020).

alan, sadece gerekli altyapıya ve yetişmiş personele sahip olan devletlere değil, yeterli bilgi birikimine sahip olan her kesimden bireye, topluluğa ve örgüte de bu alanda aktif olma imkanı tanımaktadır. Sahip olunan geniş manevra kabiliyeti, aktörün önündeki seçenekleri hiç olmadığı kadar genişletmekte ve bu opsiyonları sağlarken tamamen gizli kalabilme fırsatını da vermektedir.

Siber alanın geldiği nokta ve küresel güvenlik üzerindeki etkileri, güvenliğin karşılıklı bağımlılığının geldiği noktayı ve güvenlik kavramında yaşanan dönüşümü sergilemesi açısından önem arz etmektedir. Bireylerin devletleri ve şirketleri tehdit edebilecek asimetrik güç düzeyine kavuşmasına izin veren siber güç, güvenliğin günümüz itibariyle sahip olduğu öngörülemez ve karmaşık doğasında başlıca rollerden birini oynamaktadır (Greathouse, 2014: 30). Bu çerçevede güvenliğe yönelik en ciddi tehditlerin geldiği operasyonel alanlardan biri haline gelen siber uzay kapsamında bir siber yönetişimin geliştirilmesinin ve devletlerin kamu-özel sektör işbirliği ortaklığında stratejilerini yapılandırmasının önümüzdeki dönemin küresel güvenlik çevresinde önemli yer tutacağı ön görülmektedir.

2.1.2 İnternetin Gelişimi

Teknolojik gelişmeler uluslararası ilişkiler alanını etkileyen önemli unsurlardan biri olarak görülmektedir. Bilhassa iletişim ve bilişim alanında yaşanan gelişmeler güvenlik anlayışının yeniden şekillendirilmesinde etkili olmaktadır. Buna ek olarak, kıtalar arası haberleşmenin saniyelere, ulaşımın ise saatlere indirildiği günümüzde yaşanan teknolojik gelişmeler sonucunda devletler arasındaki mesafelerin önemini kaybetmeye başladığı görülmektedir. Esas olarak, internetin tüm dünyayı her anlamda birbirine bağlayarak iletişimde, bilgiye erişimde, ticari ürünlere, kişilere ulaşma anlamında mevcut kısıtlamaları ortadan kaldırması köklü dönüşümleri başlatmıştır. Nicholas Westcott internet gelişiminin uluslararası ilişkiler disiplini üzerinde üç temel değişikliğe sebep olduğunu belirtmektedir (Westcott, 2008: 2):

- Uluslararası politikaların geliştirilmesinde rol alan aktörlerin sayısının çoğalmasına ve seslerinin daha çok duyulmasına vesile olmaktadır. Bu sürecin uluslararası karar verme mekanizmalarının da çeşitlenmesine ve karmaşıklaşmasına yol açarak devlet tekelini giderek azaltacağı düşünülmektedir.

- Bilginin (doğru veya hatalı olmasından bağımsız olarak) yayılma hızını ve serbestliğini arttırarak herhangi bir konunun uluslararası etki yaratacak potansiyele erişmesine olanak tanımaktadır.

- Geleneksel diplomatik hizmetlerin daha hızlı ve daha az maliyetle gerçekleştirilmesini sağlamaktadır.

Klasik anlayışla askeri güvenlik üzerinden tanımlanan güvenlik anlayışı, siber alanın genişleyen yapısı kapsamında yeniden değerlendirilmekte ve bu anlamda kapsayıcı bir yaklaşıma ihtiyaç duyulmaktadır. Siber alanın sürekli olarak genişlemesi ve derinleşmesinin bir sonucu olarak, güvenliğin sağlanabilmesi için devletin yanı sıra, devlet dışı aktörleri de içine alan yaklaşımlar öne çıkmaya başlamıştır (Couchri, Madnick, ve Ferwerda, 2014: 104). Yirminci yüzyılın sonu, yirmi birinci yüzyılın başı itibariyle güvenlik kavramı sadece devlet merkezli olarak değil, buna ek olarak bireylerin refahı, ekonomik ve toplumsal güvenlik gibi parametreleri de içine alarak daha kapsamlı bir çalışma alanı haline gelmiştir. Bilhassa, internet teknolojisinin yaygınlaşması ve siber tehditlerin konvansiyonel tehditlere ek olarak yeni bir boyut meydana getirmesiyle güvenlik anlayışını olduğundan daha karmaşık bir yapıya evrilmesine sebep olmuştur. İnternet kaynaklı tehditler günden güne çeşitlenmekte ve yeni tedbirler gerektirmektedir (Chouchri ve Goldsmith, 2012: 72).

Teknoloji çeşitli düzeylerden aktörlerin amaçlarını gerçekleştirmesi için gerekli araçların temin edilmesini sağlamakta ve bu araçların hangi amaçlar için kullanılacağı aktörün takdirine kalmaktadır. İnternet kullanımının yaygınlaşmasıyla birlikte eskiden yakın çevre ile etkileşim içerisinde olan aktörler, artık dünyanın neresinde olurlarsa olsunlar ortak amaçları doğrultusunda bir araya gelebilmektedir. Bu durum bireylerin hiç olmadığı kadar özgürleşmesine ve benzer ilgi alanlarına sahip bireylerin çok daha kolay iletişim kurabilmelerini mümkün kılmaktadır. Bu unsurların neticesinde ulus devletlerin çizdiği sınırların aşılarak küresel değerlere sahip uluslararası toplumun güçlendiği görülmektedir. Diğer taraftan, Artan işbirliği imkânları karşısında ise, devletlerin ve bireylerin çeşitlenen ve öngörülemeyen tehditlerle karşı karşıya kaldığı durumlar ortaya çıkmaktadır. İnternet güvenliği bu kapsamda hayati bir rol oynamakta, internet güvenliğinin sağlanabilmesi için kapsamlı ve şebekeleşmiş bir ağ yapısı oluşturulması gerekmektedir. Güvenlik sisteminin donanımları, yazılımları ve sistem kullanıcılarını göz önünde bulunduran şekilde inşa edilmesi ve aynı zamanda toplumun internet güvenliği konusunda farkındalığının arttırılması gerekmektedir (Schmidt, 2014: 184). Bu çerçevede güvenlik yaklaşımlarının etkin olabilmesi için hiyerarşik olmayan, kapsayıcı yetkinin dağıtıldığı yaklaşımlar öne çıkmaktadır.

2.1.3 Siber Güvenliğin Tanımlanması

Siber güvenlik, bilgisayar programlarını, internete bağlı elektronik sistemleri ve ağ yapılanmalarını siber saldırılardan korumak amacıyla geliştirilen politikaların tümü olarak tanımlanmaktadır (Betz ve Stevens, 2011: 36). Her ne kadar siber güvenliğin tanımı, tanımlayan aktöre göre ofansif veya defansif yaklaşımlar içerebilse de, temel politika aktörün siber alanda güvende olmasını sağlamayı amaçlamaktadır.

Siber güvenlik, esas itibariyle aktörlerin amaçlarını gerçekleştirmek üzere donanım ve yazılımları sadece birer araç olarak kullanarak var oldukları operasyonel alanı güvenli hale getirme çabası olarak görülmektedir. Siber saldırıları savuşturmak veya maruz

kalınan saldırın etkilerinden ivedi bir şekilde onarmak amacıyla politikalar üretmek ve sahip olunan kritik altyapıları korumak ve geliştirmek amacıyla farklı yöntemler geliştirmektedir. Bu politikaların temel amacı yetkisiz mercilerin kritik bilgilere ulaşmasını engellemek ve mevcut sistemleri kendi çıkarları doğrultusunda manipüle etmelerinin önüne geçmektir. Buna ek olarak, mevcut sistemler üzerinde yapılan tüm bilgi alma, değişiklik yapma ve yönetim süreçlerinin yetkili mercilerin denetimi altında gerçekleştiğine emin olmaktır (Limba, Pleta, Agafonov, ve Damkus, 2017: 560). Farklı güvenlik anlayışına sahip devletler siber alanı ve siber güvenliği tanımlarken farklı perspektifler kullanmakta ve bu da tanımların devletlerin siber alanı kullanma amacına yönelik olarak çeşitlenmesine neden olmaktadır.

Siber alan devletlerin ulusal güvenlik stratejilerinde gittikçe önem kazanan bir yer edinmeye başlamıştır. Macaristan Milli Güvenlik Stratejisi'ne göre; siber alan küresel olarak birbirine bağlı, toplumsal ve ekonomik süreçlerin içine dâhil olduğu ve aynı zamanda yönetildiği, merkezi bulunmayan, günden güne büyüyen elektronik bilgi sistemlerinin tümüne işaret etmektedir. İspanya Milli Siber Güvenlik Stratejisi tanımı bir adım daha ileriye taşıyarak sınırların belirsizleştiği ve yeni tehditlerin ve yansımalarının ortaya çıktığı operasyonel bir alan olduğunun altını çizmiştir (Küçüksolak, 2018: 27). 2011-2015 yılları arasında 20. Genelkurmay başkanı olarak İsrail Savunma Kuvvetleri'nde görev yapmış olan Benjamin Gantz'a göre siber alan daha saldırgan bir şekilde; geleneksel yaklaşımlar ile yönetilemeyecek kadar karmaşık bir yapı olarak tanımlanmıştır. Buna ek olarak; siber alanın coğrafi, siyasi, ekonomik, askeri, sosyal sınırları veya karakteristikleri bulunmayan barışçıl bir ortam olmaktan son derece uzak bir operasyonel alan olduğu belirtilmiştir (Libel, 2016: 151). Yeni Zelanda Milli Siber Güvenlik Stratejisi'ne göre ise; siber alan içinde her türlü bilgi ve veri aktarımının gerçekleştirildiği, özel sektör, devletler, bireyler gibi birden çok aktörün aktif bir şekilde iletişim, alışveriş, bilgi depolama ve ticaret faaliyetlerini yürüttüğü sanal gerçeklik olarak tanımlanmaktadır (New Zealand Foreign Affairs ve Trade, 2020). Bu tanıma ek olarak, internet ortamındaki elektronik sistemlerin terör örgütleri veya aktivistler tarafından ele geçirilmesinin, siber saldırıların gerçekleştirilmesinin ve siber suç, siber casusluk gibi vakaların mevcudiyetinin bilhassa küçük devletler için daha fazla tehdit oluşturduğunu ve ancak ortak işbirliği metotları ile siber güvenliğin sağlanabileceğini ileri sürmektedir (Burton, 2013: 228).

Siber alandaki güvenlik önlemleri siber saldırıları önlemek için sistemin kapsamlı, proaktif ve etkin kullanılmasını gerektirmektedir. Saldırılar yerel, bölgesel veya küresel aktörler tarafından gerçekleştirilebilmekte ve failleri saptamak veya saptanan failleri cezalandırmak genellikle zorlu bir sürece işaret etmektedir. Devletlere karşı gerçekleştirilen siber saldırılar zayıflatma, savunmasız bırakma hatta altyapılara ve dolayısıyla ülke eknomomisine zarar verme amacıyla yapılmakta ve kökeni bilinmeyen (devlet destekli iddialarına rağmen kanıtlanmamış) bu saldırılar hem kamu hem de özel

sektör için büyük tehdit oluşturmaktadır. Bu çerçevede yapısal kırılganlıkların giderilmesini ve olası tehditlere karşı kamu-özel sektör işbirliğini de içeren kapsamlı tedbirlerin alınmasının büyük oranda fayda sağlayabileceği düşünülmektedir. Devlet, özel sektör ve bireylerin siber saldırılar tarafından doğrudan veya dolaylı şekilde tehdit altında olması sebebiyle, siber güvenlik altyapılarının oluşumu, gelişimi ve korunması aşamalarında ortaya konan en etkili seçenek kamu ve özel sektörün ortak işbirliklerini teşvik etmek ve var olanları güçlendirmektir (Shackelford, 2013: 1278-1281). Siber güvenlik protokollerinin hazırlanmasında öncelikle faillerin işlediği suçun boyutu, yarattığı tehdidin unsurları ve caydırıcılık politikaları ele alınmaktadır.

2.2 Siber Güvenliğin Unsurları ve Artan Önemi

Siber alanın gerektirdiği maliyetlerin askeri operasyonlara kıyasla daha ucuz olması ve fiziki anlamda insan gücüne daha az ihtiyaç duyulması sebebiyle aktör çeşitliliği son derece fazla olabilmekte ve her aktör gerekli bilgi ve teçhizata sahip olması durumunda diğer bir aktöre zarar verebilmektedir (Sheldon, 2011: 97). Buna ek olarak, siber güvenlik yaklaşımlarında defansif politikalardan ziyade agresif politikaların izlenmesinin kolaylığı[10] önemli isimlerce ortaya koyulmaktadır. Siber alanda saldırgan pozisyonda olmanın savunan tarafa kıyasla daha kolay olmasının temel sebepleri arasında büyük yatırımlar gerektirmemesi bulunmaktadır. Siber alanda stratejik bir etki yaratmak isteyen aktörün milyarlarca dolarlık yatırıma, binlerce kişiden oluşan insan gücüne veya dönümlerce alana ihtiyacı olmamaktadır. Gerekli bilgi, beceri, motivasyon ve teçhizata sahip olan tüm aktörler motivasyonları doğrultusunda farklı düzeylerde operasyon gerçekleştirebilmektedirler. Ayrıca, siber alanda aktif olmak isteyen bireylerin üstün becerilere sahip olması günümüz imkanları kapsamında zorunlu olmaktan ziyade önemli bir avantaj anlamına gelmekte, zira herhangi bir mağazadan uygun fiyatla alınabilen donanım ve bilgisayara indirilebilen yazılım yeterlilik sağlamaktadır (Korns, 2009: 97-98). Buna ek olarak, siber güvenlik sistemleri yeterli çaba doğrultusunda aşılabilen güvenlik duvarları ve tehdit saptayıcı sistemlerden meydana gelmektedir. Diğer yandan, tehditi önlemek, ortadan kaldırmak veya kırılganlığı o an gidermek sistemin gerçekleştirebileceği görevler arasında bulunmamaktadır (Clarke ve Knarke, 2010: 14).

Savunmaya yönelik yaklaşımlar tehdit belirlenmesi aşamasında çözüm üretebilmekte ve güvenliğin sağlanabilmesi tehditin ortadan kaldırılmasını zorunlu kılmaktadır. Ancak bu durumda yeni tehdit unsurlarının ortaya çıkmasını tam olarak engelleyememektedir. Siber saldırılar konvansiyonel saldırılara kıyasla oldukça hızlı gerçekleşmektedir. Bu sebeple, savunma mekanizmalarının her saldırıyı savuşturması gerekliyken, saldıran aktörün yalnızca tek bir seferde başarılı olması yeterli olabilmektedir (Sheldon, 2011: 98).

[10] John B. Sheldon 2011 yılında yayınladığı 'Deciphering Cyber Power makalesinde' siber alanda saldırının savunmadan çok daha az teknik bilgi, beceri ve personel gerektirdiğini ve bu sebeple daha fazla kullanıldığını ve savunmaya yönelik siber güvenlik politikalarının zaman kaybı olduğunu belirtmektedir.

Teknolojiyle entegre olan toplumların üretken ve sürdürülebilir bir yaşama sahip olabilmeleri için altyapılar kritik önem arz etmektedir. Bilgi teknolojilerinin gelişimiyle birbirine bağlı sistemler devletin, özel kurumların ve bireylerin hayatlarını etkin bir biçimde sürdürebilmeleri için önem teşkil etmektedir (Haimes ve Longstaff, 2002: 442).

2.2.1 Siber Suç

Siber alanda işlenen suçlar, özellikle de siber uzayın açıklarından yararlanılması yoluyla mümkün olmaktadır. Siber alan yapısı gereği siber suçlara geniş bir hareket alanı tanımaktadır. Bu hareket alanı kötü niyetli bireylerin yanı sıra suç ve terör örgütleri tarafından da etraflıca kullanılmaktadır. Ian Walden'ın yaptığı kategorizasyona göre, siber suçlar üç kategori altında incelenmektedir. İlk kategoride bilgisayarların yalnızca suç işlemek için araç olarak kullanıldığı durumlar yer almakta; internet üzerinden dolandırıcılık veya hırsızlık suçları bu kategoriye girmektedir. Örnek olarak kredi kartı dolandırıcılıkları, elektronik posta yoluyla kişisel güvenlik bilgilerinin deşifre edilmesi verilebilmekte, diğer bir deyişle geleneksel suçların bilgisayar tabanlı ortama taşınmış hali olarak gösterilmektedir. İkinci kategori altında içerik tabanlı suçlar, yani telif hakkı ihlalleri veya kanun dışı içeriklerin paylaşımı ve dağıtımı tabanlı bir kategorizasyon yapılmaktadır. İnternette bulunan eserlerin yazarların izni olmadan kopyalanması ve emek hırsızlıkları örnek olarak verilebilmektedir. Ayrıca uyuşturucu madde satışı ve pornografi paylaşımları gibi dağıtımı yasak olan materyaller ile saldırı aracı olarak kullanılabilecek ve fiziksel, bilişsel zarara sebep olabilecek unsurlar bu kategori altında incelenmektedir. Üçüncü kategoride ise, internete bağlı sistemlerin ve bilgisayarların donanımına, kullanımına ve gizliliğine zarar verme amacı taşıyan, bilgisayar korsanlığını ve virüs gönderimini içeren suçlar incelenmektedir (Walden, 2003: 295).

Siber alan bireylere ve suç örgütlerine daha önce eşi görülmemiş bir hareket alanı tanımaktadır. Özellikle bilgisayar korsanlarının küresel erişim ve anonimlik imkanları sayesinde özel kurumlar milyarlarca dolarlık zarara uğratılabilmekte, tıbbi sistemler sekteye uğratılarak can kayıplarına yol açılabilmekte, devletlerin altyapı sistemleri hedef alınarak tehditlere açık hale getirilebilmektedir. Siber saldırılar başlığı altında incelenen bu son kategoride devletlerin altyapı sistemlerine zarar verilmesi veya kritik planlarının üçüncü kişilerle paylaşılması, kurumların müşteri portfolyolarının sızdırılması, doğrudan veya dolaylı yönden finansal zarara uğratılmaları ve bireylerin kişisel verilerinin kopyalanması hem devlet hem de birey seviyesinde ciddi tehditler yaratmaktadır. Bu durum da güvenliğin siber alandaki kapsamlı dönüşümünü ve aktör düzeyinde ne derece etraflı olabileceğini ve hatta bireylerin sahip oldukları asimetrik güç unsuru ile devletleri hedef alabilecekleri kapasiteye ulaşabileceklerini göstermektedir.

2010 yılında İran'ın Natanz şehrinde bulunan uranyum zenginleştirme tesislerine yönelik bir siber saldırı kayıtlara geçmiştir. Stuxnet adı verilen virüs, o tarihe kadar geliştirilen en sofistike zararlı program olarak tanımlanmıştır. Saldırıdan sonra dünyanın çeşitli

lokasyonlarında virüse rastlanmış ancak virüsün zarar vermeyi amaçladığı programın yüklü olmadığı sistemler hiçbir zarar görmeden işlemeye devam etmiştir (Brown, 2011: 70). Saldırıdan fiziksel olarak etkilenen kimse bulunmazken, binden fazla santrifüj zarar görmüş ve Stuxnet virüsü atom bombasının siber karşılığı olarak kabul edilmiştir. Her ne kadar bu virüsün İran'a zarar vermek adına İsrail-ABD ortaklığında yürütülen Olimpik Oyunlar kod adlı projenin bir ürünü olduğu iddia edilse de kanıtlanamamıştır (Lindsay, 2013: 365). Choucri ve Goldsmith'in virüsün yaratıcısı olmakla suçladığı ABD ve İsrail'in sorumlulukları tartışmalıdır (Choucri ve Goldsmith, 2012: 73).

İran'ın nükleer yatırımlarına büyük ölçüde zarar veren ve bir yıla yakın bir sürede tesisin verimli kullanılmasına engel olan Stuxnet virüsünün kodu benzer bir saldırının yıkıcılık potansiyelini önlemek amacıyla internette paylaşılmış ve gerekli önlemlerin alınması sağlanmıştır. Stuxnet veya benzeri bir bilgisayar virüsünün nükleer bir tesiste facia yaratma potansiyeli olan bir unsur olduğuna kanaat getirilmiştir. Hatta Çernobil'deki nükleer santral felaketinden çok daha büyük hasarlar verebileceği belirtilmiştir. Bu denli zarara yol açabilecek bilgisayar programlarının varlığı, siber alana entegre devletlerin özellikle enerji altyapılarındaki kırılganlıklar üzerinde ciddi güvenlik tedbirleri almalarına neden olmuştur (Lindsay, 2013: 366).

2.2.2 Siber Tehdit

Güvenlik anlayışı aktörlerin içinde bulundukları dönemde karşılaştıkları risk, tehdit ve imkânlar aracılığıyla şekillenmekte ve güvenlik politikaları sahip olunan kapasite ve politik amaçlar doğrultusunda uygulanmaktadır. Tehdit algısının oluşumunda aktörün sahip olduğu değerler, dünya görüşü, güvenlik ortamının dinamikleri, kapasitesi ve kırılgan noktaları belirleyici rol oynamaktadır. Siber güvenlik politikaları belirlenirken öncelikle mevcut risk ve tehditlerin saptanması gerekmektedir. Mevcut riskler aktörün kırılganlıkları sebebiyle maruz kalabileceği potansiyel siyasi, ekonomik, toplumsal veya fiziki zarara işaret ederken, tehditler diğer aktörler tarafından uygulanabilecek politikalar olarak tanımlanmaktadır. Ahmet Küçükşahin'in de belirttiği üzere risk bir olasılıktır, tehdit ise yönetimin sahip olduğu yetenek ve kabiliyet doğrultusundaki yönetim sonucunda ortaya çıkmaktadır. Siber güvenlik politikalarının belirlenme aşamasında risk analizleri ne kadar tutarlı yapılırsa, karşılaşılma ihtimali olan tehditler de aynı oranda azaltılmış olacaktır (Küçükşahin, 2006: 18). Günümüzde bilgi teknolojilerinin geliştirilmesinde gelinmiş olan aşama nedeniyle karşılaşılan risk ve tehditler büyük ölçüde çeşitlenmiştir. Scott Charney altı maddelik bir liste ile bu alana politika oluşturma zorluğunun sebeplerini açıklamaktadır (Charney, 2009):

- Kötü niyetli aktörlerin çeşitliliği (bireyler, organize suç örgütleri, özel kurumlar, devletler),

- Aktörlerin amaç çeşitliliği (kişisel zenginleşme, casusluk, bir devletin altyapı sistemlerine zarar verme),

- Saldırı çeşitliliği sağlayan teknik imkânların fazlalığı ve anonimlik problemi,
- Tehdidin gerçekliğinin fark edilmesinin uzun sürmesi,
- Tehdidin sonuçlarının öngörülememesi,
- Siber alandaki aktivitenin taşıdığı yıkıcı potansiyelin korkutucu ve iç karartıcı yapısı

Siber alanı kullanan her aktör bireyler, toplumlar, kurumlar ve devletler üzerinde yıkıcı bir etkiye sahip olabilmekte ancak siber alanın karmaşık yapısı gereği savunma söz konusu olduğunda tehditleri zamanında algılamak ve çözüm üretmek oldukça güç olmaktadır (Kremer, 2014: 221-226). Charney'nin yukarıdaki maddelerde belirttiği üzere tehdidin kaynağının belirsizliği, çeşitliliğinin fazlalığı ve yapısının karmaşıklığı sebebiyle defansif siber güvenlik politikaları oldukça çetrefilli bir süreç gerektirmektedir. Tehdit senaryolarının kompleks ve kapsamlı oluşu aktör hedefli yaklaşımların yerine bütüncül tedbirlerin alınmasını zorunlu kılmaktadır.

Fiziksel ve/veya bilişsel hasar vermek amacıyla hedeflere gerçekleştirilen siber saldırılar sivil halkın ve özel kurumların faydalandığı kritik altyapı hizmetlerini, enerji santrallerini, ulaşım araçlarını, hatta ülkelerin ekonomik sistemlerini bir siber anlamda bir nevi halı bombardımanına[11] tutabilmektedir. 2007 yılındaki Estonya saldırıları ve 2010 yılında İran'a yapılan Stuxnet saldırısı tehditleri açıkça ortaya koymuştur. Söz konusu siber saldırılarda, her ne kadar can kaybı, yaralanma veya bir yapısal hasar görülmemiş olsa da devletlerin altyapılarına verilen zarar ile birlikte siyasi ve ekonomik boyuttaki kayıplar yüksek olmuştur (Kremer, 2014: 229-231).

2.2.3 Siber Caydırıcılık

Siber suçları ve siber tehditleri önlemenin en etkili yöntemi şüphesiz ki yüksek bir caydırıcılık mekanizmasına sahip olmaktır. Her ne kadar siber caydırıcılık politikalarının etkili olmadığı yönünde hakim bir görüş bulunsa da kavram doğru şekilde idrak edildiğinde siber güvenlik politikaları siber caydırıcılığa sahip olabilmektedir (Burton, 2018: 4). Siber alanda caydırıcılığın temel amacı, saldırı potansiyelinde olan aktörleri daha saldırmadan engellemek için politikalar oluşturmaktır. Saldırgan aktörün saldırısını gerçekleşmesi durumunda karşı karşıya kalacağı tehdit unsurları, saldırgan aktörü saldırıdan caydırabilmekte ve farklı kanallardan çözüm arayışı içerisine girmesine vesile olabilmektedir. Caydırıcılık tek bir aktöre yönelik olmamakta, farklı aktörlerin benzer girişimlerde bulunması ihtimallerinin önüne geçmeyi amaçlamaktadır. Diğer bir deyişle farklı aktörlere karşı farklı caydırıcılık politikaları izlenmesi gerekmektedir. Örnek olarak, Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNODC) verilerine göre Çin,

[11] Özellikle Birinci ve İkinci Dünya Savaşları'nda kullanılan hedefleri tahrip etmeye yönelik kapsamlı ve sistematik bombalama şekline verilen addır (Encyclopedia Mypedia (2013), Mimir Türk Ansiklopedisi/HukukveDevlet/Askeri https://mimirbook.com/tr/e1dd4f94d9f).

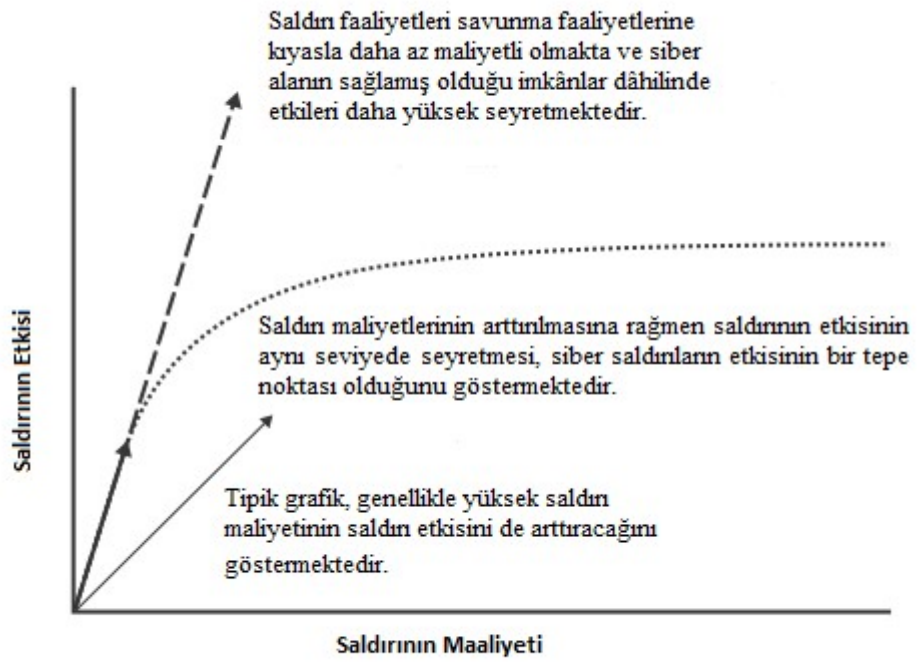
Almanya ve Japonya siber alan üzerinden işlenen suçlar için siber suçlara özgü kanunlar yaparken, kimi devletler siber suçlara yönelik olarak mevcut ceza kanunlarını hem siber hem de geleneksel yöntemler aracılığıyla işlenen suçları kapsayacak şekilde genişletmiştir. Bu sayede siber suç işleyen bireyler aynı anda iki farklı suç işlemek ile yargılanabilmekte ve caydırıcılık bu yöntemle arttırılabilmektedir (UNODC, 2019). Örnek olarak dolandırıcılık, sahtecilik, organize suç tanımlamalarında 'geleneksel ve hibrit yöntemler aracılığıyla işlenen suçlar kapsamında' ibaresi eklenerek gerçekleştirilebilmektedir. Siber suçlar kapsamında incelendiğinde, işlenen siber suçlara verilecek cezaların geleneksel cezalara kıyasla daha caydırıcı olmasının, siber suç oranlarının azaltılmasında büyük rol oynayacağı öngörülmektedir.

Caydırıcılık, güvenlik literatürüne misilleme ve esirgeme olarak iki farklı türde geçmiştir (Güntay, 2017: 91). Bu faaliyetlerin gerçekleştirilebilmesi için aktörün maruz kaldığı saldırının kimin tarafından ve ne amaçla gerçekleştirildiğinin tespit edilmesi gerekmektedir. Misilleme, saldırıların gerçekleşmesinden sonra kaynağının tespit edilmesi ve uygun aksiyonun alınması yoluyla yapılmaktadır. Ancak askeri ve siber teknolojilerin sağladığı imkânlar çerçevesinde eşit aktörler arasında karşılıklı imha durumuna yol açabileceği düşünülmektedir. Esirgeme ise, saldırıyı gerçekleştiren aktörün sahip olduğu askeri, siyasi veya ekonomik risklerin, tehditlere dönüşeceğini açıkça ifade etmek olarak tanımlanmaktadır (Davis, 2014: 6). Bu sebeple, siber saldırı uygulama potansiyeli olan aktörler esirgeme ve misilleme tehditleri ile karşı karşıya kalma ihtimallerinin yüksek olduğu durumlarda saldırı gerçekleştirmek hususunda tereddüde kapılmaktadır. Ancak siber alanda mevcut olan anonimlik, bu faaliyetlerin uygulanmasını oldukça zorlaştırmaktadır.

Üzerinde mutabık kalınmış ortak bir yaklaşım bulunmamakla birlikte klasik anlamda caydırıcılık üzerine politikalar oluşturulurken sekiz maddelik bir liste göz önünde bulundurulmaktadır. Bu unsurlar; çıkar, caydırıcı deklarasyon, inkâr yöntemleri, ceza yöntemleri, inandırıcılık, güvence, korku ve kâr-zarar hesaplaması olarak belirlenen bu elementler caydırıcılık politikalarının bel kemiğini oluşturmaktadır. Siber caydırıcılık da yine aynı elementleri dikkate alarak muhtemel kazanç ve kayıpların doğru analiz edilerek bir politika oluşturulması ile gerçekleştirilmektedir (Goodman, 2010: 108). Örnek olarak, dayanıklı ve çok katmanlı güvenlik duvarları, aktif ve pasif savunma yazılımları ve uzman personelleri tarafından korunan aktörlere karşı gerçekleştirilen siber saldırılar maliyet açısından yüksek olmaktadır. Ayrıca, nitelikli ve karmaşık hazırlanmış güvenlik politikaları saldırganların saldırı maliyetlerini arttırırken aynı zamanda tespit edilme ve açığa çıkma risklerini de beraberinde getirmektedir. Diğer yandan, tehditler hususunda caydırıcılık kaynağının asimetrik veya simetrik olması sonucu ortaya çıkan durumlar oldukça değişkenlik göstermektedir (Libicki, 2009: 28-31). Bu minvalde, ulusal ve uluslararası siber caydırıcılık politikalarının yürütülmesinde kullanılabilecek en etkili yöntem siber yönetişim araçları olarak görülmektedir. Bilhassa yetki dağıtımı ve ortak işbirliği içerisinde yürütülen çalışmalar sayesinde daha kapsayıcı bir güvenlik yaklaşımı

sunabilmektedirler. Devletlerarası işbirliği çalışmaları, çıkar çatışmaları sebebiyle belli bir düzeyi aşamamakta ve küresel güvenliğe katkıda bulunma konusunda yetersiz kalmaktadır. Siber alanda mevcut aktörlerin sadece devletler olmaması daha kollektif ve çok yönlü bir güvenlik anlayışının geliştirilmesi ihtiyacını doğurmaktadır. Siber güvenlik politikaları oluşturmak oldukça kapsamlı bir çalışma gerektirmekte ve siber alana erişimi olan büyük veya küçük ölçekli hiç bir aktörün dışarıda bırakılmaması önem taşımaktadır (Choucri ve Goldsmith, 2012: 72).

Şekil 1. Siber Saldırı Maliyeti ve Siber Saldırı Etkisi Arasındaki İlişki



Kaynak: Libicki, M. C. (2009: 33). *Cyberdeterrence and Cyber War.* Santa Monica, California: Rand Corporation.

Şekil 1'de en solda yükselen ok, az bütçe ile büyük etkiye sahip saldırıların gerçekleştirilmesinin mümkün olduğunu göstermektedir. Bu ilişki çoğunlukla asimetrik aktörler arasındaki siber etkileşim sonucu ortaya çıkmaktadır. Ortada kıvrım yapan figür ise, saldırıların sayısının ve maliyetinin artmasıyla, etkisinin belli bir süre sonra saldırıların etkisinin yükselişinin sonlanacağını göstermektedir. Bu durum genellikle simetrik aktörler arasındaki etkileşim sonucunda ortaya çıkmaktadır. Siber saldırıların maliyetleri yükseldikçe saldırı şiddetinin belli bir noktadan sonra artmayacağı gösterilmektedir (Libicki, 2009: 34)

Siber caydırıcılık politikaları amaçlarına ulaşmaları halinde savunma maliyetlerini düşürebilmektedir. Elektronik sistemlerin kırılganlıklarının azaltılması ve güncel

tutulması yüksek bir maliyet getirmektedir. Ancak, caydırıcılık politikaları devreye sokulduğunda, saldırgan aktörlerin saldırı maliyetleri de benzer şekilde artmakta ve saldıran aktörün kırılganlıkları caydırıcılık seviyesine ulaşmaktadır. Modern devletlerin işleyişinin bozulmaması için kritik altyapı sistemleri hayati önem taşımaktadır. Bu sistemlerin sahip olduğu kırılganlıkları hedef alan saldırılar siber güvenlik politikalarına verilen önemin artmasını ve savunma stratejilerinin geliştirilmesini sağlamaktadır (Stevens, 2012: 148).

2.3 Siber Güvenlik Politikalarının Uygulanma Biçimleri ve Araçları

Siber güvenlik sağlamada ilk adım kritik altyapı sistemlerini oluşturmak, geliştirmek ve korumak olmakla beraber bu süreç devlet bütçesinden oldukça yüksek yatırımlar gerektirmekte ve bu sebeple yavaş ilerlemektedir. Ayrıca, henüz saldırıya uğramayan sistemlerin kırılganlıkları tam olarak anlaşılamamakta ve emsal sistemler saldırıya uğradıkça bu kırılganlıklar giderilebilmektedir. Diğer yandan, altyapı sistemlerinde görevlendirilen personelin teknik bilgi ve becerisi de büyük önem taşımaktadır. Çeşitli sebeplerden dolayı su boruları patlayabilmekte, elektrik, internet ve telefon kabloları kopabilmekte, direkleri yıkılabilmekte veya insan hatası ve ihmalkârlığı öngörülemeyen problemler yaratabilmektedir. Buna ek olarak, teknolojinin geldiği noktada artık kritik işlemler otomasyon sistemleri aracılığıyla veya internet üzerinden birkaç tuşa basılmasıyla idare edilmektedir. Farklı altyapı sistemlerinin entegre edilmesi kırılganlıkları arttıran diğer bir faktördür. Böylece bu sistemlere donanım kırılganlıklarına ek olarak yazılım kırılganlıkları da eklenmektedir. İki altyapı sistemi birleştirildiğinde kullanım kolaylığı sağlamakta ancak aynı zamanda kırılganlıkları da çeşitlendirmektedir. Daha az maliyetle daha verimli sistemler yaratılmaya çalışılırken kırılganlıkların ihmal edilmesi güvenlik tehditleri ortaya çıkarmakta ve sonuç olarak sistemleri inşa eden, yöneten ve kullanan tüm aktörler bundan etkilenmektedir. Diğer bir kırılganlık da, teknolojinin gelişmesiyle birlikte, yazılımların kullanılmasının kolaylaşmasının, kullanıcıların bilgi ve becerisine olan gereksinimi azaltması olarak görülmektedir. Kullanıcıların sahip oldukları teknik bilgi, beceri ve farkındalık sistemin kırılganlıklarını dolaylı yoldan arttırmaktadır. Yirmi birinci yüzyıl teknolojisinin aktörlerin tüm aktivitelerini şekillendirdiği göz önüne alındığında, iletişim ve bilişim güvenliği siber alan içinde aktif olan tüm aktörler için büyük önem arz etmektedir (Goodyear, Goerdel, Portillo, ve Williams, 2010: 9).

Devletlerin siber güvenlik sağlamadaki ikinci adımı nitelikli personel yetişmesini sağlamak ve gelişmiş ülkelere göçmeleri ihtimalinin önüne geçmektir. Bu doğrultuda teknik bilgi ve strateji sahibi olan bireylerin gelişmekte olan ülkelerden gelişmiş ülkelere göç ihtimali oldukça yüksek olmaktadır. Özellikle alanında uzman bireylerin aidiyet duygusunun yüksek tutulması, devletin siber güvenlik politikasının istikrarının sürdürülmesi için kritik öneme haizdir. Bu sayede üçüncü adım olarak toplumdaki

bilincin arttırılması, siber güvenliğin sosyal ve ekonomik hayata etkin bir şekilde entegre edilmesi sağlanabilecek ve yeni yetişen siber güvenlik uzmanlarının toplumda yaratacağı farkındalık sayesinde politikalar daha etkili şekilde uygulanabilecektir. Aynı zamanda gelişen toplum bilinci özel sektörde siber güvenlik uzmanlarının daha çeşitli dallardan geçimi sürdürebilmesine olanak sağlayacak ve beyin göçü azaltılabilecektir. Özel kurumların yazılım ve siber güvenlik uzmanlarına sağladığı imkanlar, kamu-özel sektör işbirliklerinin önünü daha da açarak siber güvenlik politikalarının maliyetlerini azaltırken, verimliliğini arttıracaktır (Carr, 2016: 48).

2.3.1 Altyapı Sistemlerinin İnşa Edilmesi

Devletler, siber güvenlik politikalarını öncelikli olarak kritik altyapı sistemlerini korumak amacıyla oluşturmaktadırlar. Bu kompleks sistemler bir ülkedeki vatandaşların hayatını sürdürebilmesi ve ekonomik sistemin düzenli devam edebilmesi açısından hayati önem taşımaktadır. Kritik altyapı sistemleri kendi aralarında üç kategoriye ayrılmaktadır. Su şebekesi, kanalizasyon, toplu taşıma, telekomünikasyon, elektrik, doğal gaz ve petrol dağıtım sistemleri, acil durum müdahale ve sağlık hizmetleri tümüyle hayatın işleyişini devam ettiren sistemler olarak ilk kategoriyi oluşturmaktadır. İkinci olarak, savunma sanayisi, gıda işleme ve tarım endüstrisi yer almaktadır. Son kategoride ise, hayatın normal seyirde ilerlemesini sağlayan ilk kategoriden güç alan enerji santralleri, havaalanları ve metro istasyonları bulunmaktadır. Bilhassa son kategoride yer alan kritik altyapı sistemlerinin kırılganlıkları yoğunluğun hat safhada olduğu zamanlarda artış göstermektedir (Warfield, 2012: 128).

Devletler açısından siber suçlular ile mücadele yalnızca kritik altyapılar çerçevesinde geliştirilen yöntemlerle sınırlı kalmamaktadır. Bu önlemlere ek olarak aynı zamanda var olan kritik altyapıların güvenliğinin sağlanması ve geliştirilmesi de devlet güvenliği açısından önem arz etmektedir. Devletin, özel kurumların ve bireylerin güvenliğini sağlamak için geniş kapsamlı ve çok taraflı bir mekanizma oluşturulması zorunlu olmaktadır (Ghernaouti, 2013: 7).

İçinde bulunduğumuz bilgi çağında tüm sistemler ve aktörler karşılıklı bağımlı bir yaşam sürmektedir. Bu sebeple, bilgi güvenliği ve internet hizmeti sağlayan altyapıların güvenliğinin sağlanması da tüm aktörler için temel bir gereklilik haline gelmiştir. Örnek olarak, oy verme sistemlerinin zarar görmesi, kullanım dışı bırakılması, verilerin manipüle edilmesi veya ele geçirilmesi gibi durumlar örnek olarak gösterilebilmektedir. Ayrıca, bankacılık sisteminin kesintiye uğraması, müşteri hesaplarında onay olmaksızın işlemler gerçekleşmesi veya enerji dağıtım sistemlerinin, internet altyapısının zarar görmesi, bu hizmetlerden faydalanan milyonlarca kullanıcının mağduriyetine sebebiyet verebilmektedir (Limba, Pleta, Agafonov, ve Damkus, 2017: 561). Daha önce de

bahsedildiği üzere, kritik altyapı sistemlerinin geliştirilme süreci reaksiyonel olmaktan öteye gidememektedir. Kırılganlıkların anlaşılması ve iyileştirme süreçleri ancak emsal bir kırılganlıktan doğan tehditlerin varlığı ile karşılaşıldığında başlatılmaktadır. Diğer operasyonel alanlarda olduğu gibi, siber güvenlikte de güvenlik politikaları farklı saldırılara karşı farklı tedbirlerin geliştirmesi süreci olarak işletilmesi, bir diğer deyişle, dinamik politikalar yürütülmesi gerekmektedir (Warfield, 2012: 133).

Siber alanı güvenli hale getirmek için üçayaklı bir strateji Harknett ve Stever tarafından şu şekilde ortaya konmaktadır; ilk olarak siber tehditlerin ulus çapında bir tehdit oluşturduğunun tüm çevreler tarafından kavratılması, toplumda ve tüm özel kurumlarda farkındalık arttıracak politikaların yürütülmesi için çalışmalar yapılması gerekmektedir. İkinci olarak, devletlerarası işbirlikleri oluşturularak ortak tehditler için ortak çözümler aranması gerekmektedir. Üçüncü olarak, devletlerin ve yerel yönetimlerin kritik altyapı sistemlerinin oluşturulması, geliştirilmesi ve korunması hususlarında özel sektör ile işbirlikleri kurulması gelmektedir (Harknett ve Stever, 2009: 2).

2.3.2 İnsan Kaynağının Yetiştirilmesi

Bilişim teknolojisi her yaştan birey tarafından profesyonel ve günlük yaşam içerisinde aktif bir şekilde kullanılmakta ve modern hayatın ayrılmaz bir parçası olarak görülmektedir. Kullanıcının yerinin ve içinde bulunduğu saat diliminin önemi olmaksızın her türlü bilgiye, kişiye, ürüne veya hizmete saniyeler içerisinde ulaşmasını sağlayan bir araç olmasının avantajları aynı zamanda birçok tehdit unsurunu da içinde barındırmaktadır. Diğer operasyonel alanlardan farklı olarak, siber güvenliğin sağlanması için tüm toplumun dâhil edildiği bir politika gerekmektedir. Karmaşık altyapı sistemleri için gerekli tedbirler alındığı halde bu tesislerde görev alan kişilerin siber alanda güvenli olmaları sağlanmadıkça kırılganlıklar hala mevcut olmaya devam edecektir. Toplumda siber güvenlik bilinci oluşturmak amacıyla siber kültür oluşturmak ve vatandaşların bu konuda bilinç sahibi olmasını sağlamak gerekmektedir (Harknett ve Stever, 2009: 11).

Siber alanda gerçekleştirilmek istenen ofansif ve defansif politikalar doğrultusunda yetişmiş personelden faydalanılabilecek en uygun alan özel sektör olarak karşımıza çıkmaktadır. Özel kurumlar, sadece yetkili çalışanların erişebildiği müşteri bilgileri, ürün patentleri, çalışan özlük dosyaları vb. belgeleri sızdırma girişimlerinden korumak ve rakip kurumlar hakkında bilgi toplamak amacıyla siber alanda kendisini yetiştirmiş uzmanları yüksek ücretler karşılığı istihdam ettiği bilinmektedir. Bu nitelikli bireylerden devlet ve özel sektör işbirlikleri sayesinde, kritik altyapı güvenliği hususunda hizmet alınabilmekte ve devlet kurumlarının ve altyapı sistemlerinin güvenliği bu yöntemle daha kısa sürede ve daha az maliyetle hem de etkili bir biçimde sağlanabilmektedir. Bilhassa siber alanda

ofansif anlamda aktif olan devletler, siber alanda kendini yetiştirmiş bireylerden destek almak suretiyle makul reddedilebilirlik[12] savunması yapmayı kolaylaştırmaktadır. Bu sayede uygulanan politikalar sonucunda herhangi bir misilleme saldırısı veya uluslararası toplumdan kınama benzeri geri dönüşler ile karşılaşma ihtimali en aza indirilmektedir (Hare, 2017: 3-4).

Kritik altyapı sistemlerinin oluşturulması, geliştirilmesi ve korunması süreçlerinde insan faktörü sistemin daimi elemanı olarak yer almaktadır. Her ne kadar makineleşme ve bilgisayarlaşma süreci insan gücünün yerini çoğu aşama için devralmış olsa da, bu sistemlerin yönetilmesi ve tamiratı esnasında insan gücüne olan ihtiyaç kas gücü anlamında azalsa da, beyin gücü anlamında artarak devam edecektir (Goodyear, Goerdel, Portillo, ve Williams, 2010: 9). Ayrıca, siber güvenlik uzmanlarını yetiştirmek uzun ve pahalı bir süreç gerektirmektedir. Gelecek politikalar için bu tip bir süreç uygulamak gerekse de, hali hazırda uygulanması gereken siber güvenlik politikaları için, yetişmiş personele ihtiyaç duyulmaktadır.

2.3.3 Çok Boyutlu ve Entegre Politikaların Şekillendirilmesi

Siber güvenlik politikalarının çok boyutlu olarak şekillendirilmesi ve yürütülebilmesi amacıyla askeri, siyasi, ekonomik ve sosyal hayata entegre edilmesi gerekmektedir. Siber güvenlik politikalarının toplumun yaşayışına ve devlet fonksiyonlarına tümüyle entegre edilmesi siber alanda güvenlik sağlanması açısından önem teşkil etmektedir. Kritik altyapıların güvenliğinin sağlanması tek başına kırılganlıkların tümünü ortadan kaldıramamakta ve kullanılabilecek açıklar bırakmaktadır. Devletlerin siber alanda güvenli olmasını sağlamak amacıyla uygulanabilecek çok taraflılık ve uzun bir süreç gerektiren çeşitli stratejiler bulunmaktadır. Bir devleti siber alanda güvenli hale getiren en önemli adımlar sırasıyla; savunma sistemleri ve tüm politika araçları, iç ve dış tehditlere karşı tetikte olan bir askeri gücün varlığı, yapılanması ve işleyişi siber tehditlere karşı korunan ve geliştirilen ekonomik ve siyasi sistemler oluşmaktadır. Bunları tamamlayacak diğer önemli bir faktör ise, süreklilik sağlamak amacıyla gelecek kuşakların farkındalık seviyelerinin yüksek tutularak siber güvenlik kültürüne sahip bir toplum yaratılmasıdır (Goodyear, Goerdel, Portillo, ve Williams, 2010: 12).

Siber alanda aktif bulunan aktörler devlet kurumlarının internet sitelerine, kritik altyapı kontrol mekanizmalarına, özel kurumların bilgi depolama sunucularına, ekonomik sistemlere ve bireylere günden güne daha sık, daha organize ve daha maliyetli yöntemler geliştirerek saldırılar düzenlemektedirler. Hem internet kullanıcılarının, hem de internet ortamına aktarılan bilgi, belge yönetimi süreçlerinin ve yazılım bağımlılığının son

[12] Bkz. Makul Reddedilebilirlik (Plausable Deniability): Yeterli delil yoksunluğu sebebiyle herhangi bir eylemin kimin tarafından gerçekleştirildiğinin ispatlanamayacağını belirtmek için siyasiler ve hukukçular tarafından kullanılan terimdir. USLEGAL (2019) https://definitions.uslegal.com/p/plausable-deniability/

yıllarda büyük artış göstermesi, siber saldırıların sayısındaki artışta önemli bir faktör olarak belirmektedir. Etkili bir güvenlik stratejisi oluşturmak için mümkün olan tüm tehditlere karşı tedbir alınması gerekmektedir. Alınacak tedbirlerden ilki, tehdidin gerçekliğinin farkına varılması ve zarar verme kapasitesinin ölçülebilmesi olarak görülmektedir. Siber saldırıların hedefi her ne kadar elektronik sistemler olsa da, saldırganın başarı ölçütü elektronik sistemlere verilecek zarar üzerinden mağdur olacak kurum, kuruluş ve birey sayısı ile belirlenmektedir. Bu sebeple siber askeri güvenlik stratejileri kapsamında karşı tarafı saldırıdan caydırma (siber caydırıcılık), zayıflatma (siber savaş), aktör ve politikaları hakkında bilgi toplama (siber espiyonaj) şekillerinde ofansif stratejiler kullanılmaktadır. Devlet güvenliği açısından geliştirilen siber stratejilerin her biri farklı durumlara uygulanabilen, bir diğer deyişle, dinamik olması ve birbiri ile bütünleşebilecek şekilde işlemesi gerekmektedir. Örnek olarak, yaygın bir şekilde kullanılan haberleşme ağlarının ihtiyaç durumunda espiyonaj faaliyetlerinin yürütülmesinde bir araç olarak kullanılabilmesi ve siber saldırı gerçekleştirilmesi durumunda hedef belirlenmesinde kullanılabilecek şekilde geliştirilmesi bu hususta son derece önem teşkil etmektedir (Sarbu, 2017: 132-137).

Modern teknolojideki gelişmeler çatışma kültürünü değiştirmiş ve aktörler arasında bilhassa devletlerarası sıcak çatışmaların varlığı büyük bir otorite boşluğu bulunmayan bölgeler harici az görülür hale gelmiştir. Siber operasyonlar modern askeri yöntemler arasında aktörü birkaç adım öne geçirecek son derece faydalı yöntemler sağlayabilmektedir. Saldırı gerçekleştirilen aktör yeterli savunma stratejisine sahip değilse, siber operasyonların etkileri kritik altyapı sistemleri üzerinde oldukça yıkıcı olabilmektedir (Areng, 2016: 124). Aktif savunma politikalarının yürütülmesi siber güvenlik stratejilerinin askeri hayata entegre edilmesinde önem verilmesi gereken adımlar arasında görülmektedir. Robert S. Dewar'a göre başlıca örneklerden biri beyaz solucan[13] programlarının kullanılmasıdır. Bir diğer yöntem ise, bilgi aktarımı sırasında alıcının adresini sürekli olarak değiştiren yazılımlar kullanılmasıdır. Adres aktarımı olarak da bilinen bu yöntem sayesinde bilginin depolandığı sunucuların mevcut olduğu asıl adres güvende tutulmaktadır. Aynı zamanda sisteme sızan aktörün yerini tespit edebilmekte ve misilleme opsiyonu sunabilmektedir. Ayrıca, sisteme sızma girişiminde olan aktörlerin sistemde geçirmek zorunda kalacakları zamanı ve dolayısıyla açığa çıkma ihtimalini arttırdığı için bir caydırıcılık yaratarak siber saldırı olasılığını azaltmaktadır. Savunma sistemlerinin bu minvalde geliştirilmesi hem tehdidin orijini hakkında bilgi sağlamakta, hem de ofansif politikalar uygulama imkanı tanımaktadır (Dewar, 2014: 9-10).

Bir ülkede siber güvenlik politikalarının oluşturulmasında ekonomik ve politik süreçler de önemli rol oynamaktadır. Zira altyapı hizmetlerini güvenli hale getirmek öncelikle

[13] Beyaz Solucan: White Worms adıyla bilinen, sistemi etkileyen zararlı yazılımları bularak ve ardından etkisiz hale getiren ve güvenlik ihlallerini tespit etmede kullanılan koruma yazılımlarının bir örneğidir (Lu, Xu ve Yi, 'Optimizing Active Cyber Defence'2013: 207).

mali bir yük barındırmaktadır. Aktörün dış politika hedeflerinin göz önünde bulundurulması gerekmekte ve belirlenen bütçenin harcama alanına da bu hedefler doğrultusunda karar verilmektedir. Sonuç olarak, yetki sahibi politikacılar hangi sistemlerin tehdit altında olduğu ve hangi sisteme öncelik verilmesi gibi hususlarda karar verici rol oynamaktadır. Bilhassa kritik altyapı sistemlerinin geliştirilmesinde ve işletilmesinde rol alan karar vericilerin, bilgi çağının beraberinde getirdiği imkân ve tehditlere karşı farkındalık sahibi olması son derece önem arz etmektedir. Politikacıların halkın farkındalık seviyesi üzerinde büyük bir etkisi olduğu göz önünde bulundurulduğunda, devletin bu konuda önlem alma hızını önemli ölçüde arttırmasına katkı sağladığı söylenebilmektedir. Hangi sistemlerin tehdit altında olduğu ve hangi sistemlerin geliştirilmesi gerektiği politikacıların yeterli bilgi ve tecrübe sahibi olmadan alamayacakları kararlar olmakla beraber uzmanlık gerektirmektedir. Bu sebeple özel sektördeki uzmanlardan destek almak ve kamu-özel sektör işbirlikleri çerçevesinde kritik altyapı sistemlerinin geliştirilmesi ve korunması faaliyetlerinde bir yönetişim modeli ortaya koymak daha kapsamlı bir güvenlik yapısının oluşumuna hizmet edecektir. (Cavelty, 2013: 111-114).

Bilgi ve iletişim teknolojilerinin modern hayatın ayrılmaz bir parçası haline geldiği dünya düzeninde, yerel risk olarak adlandırılabilecek tehditler kolayca sistemik tehditler haline gelebilmekte ve kullanıcıların mağduriyetine sebebiyet verebilmektedir. Örnek olarak, yalnızca birkaç saat için bankacılık sistemlerinin işleyişini durduracak siber saldırılar, ekonomik sistemin hasar görmesine ve dolayısıyla tüm aktörlerin mağduriyetine sebebiyet verebilmektedirler. Teknolojik ilerlemenin yanı sıra küreselleşmenin de bir sonucu olarak serbest piyasa ekonomisinde özel kurumların bilhassa ürün geliştirme süreçlerinde kritik bilgi bankalarını yetkili birimler[14] ile paylaşma zorunluluğu doğmuştur. Şirketler arası rekabetin yol açtığı sanayi casusluğu vakaları sonucunda ticari sırlar, müşteri ve çalışan bilgileri gibi bilgilerin bulunduğu kritik bilgi bankaları saldırıya uğrayabilmekte ve korunması gittikçe zorlaşmaktadır. Günlük ticari faaliyetin büyük çoğunluğunun siber alan üzerinden gerçekleştiği düşünüldüğünde, bu alanın güvenli hale getirilmesindeki gereklilikler ve karşılaşılan güçlükler daha net anlaşılmaktadır (Andrijcic ve Horowitz, 2006: 907-908).

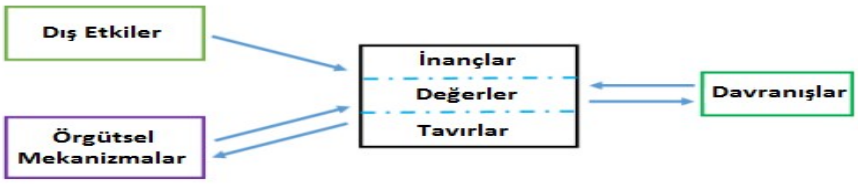
Siber güvenliğin sağlanması amacıyla yapılan yatırımların gerçekleştirilmesi öncesinde karşılaşılmakta olan en büyük güçlüklerden biri de tehdidin gerçekliğinin kavranması süreci teşkil etmektedir. Çağdaş bir planlama doğrultusunda yapılacak tüm yatırımlar altyapı sistemlerini güvence altına alacak ve beklenen zararı azaltmada önemli rol oynayacaktır. Yatırım planlamaları uzun bir süreçten oluşabilmekte, güncel tehditlere ve

[14] Müşteriler, tedarikçiler, taşeronlar, danışmanlar ve stratejik ortaklar.

politik amaçlara paralel olarak kademeli şekilde uygulanabilmektedir. Bunun yanında, ne kadar bütçe ayrılması gerektiği ile ayrılan bütçenin nasıl harcanması gerektiği birbirinden farklı süreçler olmakta ve aktörün başlangıçta analiz sürecini gerçekleştirirken hesaba katması gereken faktörler, alacağı geri dönüşlerde belirleyici rol oynamaktadır. Yatırımların güncel tehditler ve kırılganlıklar üzerine yoğunlaşması izlenebilecek en sağlıklı politikaların başında gelmektedir. Ardından yapılacak yatırımlar defansif politikalara katkı sağlamak amacıyla uygulandığında, aktörün amacına ulaşma ihtimali yükselmektedir (Rue ve Lawrance Pfleeger, 2009: 55-58).

Yapılan yatırımların ve uygulanan siber güvenlik politikalarının etkili bir şekilde yürütülmesinin en önemli adımlarından biri de bireysel farkındalık yaratmaktır. Muazzam bütçeler ve son teknoloji kullanarak yapılan yatırımların başarısız olması ve güvenlik duvarlarının aşılması için yanlış bir tıklama (kaynağı bilinmeyen bir mailin açılması) yeterli olmaktadır. Bu sebeple güvenliğin sağlanması için siber alanda aktif tüm bireylerin hem profesyonel hem de günlük yaşamlarında bir siber kültür sahibi olması ve farkındalık derecelerinin yüksek olması gerekmektedir (Ponemon Institute LLC, 2018: 24).

Şekil 2. Siber Güvenlik Kültürünün Oluşum Çerçevesi



Kaynak: Huang, K., ve Pearlson, K. (2019: 6399). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences* (s. 6398-6407). Hawaii: HICSS. https://hdl.handle.net/10125/60074 adresinden alındı.

Bireylerin bilgi güvenliği ve siber güvenlik kültürüne sahip olabilmeleri için dış bir etken olarak verilmesi gereken farkındalık eğitimleri atılması gereken ilk adım olarak görülmektedir. Sistemin kırılganlıkları, korunma yöntemleri ve siber saldırıların potansiyel etkileri konusunda bilgi sahibi olan bireyler, siber alandaki aktiviteleri esnasında daha temkinli ve bilinçli hareket edeceklerdir. Sadece profesyonel yaşamda değil, günlük yaşamda ihmal edilen güvenlik önlemlerinin de güvenlik politikalarının başarısızlığına sebep olabileceği kavranmalı ve davranışlar bu doğrultuda şekillendirilmelidir. Verilen eğitimlerin zaman içerisinde bireylerin inançlarına, değerlerine ve tavırlarına yansımaya başlaması için uygulanması gereken örgütsel mekanizmalar son derece önemlidir. Eğitimler, bu mekanizmalar ile desteklendiğinde

doğru davranışlar ortaya çıkmaya ve siber kültür oluşmaya başlayacaktır (Huang ve Pearlson, 2019: 6399).

2.3.4 Özel Sektör ile İşbirliklerinin Çeşitlendirilmesi

Kritik altyapı sistemlerinin korunması devletlerin siber anlamda güvende olabilmeleri için atmaları gereken adımların başında gelmektedir. Bu sistemlere yönelik tehditlerin tamamiyle yok edilmesinin mümkün olmamakla beraber, aynı zamanda mevcut tehditler de günden güne çeşitlenmektedir. Bilgi çağında üretilen politikaların kapsayıcı olması son derece önem teşkil etmektedir. Zira, serbest piyasa ekonomisinin tüm dünyaya yayılması ve küreselleşmenin tüm dünyayı karşılıklı bağımlı hale getirmesi devletler arasındaki siyasi sınırları belirsizleştirdiği gibi, devletin temel sorumluluğu olan temel altyapı hizmetlerini sağlama görevlerinin de özel sektöre devredilmesine vesile olmuştur. Dış müdahele, sistem arızaları veya insan hatası sonucu zarar görmesi altyapı hizmetlerinden yararlanan tüm aktörlerin mağduriyetine neden olma potansiyelini taşımaktadır. Bu sebeple, tüm altyapı sistemlerinin oluşturulma, geliştirilme ve korunma süreçlerinin yalnızca devlet tarafından gerçekleştirilmesi yerine, hali hazırda işletmesi özel sektöre devredilmiş olan sistemlerin siber alana entegre edilmesi ve gerekli tedbirlerin alınması devlet ve özel sektör arasında karşılıklı bir sorumluluk olarak görülmektedir.

Kamu-özel sektör işbirlikleri bilhassa siber güvenlik altyapı sistemleri oluşturma, geliştirme ve koruma süreçlerinde dünyanın birçok ülkesinde yaygın bir biçimde kullanılmaktadır. Özelleşen hizmetlerin bürokratikleşmenin azalmasını sağlaması ve rekabet ortamını arttırmasıyla halkın hizmetlere daha cüzi bir miktar karşılığında erişmesi, kamu-özel sektör işbirliklerinin yaygınlaşmasındaki başlıca etkenler olarak kabul edilmektedir. Bahsedilen işbirlikleri devlet ve özel sektör arasındaki üst-ast ilişkileri olarak değil, kendi kendine organize olabilen ve kendi kendini yöneten mekanizmalar oluşturmaktadır. Bir diğer deyişle, devletin görevi kendi kendini yöneten mekanizmaları yakından kontrol etmek değil, yönetişim çerçevesinde kritik altyapıların güvenliğini sağlayan ağların oluşumu için gereken ortamın oluşmasına vesile olmak ve koordinasyon çalışmalarını üstlenmektir. Kamu özel-sektör işbirliklerinin kritik altyapı güvenliğinde yaygın olarak kullanılmasının başlıca sebebi bu tip teknolojik uzmanlık gerektiren çalışmaların hayata geçirilme süresinin kaydadeğer oranda kısaltması olarak görülmektedir. Özel sektörde bu alanda hizmet veren şirketlerin varlığı güvenlik politikalarının geliştirilme hızının artmasında önemli bir rol oynamaktadır. Bu minvalde kamu-özel sektör işbirlikleri hem milli güvenlik hem de küresel güvenlik yaklaşımları tarafından oldukça kullanışlı yönetişim araçları haline gelmiştir (Dunn-Cavelty ve Suter, 2009: 180).

Tehdit unsurlarının orijininin muğlak ve kritik altyapıların siber saldırılara karşı savunmasız olduğu bilgi çağında güvenlik stratejileri kamu-özel sektör işbirlikleri ile etkili bir şekilde yürütülebilmektedir. Zira özel sektörün sürece dahil edilmesiyle devlet

güvenliği perspektifine ek olarak daha liberal politikalar da gözetilebilmekte ve bütüncül bir güvenlik anlayışı inşa edilebilmektedir. Kamu-özel sektör işbirliklerinin etkili birer araç olarak kullanılabilmesi için, risklerin iyi analiz edilmesi ve bu doğrultuda stratejik hedeflerin önceden belirlenmesi gerekmektedir. Aynı zamanda tarafların arasındaki ilişkinin karşılılıklı güvene dayanması son derece önem taşımaktadır. Bu ilişkinin oluşturulması ve geliştirilmesi amacıyla kamu özel sektör işbirliklerinin daha küçük ölçekte başlatılarak belli bir süre zarfında geliştirilmesi önerilmektedir (Manly, 2015: 90-91). Örnek olarak, şehir planlama faaliyetlerinde, ulaşım hizmetlerinin sağlanmasında, eğitim, sağlık ve cezaevi tesislerinin hayata geçirilme süreçlerinde yap-işlet-devret metodu kullanılarak özel sektöre devredilmesi, devlet-özel sektör-birey üçgeni arasındaki karşılıklı güven ilişkisinin sağlamlaştırılması amacıyla atılması gereken adımlardan biri olarak gösterilmektedir .

Bilhassa modern toplumlarda iş bölümü her geçen gün daha çok yaygınlaşmakta ve uzmanlık gerektiren yeni alanlar ortaya çıkmaktadır. Siber güvenlik politikalarının bu alanlardan biri olması sebebiyle özel şirketlerin bu sürece dahil edilmesi, kapsayıcı bir güvenlik yaklaşımı oluşturabilmesi için gereklilik teşkil etmektedir. Geçmişte devlet tarafından gerçekleştirilen hizmetlerin büyük çoğunluğu bugün özel sektör tarafından sağlanmaktadır. Hem devlet hem de özel sektör kritik bilgi bankalarının sızdırılması ihtimaline karşı önlemler almaktadır. Karşılıklı güven ilişkisinin oluşması, ancak ortak bir çaba doğrultusunda tarafların başarı elde edebileceğinin anlaşılmasına dayanmaktadır. Devletin özerk yapılar kurulmasına yönelik ortam sağladığı ve özel sektörün bu alanda yapılandığı bir siber güvenlik sistemi meydana getirmek kademeli bir gelişim süreci gerektirmektedir (Dunn-Cavelty ve Suter, 2009: 185).

Tarih boyunca geliştirilen diğer tüm teknolojilere kıyasla, internet kullanımı tüm dünya tarafından oldukça hızlı benimsenmesiyle öne çıkmaktadır. Buna ek olarak, internet teknolojisinin kısa bir zaman içerisinde günlük, siyasi, ekonomik hayatın ve askeri teknolojilerin kullanım alanı haline gelmesiyle internet güvenliği büyük önem kazanmıştır. Bilhassa internet güvenliğinin ulusal ve uluslararası alanda sağlanabilmesi için gereken farkındalık tehditlerin ve siber saldırılara maruz kalan devletlerin çoğalmasıyla artış göstermektedir. Ancak koordine edilmiş bir takip mekanizması veya tehditleri bertaraf etmek amacıyla belirlenmiş ortak stratejiler oluşturulmadığı takdirde güvenlik inşa etme çabalarının yetersiz kalacağı öngörülmektedir (Choucri, Madnick, ve Ferwerda, 2014: 98).

Siber güvenlik politikaları ve kritik altyapıları için yürütülen politikalar hem devletin hem de özel sektörün kontrolünde bulunan altyapıların korunması amacıyla gerçekleştirilmektedir. Serbest piyasa ekonomisinin hakim olduğu ülkelerde[15] altyapı

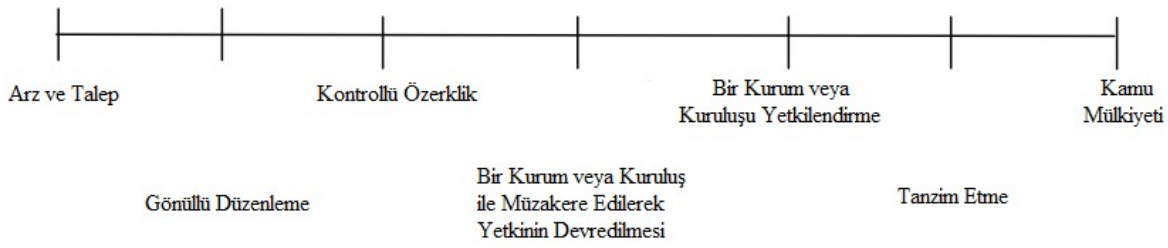
[15] Örnek olarak, ABD'de kritik altyapı hizmetlerinin %90'ından fazlası özel sektörün kontrolünde bulunmaktadır.

hizmetlerinin büyük çoğunluğunun özel sektörün kontrolünde olduğu göz önüne alındığında kapsamlı bir siber güvenlik politikasına duyulan ihtiyaç daha net anlaşılmaktadır (Singer ve Friedman, 2014: 20). Etkin bir güvenlik politikası uygulayabilmek için rekabetçi olmayan, hiçbir aktörün dışarıda bırakılmadığı ve toplum faydasını her şeyin önüne koyan yaklaşımların benimsenmesi gerektiği düşünülmektedir (Shore, Du, ve Zeadally, 2011: 4).

3. BÖLÜM: KAMU – ÖZEL SEKTÖR İŞBİRLİĞİ KAPSAMINDA ŞEKİLLENDİRİLEN SİBER GÜVENLİK POLİTİKALARI VE ÖRNEKLERİ

Kamu ve özel sektörün bir araya gelerek oluşturduğu işbirlikleri tüm dünyada yaygın bir şekilde kullanılmaktadır. Bu işbirlikleri yirminci yüzyılın sonundan günümüze uzanan süreçte, gerekli kritik altyapı sistemlerinin inşa ve işletim süreçlerinde rol almakta ve halka hizmet götürme anlamında önemli katkılar sağlamaktadır. Modern hayatın kesintisiz devamlılığı için, devletin sağladığı imkânlar doğrultusunda kamu-özel sektör işbirlikleri aracılığıyla kritik altyapı sistemlerinin inşa, finansman, işletme ve onarım aşamaları özel sektöre devredilebilmektedir. Ancak, bu sistemlerin haiz olduğu risk ve tehdit unsurlarına karşı ortak sürdürülebilir güvenlik politikaları uygulanabilmesi için yönetişim mekanizmalarına ihtiyaç duyulmaktadır. Bilhassa altyapı sistemlerinin siber alana entegre edilmesi ile birlikte uzaktan yetkisiz erişimler veya kullanıcı hataları sistemlerin arızalanmasına ve işlevselliklerinin tehlikeye girmesine sebep olabilmektedir. Bunu önlemek amacıyla altyapıların ve kullanıcılarının ulusal güvenlik politikalarının bir parçası haline getirilmesi giderek daha fazla önem kazanmaktadır.

Şekil 3. Kamu-Özel Sektör İşbirliği Yelpazesi



Kaynak: Shore, M., Du, Y., ve Zeadally, S. (2011: 5). Public Private Partnership Model for National Cybersecurity. *Policy Studies Organization*, Vol. 3, Iss. 2, Article 8.

Şekil 3'te de gösterildiği üzere kamu-özel sektör işbirliklerinde soldan sağa doğru ilerledikçe devletin, sağdan sola ilerledikçe de serbest piyasa kontrolünün arttığı görülmektedir. Devletin, işbirliği yapmayı seçtiği kuruma olan güveni, toplumun ihtiyacı ve altyapı sistemlerinin gereksinimleri doğrultusunda seçilmekte ve politikalar bu doğrultuda uygulanmaktadır. Mevcut altyapı sistemlerinin devlet güvenliği açısından son derece önemli olması durumunda bu sistemler özel sektöre devredilmeyerek kamu mülkiyetki korunmakta ve devlet tam kontrol sahibi olmaktadır. Bu sayede küresel ekonomik krizlerden en az zararla çıkılabilmesi, talep arttırma, ekonomik durgunlukları önleme ve devlete olan güven ortamının arttırılarak ülkeye yatırımcı çekilmesi bağlamlarında politikalar yürütülebilmektedir. Örnek olarak, Çin'in uygulamakta olduğu kamu mülkiyeti sistemi 2015 yılında kamu mülkiyetinde bulunan 106 büyük şirketin 47'sinin Fortune 500 listesine girmesine imkan sağlamıştır (Qi ve Kotz, 2019: 4-6).

Tanzim etme yönteminde devletin siber güvenlik politikaları çerçevesinde belirlemiş olduğu standartlar kapsamında, devlet görevin tanzim edildiği özel sektör temsilcisinin

yönetimini düzenli olarak denetlemekte ve standartlara uyulmaması durumunda cezai yaptırım uygulamaktadır. Oldukça müdahaleci bir yöntem olduğu için emir ve kontrol sistemi adı ile de bilinmektedir. İsrail'in uygulamakta olduğu siber güvenlik politikaları bu yöntem ile yürütülmektedir (Assaf, 2008: 7). İsrail'in karşı karşıya olduğu siber tehditler göz önüne alındığında politikaların söz konusu biçimde yürütülmesinin sebepleri ilerleyen başlıklar altında incelenecektir.

Bir kurum veya kuruluşun yetkilendirilmesi yönteminde kural koyma yetkileri kamu idarelerine delege edilmiştir. Bu kurumların yetkileri, uygun gördükleri takdirde standart belirleme, denetleme ve yaptırım uygulama seçeneklerini mümkün kılmaktadır. Özel sektörün sahip olduğu uzmanlığın ve yürütülen politikaların işlevselliğinin, siyasi etki altında kalınmadığı ve bağımsız bir şekilde uygulanmasına müsaade edildiği durumlarda etkili sonuçlar ortaya çıkarılabileceği öngörülmektedir. Yeni Zelanda devleti telekomünikasyon endüstrisini bu yöntem aracılığıyla idare etmektedir. Bu sayede tek bir şirketin fazla büyüyerek tekelleşmesinin önüne geçilmekte ve rekabet ortamının önü açılmaktadır. Şekil 3'te görülen gönüllü düzenleme yöntemi ile de telekomünikasyon sektörü ile devlet arasında yürütülen işbirlikleri kısa süreli olarak gerçekleşmiş, ancak devletin özel sekörden beklediği sınırlama girişimlerinin devletin gözünde yeterli görülmemesi sonucunda bu uygulamaya son verilmiştir (Shore, Du, ve Zeadally, 2011: 5).

3.1 İsrail Örneği

İkinci Dünya Savaşı'nın sona ermesinden üç yıl sonra 1948 yılında İsrail devleti resmi olarak kurulmuş ve uluslararası düzene dâhil olmuştur. Ancak yer aldığı coğrafya sebebiyle kuruluşundan bu yana çatışma ortamı içerisinde varlığını sürdürmektedir. Hem sınır komşularıyla hem de terör örgütleriyle tekrar eden çatışmalar, bitmeyen düşmanlıklar, Suriye, Ürdün, Mısır ve Filistinliler ile yürütülmeye çalışılan başarısız barış süreçleri yıllar içerisinde kötü bir imaj inşa etmiş ve bu süreç İsrail'in saldırgan bir güvenlik politikası geliştirmesine vesile olmuştur (Freilich, 2006: 635).

Bulunduğu jeopolitik konumun hassasiyeti itibariyle 60 yıl boyunca milli güvenlik politikalarını ön planda tutmuş olan İsrail'in sahip olduğu kurumlar tüm dünyada işlevsellikleri ve kapsamlı yapılarıyla itibar kazanmışlardır. İsrail Silahlı kuvvetleri, istihbarat servisi, savunma ve dış işleri bakanlığı kurumlarının kalitesi, işlevselliği, kurulmuş olan sistemin karmaşıklığı ve de ölçeği bakımından en kapsamlı milli güvenlik stratejilerinden biri olarak görülmektedir. Orta Doğuda kurulmuş ve göreceli olarak küçük bir devlet olmasına rağmen, İsrail karşı karşıya kaldığı askeri, siyasi, ekonomik, teknolojik ve çevresel tehditler sebebiyle kapsamlı bir güvenlik stratejisine ihtiyaç duymaktadır. Örneklendirmek gerekirse; Irak, İran ve Libya'nın sahip olduğu kitle imha silahları tehditler listesinde ilk sırada yer almaktadır. ABD ile silah teknolojileri ve terör karşıtı strateji geliştirme alanlarında stratejik ortaklıklar kurulmasının sonucunda küresel

bir aktör olmayı amaçlayan İsrail, teknolojik gelişmeleri yakından takip ederek kısa sürede bu amaçlarına ulaşmayı-günümüz itibariyle-başarmıştır. Diğer taraftan, İsrail dünyanın dört bir yanındaki Yahudi diasporasına ek olarak farklı çevrelerden de göç almıştır. İlk yıllardaki kısıtlı insan kaynağı ile yürütülmüş olan politikalar İsrail için küçük ölçekli olmalarıyla mali yönden avantaj, uzman personel yönünden kısıtlı olmasıyla dezavantaj yaratmıştır. Farklı bölgelerden göç alan İsrail zaman içerisinde birçok ülke ile diplomatik ilişkilerinde farklı politikalar izlemek durumunda kalmıştır. Örneklendirmek gerekirse; Soğuk Savaş sonrasında Sovyetler Birliği'nin dağılması sonucu bölgeye göç eden Rus göçmenler Rusya ile olan ilişkilerin derinleştirilmesini gerektirmiştir ve hem göçmenlerden işgücü anlamında faydalanabilmek hem de Rusya'nın Orta Doğu'daki politikalarının kendi amaçlarıyla çatışmasını engellemek için politikalar geliştirilmesi gerekmiştir (Freilich, 2013: 259).

20. yüzyılın son on yılına gelindiğinde ulusal güvenlik kurumları kayda değer ölçüde büyümüş, var olan kurumlara yenileri eklenmiş, çalışan sayıları ve kalitesi yükseltilmiştir. Aynı zamanda geçmişte yapılan yatırımlar bu yapıların kompleks süreçler ile yönetilebilmesine imkan tanımıştır. Bilgi teknolojilerinin de yaygın kullanımı sayesinde kapasite büyük oranda arttırılmıştır. Askeri teknolojilerde gelinen noktada üretilen uydular, hava araçları, anti füze sistemleri bağlamında sahip olunan son teknoloji İsrail'e hem ekonomik gelir kaynağı, hem de askeri avantaj sağlamıştır. Söz konusu teknoloji her ne kadar çeşitli biçimlerde İsrail'in teknolojik ilerlemesine yardımcı olduysa da aynı zamanda yeni kırılganlıkların oluşumuna sebebiyet vermiştir. Bilindiği üzere, etkin bir üretim ve planlama sistemi kurulabilmesi için bilişim teknolojilerine ihtiyaç duyulmakta ve bilişim teknolojilerinin vardığı nokta siber güvenlik politikalarının şekillenmesinde etkili olmaktadır. Zira İsrail'in kurmuş olduğu bilişim teknolojilerine ağırlıklı olarak bağımlı sistemler devamlı olarak siber saldırılara maruz kalmaktadır. Örnek olarak, 2012 yılındaki toplam saldırılar dakika başına yaklaşık olarak bin saldırıya tekabül etmektedir (Grauman, 2014: 64-66). 2014 yılında ise Gazze'de Hamas'a karşı yapılan operasyon süresince siber aktivistler sistemleri ele geçirerek günde bin roket ile saldırıda bulunacaklarını sosyal medya hesapları üzerinden duyurmuş ve gerçekleştirilen dağıtılmış hizmet engelleme saldırıları günde bir milyona kadar ulaşmıştır (Fowler, 2014: 4).

Milyonlarca saldırının sadece birinin güvenlik duvarlarını aşmayı başarması bile tüm sistemin başarısızlığı anlamına gelmektedir. Bu sebeple tehditleri ortadan kaldırmak amacıyla İsrail siber alanı sadece savunma için değil ofansif politikalar yürütmek için de kullanmaktadır. Bu sayede büyük teknoloji şirketleri İsrail'in potansiyelinin farkına vararak İsrail'de ofisler açmışlar ve devlet siber alanda aktif çalışacak şirketler için teşvikler vermiştir (Cohen, Freilich, ve Gabi, 2015: 1). Siber güvenlik alanında hizmet veren servisler ile yetenekli personel, ulusal güvenliğe önemli katkılarda bulunmaktadırlar. Küresel siber güvenlik endüstrisi 2015 yılında 75 milyar dolara tekabül etmekteyken, 2020 yılında yükselmesi beklenen ihracat değerleri ile 170 milyar dolar hacme ulaşacağı öngörülmüştür. 2015 yılındaki verilere göre İsrail'in küresel siber

endüstrideki payı yıllık 2 milyar dolar olarak kayıtlara geçmiştir (Nevill, 2016: 223; Morgan, 2015).

3.1.1 Altyapı Sistemlerinin Oluşturulması

İsrail kuruluşundan itibaren tehdit unsurlarını temel ve güncel tehditler olarak iki bölüme ayırarak çerçevelendirmektedir. Temel tehditler İsrail'in bütünlüğüne tehlike arz eden mevcut ve potansiyel tehdit unsurlarını, konvansiyonel savaşları ve büyük ölçekli sıcak çatışmaları kapsamaktadır. Güncel tehditler ise, devletin bütünlüğüne hali hazırda tehdit oluşturmayan ancak büyümesi sonucu tehditlere dönüşme potansiyeli olan düşük yoğunluklu çatışmaları, küçük çaptaki terör eylemlerini, İsrail'in bütünlüğünü tehdit edecek kadar ciddi olmayan sınır çarpışmaları gibi düşmanca müdahalelerin tamamını içermektedir (Raska, 2015: 3). Ayrıca güvenlik politikalarının uygulanmasında tehdidin geldiği merkeze göre ayrılan 'savunma halkaları' geliştirmiştir. İlk halka çevre savunması (perimeter) olarak adlandırılmakta ve İsrail'in toprak bütünlüğüne karşı tehlike içeren konvansiyonel askeri tehditleri ifade etmektedir. Suriye, Ürdün, Mısır gibi komşu ülkelerin sınırda hazır bekleyen silahlı güçleri bu politikanın gerekçelerinden biri olarak gösterilmektedir. İkinci halka sınır içi güvenliği (intra-frontier) olarak isimlendirilmekte ve devlet sınırları içerisinde gerçekleştirilen terör saldırıları ve düşük yoğunluktaki çatışmaları ele almaktadır. Hamas'ın gerçekleştirdiği terör eylemleri sonucu gerçekleşen küçük çaplı çatışmalar örnek olarak verilebilmektedir (Raska,2015: 4).

Son halka olan dolaylı sorumluluklar (remote commitments) ise, sınır güvenliğini veya toprak bütünlüğünü tehdit etmeyen ancak devlet güvenliğine farklı biçimlerde zarar verebilme potansiyeli olan tehditler ile meşgul olmaktadır. Örnek olarak, İsrail'e karşı gerçekleştirilen siber saldırılar veya ekonomik ambargolar verilebilmektedir (Raska, 2015: 3). 1990'lardan itibaren teknolojide yaşanan gelişmeler İsrail'in güvenlik politikalarının da güncellenmesini gerektirmiştir. Bu minvalde yukarıda sözü geçen savunma halkalarına verilen önem Soğuk Savaş döneminde birinci halkada ağırlıklıyken, siber güvenlik çalışmalarının da politikalara eklenmesiyle ikinci ve hatta üçüncü halkaya verilen önem ile ayrılan kaynak miktarı artış göstermiştir. İlk halkanın savunulması hususunda rakip aktörlere karşı geçmişte sağlanan üstünlük diğer halkalara kaynak ayrılmasına olanak tanımıştır. Buna rağmen, İsrail her ne kadar sınırlarını güvence altına almakta başarılı olsa da, siber alanda coğrafyası ve kimliği belirsiz tehditlere karşı ilk başlarda defansif politikalar uygulamaktan öteye gidememiştir. İsrail Savunma Kuvvetleri 14. Kurmay Başkanı Ehud Barak'ın döneminde, siber alandaki tehditlere karşı güvenlik altyapılarının kademeli olarak arttırılması ve var olanların da geliştirilmesi gerektiğini belirtilmiştir. Siber alan geleceğin savaş alanı olarak öngörülmüş ve konvansiyonel savaşların yanında siber saldırıların denge bozucu bir faktör olarak kullanılabileceği ifade edilmiştir (Raska, 2015: 4).

Toplu taşıma, enerji sağlama ve finans hizmeti gibi kritik altyapıların sorunsuz şekilde işlemesi için, telekomünikasyon, bilgisayar ve bulut teknolojileri gibi uzaktan erişimi mümkün kılan teknolojiler üzerinden siber alana erişimlerin sekteye uğramaması gerekmektedir. Kritik altyapıların siber alan üzerinden birbirlerine bağlanması ve yazılım teknolojileri kullanılarak uzaktan yönetilmesi daha önce karşılaşılmayan güvenlik tehditlerinin ortaya çıkmasına sebep olmuştur. Kullanılan donanım, yazılım veya sisteme erişimi olan kullanıcıların yarattığı riskler İsrail'in siber güvenlik politikalarında kritik altyapı güvenliğine verdiği önemin artmasını sağlayarak farkındalık gelişmesini sağlamıştır. Hizmetlerin siber alana olan bağımlılıkları artış gösterdikçe tehditlerin de çeşitleneceği öngörülerek devletin kurmuş olduğu sistemlerin diğer aktörler tarafından kendi çıkarları doğrultusunda kullanılabileceği belirtilmiştir. 20nci Genelkurmay Başkanı Benny Gantz, sahip olunan kırılganlıkların siber teknolojiler aracılığıyla siber casusluk eylemlerinde kullanılabileceği gibi, aynı zamanda sınır çatışmalarının öncesinde, süresince ve sonrasında düşmanı zayıflatma aracı olarak etkili olabileceğini, bilhassa sivillere ve sivillerin kullanmakta olduğu altyapı sistemlerine zarar vermek için çeşitli opsiyonlar sunabileceğini ve neredeyse tamamen şeffaf bir şekilde herkesin gelişmeleri anlık olarak takip etme imkânının siber alanda mevcut olduğunu belirtmiştir (Harel, 2013: 2).

Sivil sistemlerin tehditlere karşı korunması 2002 yılında İsrail Parlamentosundan geçmiş olan 84/B yasası ile sağlanmaya başlamış ve zamanla de facto[16] olarak milli siber güvenlik politikası haline gelmiştir. Yasa tasarısının hazırlanmasında görev alan sekiz kurumun sorumlulukları şu şekilde sıralanmıştır (Tabansky, 2013: 81):

- Tehdit tabiatını belirlemek ve komitenin onayına sunmak,

- Sistemleri kritik olarak sınıflandırılmak ve gözetim altında tutulmasını komiteye önermek,

- Çeşitli tehditler için çeşitli savunma yöntemleri geliştirmek,

- Farklı alanlardan toplanmış olan bilgileri birleştirmek ve amaca uygun kullanım araçları oluşturmak için kullanmak,

- İşbirliği kurulan kurumlara siber güvenlik konusunda farkındalık eğitimleri vermek ve ihtiyaçları olan bilgilere ulaşmalarını sağlamak,

- İşbirliği yapılan kurumların uyması gereken standartları belirlemek,

- Ülke içinde ve dışında ortaklık içerisinde bulunulan kurum ve kuruluşlara teknik destekte bulunmak ve yeni teknolojiler geliştirmek,

[16] De facto: uygulamada geçerli, fiilen, gerçekte anlamlarında kullanılan Latince söz öbeği. https://dictionary.cambridge.org/tr/sözlük/ingilizce/de-facto

- Savunma kapasitesinin arttırılması için araştırmalar yürütülmesine önderlik etmek ve desteklemek

Bu yasa, daha sonra Kritik Bilgisayar Sistemleri adlı politikanın gelişmesine de temel hazırlamıştır. Yasanın geçtiği 2002 yılında, İsrail'de devlet ve özel sektör kontrolünde toplam on dokuz adet[17] kritik altyapı sistemi bulunmaktaydı. Altyapıların siber alana entegre edilmesiyle birlikte ortaya çıkan kırılganlıkların giderilmesi amacıyla, devlet politikalarının altyapı sistemlerini ve kullanıcılarını kapsayacak şekilde genişletilmesine ve derinleştirilmesine ihtiyaç duyulmuştur. Çeşitlenen güvenlik tehditleri İsrail'in güvenlik politikaları uygularken kapsayıcı yöntemlere başvurarak siber güvenlik kapasitesini arttırmasını gerektirmiştir. Paylaşılmış bir sorumluluk algısı güdümünde sistemlerin kimin kontrolünde olduğu fark etmeksizin hem kullanıcılar hem de sağlayıcılar ortak güvenlik politikaları uygulamıştır. Esasen sistemleri işletmekte olan özel şirketler sistemlerin finansman, koruma, bakım onarım, geliştirme, yedekleme ve kurtarma faaliyetlerini yürütürken, bir taraftan da gerçekleştirilen operasyonların bilgisini Milli Bilgi Güvenliği uzmanlarıyla paylaşarak siber güvenlik politikalarının daha dayanıklı hale getirilmesine katkı sağlamıştır. Yaklaşık on yıllık bir süreç içerisinde de facto olarak yerleşen bu sistem yasal sorumlulukları, işlevleri ve sorumlu devlet birimine sahip olan kompleks bir yapı halini almıştır. Ciddi tehdit içermediği düşünülen sivil sistemlerin birçoğu siber saldırılara maruz kalmaya başladığı zaman daha detaylı bir güvenlik sisteminin gerekliliğinin anlaşılmasıyla bu sistemler hatta bölümlere ayrılmış ve sorumluluk, yetkili birimler arasında dağıtılmıştır. 2010 yılında Başbakan Benjamin Natenyahu siber güvenliğin İsrail'in uluslararası statüsünü korumak için son derece gerekli olduğunu, bilgi teknolojilerinin geliştirilmesi ve siber alandaki güvenlik önlemlerinin hız kesmeden arttırılmasının; İsrail'in ekonomik ve ulusal dayanıklılık kapasitesini de iyileştireceğini, bu sayede açık demokratik ve bilgi temelli bir toplum oluşmasının önündeki engellerin kaldırılacağını belirtmiştir. Bunlara ek olarak, yürürlüğe konan politikalar sayesinde İsrail'in beş yıl içerisinde siber alanda öncü olan beş devletten biri olacağını belirterek araştırma ve geliştirme faaliyetlerine ağırlık verilmesine vesile olmuştur (Tabansky, 2013: 81).

2011 yılına gelindiğinde 80 uzman tarafından yürütülen projelerin kapsamı, süreci ve çıktılarının benzersiz oluşu da İsrail'in siber alanda sahip olduğu potansiyeli göstermek açısından önemli bir kanıt niteliğindedir. Teşkil edilen sekiz alt komitenin üyelerinde bakıldığında kıdemli karar vericilerin yanında, savunma AR-GE politikaları biriminden, Ekonomi Bakanlığından, Başbakanlık Ofisinden, Bilim ve Teknoloji Bakanlığından, İsrail Savunma Kuvvetleri Terörle Mücadele Merkezinden, Milli Bilgi Güvenliği Ajansından ve Atom Enerjisi Komisyonundan uzmanların olduğu görülmektedir. Bu

[17] 2011 yılına gelindiğinde devlet ve özel sektör kontrolündeki kritik altyapıların sayısı dört kattan fazla artış göstermiştir ve halka açık kaynaklarda seksen ve üzeri olarak belirtilmektedir (Cohen, Freilich, ve Siboni, 2015:6).

yapıya, ilerleyen dönemlerde ordudan, akademiden ve diğer bakanlık temsilcilerinden oluşan üyelerin de eklenerek ve altı aylık bir çalışma yürütülerek başbakana ve kabineye önerilerde bulunulduğu bilinmektedir (Government Decision 3611, 2011).

Yukarıda bahsedilen alt komitelerin siber güvenliğin ülke çapında iyileştirilmesi için uygulamaya koyduğu politikalar şu şekilde aşağıda sıralanmaktadır (Tabansky Y, 2013: 86):

- Disiplinler arası AR-GE projelerinin yürütülerek eğitim yoluyla toplum genelinde temel farkındalık arttırıcı politikaların geliştirilmesi,

- AR-GE departmanlarının altyapı, bilgi güvenliği ve güvenli kod gelişimi hususlarında çalışma yapmasını destekleyici ve akademik kurumların ülke içindeki üniversitelerde ve teknik kurumlarda insan kaynağı yetiştirmesini teşvik edici politikaların başlatılması,

- Siber saldırılardan korunmak amacıyla devlet genelinde savunma kalkanı yaratılması ve bu anlamda gizliliğin korunması,

- Milli siber güvenlik kapasitesinin geliştirilmesi için operasyonel yeteneklerin arttırılması amacıyla rutin ve acil durumları yönetecek hukuki ve finansal stratejilerin geliştirmesi,

- Kanunların ve teknik altyapının savunmayı güçlendirecek ölçekte geliştirilmesinin sağlanması,

- İsrail'e özgü teknolojilerin geliştirmesi için ülke içinde aktif özel şirketlerle işbirlikleri oluşturulması ve geliştirilmesi için teşviklerde bulunulması

Espiyonaj faaliyetleri yürütülerek kritik devlet bilgilerinin ele geçirilmesi siber saldırıların en tehlikeli formlarından biri olarak görülmektedir. İsrail'in bu faaliyetleri engellemek için yeterli kapasiteye sahip olduğu teorik olarak kabul edilse de uygulamaya koyulmaya çalışılan politikaların teknik ekipman ve personel anlamında yetersiz kaldığı görülmüştür (Tabansky, 2013: 87). Bu sorunun üstesinden gelmek amacıyla İsrail Savunma Kuvvetleri üniversiteler ile işbirikleri kurması alt komiteler tarafından önerilen çözümler arasında yer almıştır. Kritik altyapıların korunması amacıyla alınan kararlara ek olarak İsrail'in siber güvenlikteki normları hukuki ve siyasi boyutlarıyla ülke içinde ve dışında inşa etmesi önem taşımaktadır. Bu çerçevede sivil şirketlerin ve toplumun siber güvenlik konusunda bilgi sahibi olması ve temel korunma yöntemlerine aşina hale getirilmesi yönünde çalışmalar yapılmıştır. Alınan proaktif tedbirler sayesinde toplum, devletin gerisinden gelmek yerine bilgi çağına devlet ile eşzamanlı olarak ayak uydurmayı başarmıştır.

Kritik altyapıların yapılanmasına ve korunmasına etki eden faktörler sırasıyla, toplum davranışı, ideoloji, sosyal yapı, ekonomik kalkınma, piyasa stratejisi, rekabetçi iş ortamı ve siyasi sistemin yapısı olarak belirtilmektedir. Siber güvenlik teknik becerilerin yanı sıra sosyal, ekonomik ve siyasi yapılanmanın da yakından takibini gerektiren uzun vadeli bir süreç gerektirmektedir. 21. yüzyılda kapsayıcı ve dayanıklı bir güvenlik politikasına sahip

olmak; katılımcı, paylaşımcı ve yekinin resmi ve gayri resmi kurumlar arasında ortak dağıtıldığı yönetişim anlayışıyla paralellik göstermekte ve ortak çıkarların savunulduğu politikaların önemini ifade etmektedir.

3.1.2 İnsan Kaynağının Yetiştirilmesi

Bilişim teknolojilerinin büyüme hızı üstel olarak gerçekleşmekte ve bu hız beraberinde ekonomik ve sosyal değişimi getirmektedir. Modern toplum yapısı içerisinde iletişim ve bilgisayar teknolojisi sosyal yapının bir parçası haline gelmekte ve günlük hayatın vazgeçilmez bir parçası olmaktadır. Sonraki jenerasyonlar bilgi teknolojilerinin geliştiği dünya düzeninde yetişmekte ve teknolojiye bir önceki kuşaktan daha bağımlı olarak hayata atılmaktadırlar. Teknolojiye olan bağımlılık üzerinden şekillenen bu ortamda, siber alanın yarattığı kırılganlıklar ve toplum düzenini tehdit eden durumlar yükseliş göstermiştir. Toplumun ve devletin refahı için bilgi teknolojileri alanında kendini yetiştirmiş insan kaynağına, özel sektör girişimcilerine ve sivil toplum kuruluşlarına ihtiyaç duyulmaktadır (Tabansky ve Israel, 2015: 3).

İsrail yüksek teknoloji alanında küresel çaptaki liderler arasında bulunmaktadır. Bulunduğu konum itibariyle doğal kaynaklara erişimi sınırlı olan İsrail sahip olduğu insan kaynağına bilim, teknoloji ve eğitim alanları başta olmak üzere ciddi yatırımlar gerçekleştirerek bu açığını oldukça başarılı bir şekilde kapatmayı başarmıştır. Kuruluşunun hemen akabinde, ilk başbakan David Ben-Gurion Filistin'de yirminci yüzyılın başında kurulmuş olan Techion in Haifa ve Hebrew Üniversitelerine yatırımı öncelik haline getirerek son teknoloji araştırma merkezleri kurulmasını sağlamıştır. Buna ek olarak, İsrail Savunma Kuvvetleri'nin içerisinde şu an RAFAEL adıyla bilinen Bilim Komitesinin ilk atamalarını gerçekleştirmiştir (Haan, 2011: 312). Yürürlüğe konan politikaların yetiştirdiği nesillere ek olarak Sovyetler Birliği'nin dağılmasından hemen öncesinde ve sonrasında İsrail'e göç eden eğitimli nüfusun etkisi de azımsanmayacak derecede yüksektir[18].

İsrail Savunma Bakanlığı'nın sahip olduğu insan kaynağını yetiştirme, işe yerleştirme ve değerlendirme süreçleri de başarılı politikaların temel sebepleri arasında yer almaktadır. Öncelikle uzun eğitimler gerektiren siber güvenlik alanı ve benzeri pozisyonlar için düşünülen adayların zorunlu hizmet[19] süresinden daha fazla çalışmayı peşinen kabul etmesi gerekmektedir. Ayrıca her yıl lise mezunları arasından seçilen bin kişilik seçkin bir öğrenci grubuna zorunlu askeri hizmetlerini gerçekleştirmeden önce bilhassa bilim ve mühendislik alanlarında yükseköğrenime devam etmeleri için teşvikler verilmekte ve

[18] Resmi kaynaklara göre 1989 ve 1992 yılları arasında Sovyetler Birliği eğitimli 80.000 mühendis İsrail'e göç etmiştir (Tabansky ve Israel, 2015: 18).

[19] Zorunlu hizmet süresi İsrail Savunma Bakanlığı tarafından 3 yıl olarak belirlenmişse de seçkin adayların hizmetlerini 5 yıla kadar uzatmaları beklenmektedir. Pozisyonlarında kendilerini kanıtlayan ve yükselen adaylar ise 6 – 10 yıl arası görev yapmaktadır (Tabansky ve Israel, 2015:19).

eğitimleri tamamlanana kadar askeri hizmetleri ertelenmektedir (Tabansky ve Israel, 2015: 22). Örnek vermek gerekirse; 'Talpiot' adlı 40 haftalık elit eğitim programı 1979'da lise mezunu öğrencilere girişimcilik aşılamak ve teknolojik kabiliyet kazandırmak amacıyla yürürlüğe konmuştur. Nerdeyse tüm vatandaşların ilk işvereni doğrudan devlet olmaktadır. Yeteneklerine uygun pozisyonlarda devlete ve topluma katkı sağlayacakları görevler gerçekleştiren bireyler aidiyet duygusu yüksek vatandaşlar yaratmaktadır. Askeriyede görev yapan tüm bireyler yüksek teknoloji ile çalışma, sosyal bağlantı kurma, iş etiği, takım çalışması konularında tecrübeli olarak hayata atılmaktadır. Bu hummalı çalışmanın ardından Milli Siber Büro'nun kurulmasına oybirliğiyle 2011'in Ağustos ayında karar verilmiştir.

Milli Siber Büro 2011 yılında kurulmasının ardından, toplumda siber alandaki tehditler hususunda farkındalık yaratmak, hem iç hem de dış politikada işbirliğini desteklemek ve siber AR-GE endüstrisinin gelişimini sağlamak amacıyla birtakım önerilerde bulunmuştur. Bu öneriler hem siber alanda iş gücü yaratmak hem de toplumun genelinin siber alanda güvende olmasına yardımcı maddeler içermektedir (Singer ve Friedman, 2014: 239):

- Bilgi işlem, kod geliştirme, simülasyon ve istihbarat alanlarında ulusal bilgi merkezleri ve siber alan AR-GE tesislerinin kurulmasını teşvik etmek,

- İsrail'in sahip olduğu teknolojiler kapsamında milli siber güvenlik parametresini belirlemek ve ihtiyaç duyulan uygulamalar için politikalar geliştirecek insan kaynağı yetiştirmek,

- Siber alanda ihtiyaç duyulma ihtimali yüksek olan teçhizatların geliştirilmesini sağlamak,

- Finansal, ahlaki, hukuki politikalar geliştirerek hem savaş hem de barış zamanı karşılaşılması muhtemel tehditlere karşı hazırlıklı olmak,

- Teknik ve teknik olmayan hukuki maddelerin uluslararası antlaşmalar ile paralel hale getirilmesi için çalışmalar yürütmek,

- Askeriye, savunma endüstrisi, hükümet, sivil sanayi ve akademinin AR-GE konularında ortak projelerde bulunmasını sağlamak ve küçük çaplı anlaşmazlıkları gidermede arabuluculuk gerçekleştirmek,

- Mevcut siber tehditleri önleyici teknolojilerde AR-GE çözümleri sunmak ve ihracat kapasitesini bu yönde arttırmak,

Yeni nesilleri siber alan konusunda yetiştirmek amacıyla ise 'Magshimim' adında bir program yürütülmektedir. Bütçesi Savunma Bakanlığı ve STK'lar tarafından karşılanan bu programın amacı 10 – 12. sınıf arası seçkin öğrencilere siber alanda aktif olmalarını sağlayan yetenekler kazandırılmaktadır. Savunma Bakanlığından ve özel sektörden danışmanlar aracılığıyla yürütülen programda öğrenciler bilgisayarlar, ağ yapılanmaları,

bilgisayar dilleri, algoritma yaratma, yaratıcı düşünme konularında eğitimler almaktadır (Raska, 2015: 9). İnsan kaynağı yaratmak için uygulamaya konan bir diğer eğitim programı Ulusal Siber Güvenlik Eğitimi Girişimi olarak bilinmektedir. Üniversite öğrencilerine on haftalık stajlar aracılığıyla siber güvenlik eğitimi verilmesi ve mezuniyet sonrasında geniş iş imkânları sağlanmasını kapsamaktadır. Hem özel sektörün hem de Savunma Bakanlığının benzer türlerde birçok girişimi bulunmaktadır. Dahası, mezunların tamamı siber güvenlik alanında çalışmayı seçmek zorunda bırakılmamaktadır. Eğitim programlarının yanı sıra siber alanda yetenekli gençleri ortaya çıkarmak için ödüllü yarışmalar düzenlenmekte ve burslu eğitimler akabinde teklif edilen profesyonel kariyer fırsatları sayesinde oldukça başarılı politikalar izlenmektedir.

3.1.3 Çok Boyutlu ve Entegre Politikaların Şekillendirilmesi

Milli Siber Büro'nun kuruluşundan itibaren İsrail'in siber güvenlik politikalarının başarıya ulaşması için iki ana varsayım öne çıkmaktadır. İlk olarak, siber alanın askeri, siyasi, ekonomik ve sosyal hayat ile bütünleşmesi sonucunda devleti oluşturan tüm unsurların da eşit derecede tedbirlerle donatılması gerekmektedir. Sınırları koruyan ordular, uluslararası barış antlaşmaları ve ülke içinde mevcut polis gücü siber saldırılar karşısında etkisiz kalmaktadır. Fiziksel savunma stratejilerinin devre dışı kaldığı bu tip durumlarda, kritik altyapıların zarara uğramaması için çeşitli stratejilerin geliştirilmesi uygun görülmüştür. İkinci varsayım ise, mevcut sivil/askeri siber güvenlik sistemlerinin ve örgütsel yapılanmaların siber alanın gelişim hızına yetişemediği ve daha kapsamlı güvenlik stratejilerinin uygulanması gerektiğine karar verilmiştir. İsrail'in siber güvenlik stratejileri, mevcut tehditlere karşı tedbirler alınmasını ve bunun yanında risk unsurlarının da tehditlere dönüşmesini engelleyecek politikalar edinilmesini amaçlamaktadır. Bilhassa finans, enerji ve ulaşım sektörlerinin yürüttüğü operasyonlar, telekomünikasyon teknolojilerine bağımlı olarak işlemektedir. Kritik altyapılara ek olarak bireylerin ve özel sektörün işlevsel devamlılığının siber saldırılar tarafından zarara uğratılması doğrudan milli güvenliğe tehdit oluşturmaktadır (Raska, 2015: 5).

Askeri güvenliği arttırmak amacıyla uygulanan politikalar son teknoloji siber savunma sistemlerine bağımlı operasyonlar yürütmek yerine disiplinler arası yöntemler kullanarak çok boyutlu bir milli siber ekosistem yaratmak amacıyla yürütülmektedir. Savunma stratejilerinde bilişim sistemlerinin önemi oldukça yüksek olsa da yetersiz kalmaktadır. Zira gerekli teçhizat, zaman ve teknik bilgi sağlandığında ele geçirilemeyecek bir sistem bulunmamaktadır. Ülke içinde bulunan araştırma laboratuvarları, askeri istihbarat birimleri, Milli Siber Büro ve özel sektörden girişimci teknoloji firmaları çok katmanlı bir siber güvenlik stratejisi oluşturmak amacıyla entegre olabilmektedir. Yüksek teknoloji kullanılan otomatik sistemlerin yanı sıra, kıdemli teknik personele, istihbarata, erken uyarı sistemine, aktif ve pasif savunma stratejileri uygulayabilme kabiliyetlerine sahip sivil/askeri yapılanmalar yüksek güvenlik imkânı sunmaktadır. Siber alanda sahip olunan yeteneğin, defansif politikaların yanı sıra saldırgan politikaların da boyutunun ve etkisinin

de ne ölçüde arttırılabileceğine örnek olarak 2007'de İsrail'in Suriye'de Deir ez-Zor bölgesinde bulunan sözde nükleer tesise gerçekleştirilen siber müdahale ve ardından gerçekleştirilen hava saldırısı ile meydana gelen 'Orkide Operasyonu' verilebilmektedir. Saldırının yapıldığı, 2018'e kadar İsrail otoriteleri tarafından kabul edilmemiştir. Hava savunma sistemlerinin siber saldırılar aracılığıyla etkisiz hale getirilmesi sonucu hedef savunmasız hale getirilmiş ve hava saldırısı gerçekleştirilmiştir. Bu örnek gelecek savaşların akıbeti hakkında oldukça belirgin tahminler yürütülmesine imkân tanımaktadır. İkinci bir örnek olarak da 2010'da İran'ın uranyum zenginleştirme tesislerinde bulunan santrifüjlerin Stuxnet virüsüyle enfekte edilmesi verilebilmektedir. Her ne kadar resmi olarak İsrail tarafından üstlenilmemiş olsa da uluslararası basın İsrail/ABD ortak çalışması olduğu sonucuna varmıştır. Gerçekleştirilen saldırı İran'ın nükleer çalışmalarına zarar verdiği gibi, Hiroşima benzeri bir felaket yaşanma ihtimalini de beraberinde getirmiştir. Siber alanın askeri yöntemlere entegre edilmesiyle, siber saldırılar bir kuvvet çarpanı olarak kullanılmakta ve fiziksel saldırıların etkisi arttırılabilmektedir. Geliştirilen yeni hibrit savaş yöntemlerinin geleneksel savaş stratejilerine kıyasla oldukça yüksek yıkım kapasitesine sahip olacağı öngörülmektedir. Hibrit saldırıların etkisinin ne ölçüde olabileceği hakkında Robert Raska siber alanın geleneksel savaş yöntemlerini nasıl dönüştürme potansiyeline sahip olduğunu üç maddede açıklamaktadır (Raska, 2015: 6):

- Muhtemel tehdit unsurlarının siber alanın mümkün kıldığı uydular gibi sofistike araçlarla belirlenmesi ve istihbarat toplanılması,

- Saldırı veya savunma sistemlerine gerçek zamanlı müdahaleler gerçekleştirme esnasında karşılaşılma potansiyeli olan engellerin ortadan kaldırılması,

- Geleneksel kara, hava, deniz ve hava operasyonlarının siber teknolojiler ile birleştirilerek yıkıcılık kapasitesinin arttırılması

Siber saldırıların çıkış noktalarının belirlenememesi, faillerin gizli kalabilmesini mümkün kılmakta ve karşı saldırı ihtimallerini ortadan kaldırmaktadır. İsrail'in bilgi ve iletişim teknolojilerine yıllar içerisinde yapmış olduğu yatırımlar ofansif ve defansif amaçlarla kullanılabilecek yüksek teknoloji ürünü teçhizatlar, iyi yetişmiş uzman çalışanlar, kompleks örgütsel yapılanma, bilinçli ve aidiyet duygusu yüksek toplum ve gelişmiş bir sanayi yaratmıştır.

İsrail uzun yıllar devam eden politikalarının bir sonucu olarak siber alana entegre bir devlet haline gelmiştir. Bilişim teknolojilerinin hayatın her alanında kullanılmaya başlanmasının bir sonucu olarak 2002'de yürürlüğe konan B/84 yasası ile ülke dâhilinde siber alanda aktif operasyon yürüten birey, özel şirket, STK gibi tüm aktörlerden zorunlu bilgi paylaşımı talep edilmiştir. Paylaşılan bilgiler analistler tarafından işlenmiş ve açıkları tespit edilen sistemlerin güvenli hale getirilmesi sağlanmıştır. Bu operasyonu

İsrail Savunma Kuvvetleri'ne bağlı Ulusal İstihbarat ve Güvenlik Ajansı[20] (NISA) yürütmüş ancak iyileştirme çalışmaları yapmak tek başına yetersiz kalmıştır. Dönemin başbakanı Natenyahu, daha proaktif önlemlerin gerekli olduğu kanaatine varmış ve siber alanda gerekli tedbirlerin alınmasının milli güvenlik açısından hayati önem taşıdığını öngören İsrail, 2010 yılında Milli Siber Girişimi[21] (NSI) başlatarak operasyonel bir çerçeve oluşturmuştur. İsrail Savunma Kuvvetleri de bu tarihe kadar siber güvenlik politikasını, de facto olarak şekillendirmiştir (Libel, 2016: 143).

Başbakan Natenyahu İsrail Milli Siber Büro'yu[22] (INCB) kurarak devlete ait olmayan tüm ticari ve ticari olmayan işletmelerin de milli siber güvenlik politikasının bir parçası olması gerektiğini belirtmiştir. Siber güvenlik politikalarının askeri anlayışın yanı sıra siyasi, ekonomik, bilimsel kurumlardan oluşan temsilciler tarafından ortak çıkar esasına dayanarak yönetilmesi sonucu İsrail'in dünyanın en büyük ilk beş siber gücünden biri olmasıyla sonuçlanan oldukça başarılı eğitim ve AR-GE projeleri yürütülmüştür. Başbakan Natenyahu tarafından tüm ilgili devlet birimlerinden danışmanlar atanması, siber güvenliğe verilen önemi göstermektedir. 2015 yılına kadar kurulan ve yönetilen siber güvenlik birimleri meclisten geçirilen yasalar doğrultusunda oluşturulmakta ve yönetilmekteydi. 2015 yılında meclisten geçen 2443 numaralı yasa doğrultusunda Milli Siber Güvenlik Otoritesi[23] (NCSA) oluşturularak özel sektörden kaynaklı oluşabilecek kırılganlıkların giderilmesi amaçlanmıştır. Kendi yasal otoritesine sahip olan NCSA kendinden önceki kurumlara kıyasla daha kapsamlı bir yapı olarak kurulmuştur. INCB ile işbirliği içerisinde çalışan operasyonel bir ajans olmasının yanı sıra NSCA İsrail'in uluslararası olarak siber alandaki liderlik iddiasına paralel yönde politikalar inşa etmekte ve sahip olduğu yasal otorite sayesinde koymuş olduğu kurallar doğrultusunda siber alan için uluslararası siber güvenlik hukuku oluşturma çalışmalarında bulunmaktadır. INCB'nin görevleri şu şekilde sıralanmaktadır (Tabansky ve Israel, 2015: 58):

- Başbakana, hükümete ve komitelerine siber güvenlik konusunda danışmanlık hizmeti vermek,

- Milli siber güvenlik politikasının oluşturulmasında yasama işlemlerini başlatmak, hükümet politikasını ilan etmek, uygulama sürecini yakından takip ederek denetlemek,

- Mevcut kaynaklardan istihbarat toplayarak siber tehditlerin belirlenmesini sağlamak,

- Siber alanın daha etkili kullanabilmesi kapsamında yeni eğitim politikaları geliştirmek, özel sektörün geliştirilmesi amacıyla hem devlet hem de sivil AR-GE projelerine teşvikler vermek,

[20] National Intelligence and Security Agency (NISA)
[21] National Cyber Initiative(NCI)
[22] Israel National Cyber Bureau (INCB)
[23] National Cyber Security Authority (NCSA)

- Siber alanda mevcut olan tehditler konusunda toplumda farkındalık oluşturmak, düzenli bilgi paylaşımı yapmak, uyarılar ve direktifler yayınlamak,

- Siber güvenlik konusunda ulusal ve uluslararası işbirliği projelerini desteklemek,

INCB'nin üzerine düşen görevleri gerçekleştirmesi için yıllık 130 milyon dolarlık bir bütçe ayrılmıştır (Tabansky, 2013: 85). Siber güvenlik politikalarının finanse edilebilmesi için gereken bütçe İsrail'in ihracat odaklı sektörlerinden sağlanmaktadır. İsrail ilk on yıllarında gerçekleştirmiş olduğu uygulamalı tarım çalışmaları sonucunda zirai endüstrisini geliştirmiş ve bu sayede siber güvenlik yatırımları için gerekli finansman elde edilebilmiştir. Büyüyen ekonominin de etkisiyle daha önce askeri teknolojilerini ihraç eden İsrail, 1960'lardan itibaren askeri teknolojileri kendisi üretmek için yatırımlara başlamıştır. Askeri teknolojilerin üretimi için ayrılan bütçe 1966'da GSMH'nin %10,4'ünü kapsarken, 1980'de %25,4'e ulaşmıştır. 1984'te ise askeri endüstri 25.000'i bilim insanı, mühendis ve teknisyen olmak üzere 65.000 kişiye istihdam sağlamıştır (Haan, 2011: 308). Ekonomik büyümenin getirdiği bir diğer fayda ise bilhassa 1990'lardan başlayarak ihraç edilen ürünlerin artık tarım ürünlerine ek olarak yüksek teknolojili ürünleri de içermesi olarak görülmektedir. Ayrıca büyüyen ekonomi ve artan teknolojik kapasite dünya devi şirketlerin İsrail'de ofisler açmasını ve binlerce vatandaşa teknoloji alanında istihdam yaratılmasını sağlamıştır. INCB'nin kurulmasından yaklaşık iki yıl sonra siber güvenlik alanında çalışan özel şirketlerin sayısı 50'den 220'ye yükselmiştir. Kurulmuş olan yerel işletmelerin yanı sıra dış yatırımlar aracılığıyla İsrail'de 20 AR-GE merkezi kurulmuştur. Büyük şirketlerin kendi topraklarında aktif olmasının yarattığı imkân ile INCB uluslararası siber güvenlik ve siber teknoloji konferansları düzenleyerek İsrail menşeli şirketlerin dünya devleri ile aynı platformda yer aldığını dünyaya göstermiştir (Tabansky ve Israel, 2015: 53).

2017 yılında mevcut INCB ve NCSA birleştirilerek Ulusal Siber Direktörlüğü (INCD) kurulmuş ve INCB başkanı Direktörlüğün başına atanmıştır. Önceki süreçte NCSA siber koruma eylemlerinin gerçekleştiği birim, INCB ise siber politikaların uygulanması amacıyla personel yetiştirme, teknik kapasitenin arttırılması ve siber güvenlik uygulamalarından sorumlu birim olarak hizmet vermiştir. INCD'nin kurulmasıyla birlikte siber güvenlik politikaları hem askeri hem de sivil politikaların geliştirilmesinde ana merci olmuş ve siber güvenlik kapasitesi arttırılmıştır. Bu nokta da İsrail'in devlet politikaları çerçevesinde siber güvenliği ne derece kapsamlı ve çok boyutlu olarak ele aldığını ve bu yönde kurumsallaşmaya gittiğini göstermektedir (Tabansky ve Israel, 2015: 28).

Tablo 3. OECD Ülkelerinde Gayrisafi Yurtiçi Hasılanın Sivil AR-GE Çalışmalarına Aktarılması

Location	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Israel	3.933	4.185	4.131	3.893	3.873	4.048	4.141	4.422	4.342	4.133	3.935	4.015	4.161	4.096	4.174	4.265	4.512	4.816	4.941
Korea	2.125	2.279	2.208	2.277	2.442	2.523	2.719	2.873	2.989	3.147	3.316	3.592	3.850	3.951	4.078	3.978	3.987	4.292	4.528
Sweden	..	3.896	..	3.602	3.383	3.381	3.499	3.256	3.485	3.406	3.171	3.195	3.239	3.273	3.111	3.228	3.247	3.366	3.309
Japan	2.906	2.972	3.014	3.043	3.030	3.181	3.278	3.340	3.337	3.231	3.137	3.245	3.209	3.315	3.400	3.282	3.155	3.213	3.264
Austria	1.886	1.992	2.066	2.175	2.166	2.373	2.359	2.418	2.569	2.597	2.726	2.669	2.915	2.955	3.084	3.050	3.117	3.049	3.175
Germany	2.410	2.404	2.436	2.475	2.435	2.442	2.472	2.460	2.615	2.743	2.730	2.806	2.882	2.836	2.878	2.930	2.941	3.068	3.133
Denmark	..	2.325	2.441	2.511	2.419	2.393	2.403	2.515	2.773	3.055	2.917	2.945	2.981	2.970	2.914	3.055	3.093	3.050	3.033
United States	2.629	2.648	2.559	2.565	2.502	2.517	2.558	2.632	2.768	2.813	2.735	2.765	2.682	2.710	2.718	2.717	2.760	2.813	2.826
Belgium	1.936	2.033	1.903	1.841	1.821	1.791	1.823	1.850	1.937	1.999	2.062	2.173	2.281	2.331	2.370	2.428	2.522	2.659	2.764
Finland	3.241	3.194	3.253	3.298	3.309	3.324	3.332	3.337	3.537	3.734	3.705	3.618	3.398	3.271	3.148	2.870	2.725	2.734	2.746
France	2.093	2.138	2.174	2.120	2.095	2.052	2.051	2.025	2.061	2.212	2.179	2.192	2.227	2.237	2.276	2.267	2.222	2.206	2.200
Netherlands	1.790	1.796	1.745	1.784	1.789	1.774	1.741	1.670	1.623	1.666	1.704	1.881	1.916	1.930	1.976	1.985	1.997	1.983	2.164
Norway	..	1.563	1.630	1.680	1.544	1.482	1.455	1.565	1.554	1.725	1.650	1.627	1.621	1.652	1.715	1.935	2.045	2.099	2.073
Iceland	2.578	2.850	2.828	2.709	..	2.686	2.894	2.549	2.487	2.595	..	2.414	..	1.702	1.948	2.197	2.128	2.104	2.030
Slovenia	1.360	1.468	1.443	1.248	1.370	1.418	1.537	1.427	1.627	1.812	2.051	2.413	2.561	2.565	2.365	2.196	2.011	1.866	1.950
Czech Republic	1.113	1.103	1.102	1.147	1.146	1.168	1.232	1.302	1.239	1.294	1.337	1.556	1.782	1.900	1.973	1.929	1.680	1.791	1.930
United Kingdom	1.617	1.605	1.615	1.582	1.534	1.553	1.573	1.613	1.613	1.671	1.646	1.650	1.577	1.620	1.643	1.650	1.660	1.646	1.706
Canada	1.858	2.021	1.972	1.968	1.997	1.971	1.943	1.904	1.856	1.917	1.825	1.787	1.772	1.705	1.714	1.693	1.729	1.669	1.563

Kaynak: OECD. (2020). *Gross domestic spending on RveD Total % of GDP, 2000-2019.* OECD Data: https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm adresinden alındı.

Tablo 3'te verilmiş olan 2000-2018 yılları arası GSYİH'nin sivil AR-GE çalışmalarına aktarıldığı yüzdelik dilim gösterilmektedir. Görüldüğü üzere 18 yıllık süre içerisinde İsrail OECD'ye üye devletler arasında GSYİH'sinden sivil AR-GE çalışmalarına en fazla miktarı aktarmış olan devlet olarak görülmektedir. Yüksek teknolojili ürünleri üretme ve ihraç etme kapasitesine sahip olan İsrail kazanmakta olduğu yıllık kârın belli bir bölümünü AR-GE çalışmalarına her yıl arttırarak aktarmakta ve bu sayede her geçen yıl son teknoloji alanında üretim ve ihracat kapasitesini yükseltmektedir. Bu noktada siber alan ve bu alandaki gelişmeler konusunda İsrail'in ön saflarda yer almasına ciddi katkı sunmaktadır.

Günlük hayatın her alanı teknolojik araçlar ile donatılmış ve birçoğu siber alana bağımlı hale gelmiştir. Suriye ve İran'ın nükleer tesislerine yönelik olan gerçekleştirilmiş siber saldırılar da tehditlerin ne derece ciddi ölçekte etki yaratabileceğini göstererek, gerek tehditlerin gerekse alınması gereken tedbirlerin yapısının ne ölçüde çeşitlendiğini ve farklılaştığını gösterir niteliktedir.

İsrail'in güvenlik algısının önemli bir boyutunu oluşturan siber güvenliğin, çok taraflı ve çok boyutlu ele alınması kapsamında toplumun siber güvenlik alanında bilgi sahibi olması ve farkındalık inşa edilmesi gittikçe önem kazanmıştır. Bu anlamda bütüncül bir yaklaşımla, NISA, NSI ve INCB'nin çalışmaları siber güvenlik politikalarının askeri, ekonomik ve siyasi hayata entegre edilmesi sürecinde etkili olmuştur. Uzun dönemli ve entegre politikalar kapsamında siber alanın yarattığı tehditlere yönelik olarak farkındalık oluşturma çabaları toplumun çeşitli kesimlerine yıllara yayılmış olarak verilmeye çalışılmış ve bilhassa lise, üniversite ve zorunlu askerlik eğitimi boyunca konu üzerinde durulmuştur (Tabansky ve Israel, 2015: 19). Günümüz itibariyle, siber alanda aktif operasyon yürüten özel şirketler ve kamu-özel sektör işbirlikleri INCB tarafından düzenli olarak teftiş edilmekte ve sistem açıkları belirlenmektedir. Uzun dönemli devlet politikaları sonucunda oluşan siber kültür epistemik topluluklar tarafından ulusal politikalara entegre edilerek günümüz İsrail toplumunun güvenliğine katkı sağlayan süreci başarılı bir şekilde yönetmiştir (Libel, 2016: 138).

3.1.4 Özel Sektör ile İşbirliklerinin Çeşitlendirilmesi

Kritik altyapı sistemlerinin korunması; hizmet sağlanan sistemin işleyişini sağlayan donanım ve yazılımın, içerdiği bilginin ve kullanan personelin korunması anlamına gelmektedir. İsrail'de mevcut tüm kamu özel sektör işbirlikleri bu bağlamda 2010'a kadar düzenli olarak diğer tüm özel sektör kuruluşları gibi NISA yetkililerine rapor vermiştir (Limba, Pleta, Agafonov, ve Damkus, 2017: 560). Ancak, İsrail Savunma Kuvvetleri'ne bağlı kurumların özel sektör ve kamu özel sektör işbirliklerini denetlemesi zaman içerisinde yasal ve etik sorunlar doğurmaya başlamıştır (Cavelty, 2013: 118). INCB'nin kurulmasını izleyen süreçte mevcut özel sektör ve kamu özel sektör işbirliklerinin idaresinde bulunan altyapıların siber güvenlik politikalarının oluşturulması hem işbirlikçi kurumların hem de INCB'den temsilcilerin ortak katılımıyla gerçekleşmektedir. Özel sektörün ve devletin bu tip bir işbirliği içinde bulunması, politikaların daha kapsayıcı bir çerçevede geliştirilmesi açısından anlamlıdır. Kamu-özel sektör işbirliklerinin tanzim etme aşamasından ileriye taşınmamasının en temel sebeplerinden biri, İsrail'in içinde bulunduğu coğrafyanın haiz olduğu tehdit unsurlarıdır. Geçmişte ve günümüzde sahip olunan risk unsurlarının çeşitliliği İsrail'in tedbiri elden bırakmamasını gerektirmiştir. Başlangıç projeleri olarak görülen kamu-özel sektör işbirlikleri İsrail'de yaklaşık son 40 yıldır aktif bir şekilde uygulanmaktadır. Tehdit unsurlarının azalmaya başlayabileceği noktada devletin, altyapıları özel sektörün kontrolüne devrederek daha az müdahaleci bir sistemin oluşturulabileceği öngörülmektedir.

Kamu özel sektör işbirlikleri İsrail'de 1980'lerden itibaren uygulanmaya başlanmıştır. Uygulanan projeler genellikle proje bazlı gerçekleştirilmiş kısa süreli çalışmalar olarak görülmektedir ve haklarında çok fazla bilgiye rastlanmamaktadır. Diğer yandan yerel anlamda ilk kamu özel sektör işbirlikleri 1990'lardan itibaren bilhassa inşaat sektöründe yerel yönetimler ve özel sektör arasında görülmeye başlanmıştır. 1990'ların sonunda

devletin bütçe ayıramadığı birçok şehrin kanalizasyon arıtma tesisleri bu şekilde inşa edilmiştir. İnşa edilen altyapıların işletmesi özel sektörün elinde olup, denetimi devlet tarafından tanzim etme[24] yöntemi günümüz itibariyle siber alan çerçevesinde özel sektör ile yenilikçi çalışmalar yapmak ve siber güvenlik kapasitesini arttırmak amacıyla gerçekleştirilmektedir. Örneklendirmek gerekirse; CyberSpark girişimi 2017 yılında INCB, Ben Gurion Üniversitesi ve siber güvenlik endüstrisinde lider konumdaki şirketlerin ortak çabalarıyla başlatılmıştır. Bilgisayar laboratuvarları kurulması ve gerekli tesislerin yapılandırılma süreçleri INCB'nin belirlediği standartlar doğrultusunda, akademisyenlerin teorik bilgileri ve endüstri temsilcilerinin tecrübeleri birleştirilerek gerçekleştirilmiş ve çalışmalar başlatılmıştır. Daha dayanıklı siber güvenlik politikaları geliştirmek amacıyla ulusal ve uluslararası paydaşlar ile çeşitli çalışmalar yürütülmektedir (CyberSpark, 2017). Siber Güvenlik Çalıştayları yıllık olarak düzenlenmekte ve yapılan çalışmalar şeffaf bir biçimde paylaşılmaktadır. Hatta siber güvenlik alanında Güney Kore, Almanya gibi öncü ülkeler ile ortak projeler gerçekleştirilmekte ve siber güvenlik alanında yenilikçi çalışmalara imza atılmaktadır (Ben Gurion University of the Negev, 2017). Burada kullanılan tanzim etme yöntemi siber güvenlik açısından bilginin paydaşlarla paylaşılması ve kırılganlıklara karşı ortak tedbirler geliştirilmesi anlamında önemli bir yöntem olarak öne çıkmaktadır. Zira tanzim etme yöntemi kapsamında meydana gelen veya girişilen siber saldırılarla ilgili bilgilerin kamuoyuyla paylaşımına önem verilmekte geleceğe yönelik tedbirlerin alınması konusunda üzerinde hassasiyetle durulmaktadır.

İçişleri Bakanlığının özel sektöre olan güvenini sağlama ve işbirliklerini bir üst aşamaya taşıma anlamında bu süreç önem taşımaktadır. İlerleyen süreçte su ve kanalizasyon hizmetlerine ek olarak; şifalı su tesisleri, yüzme havuzları ve eğlence tesisleri gibi sosyal hizmetler kamu-özel sektör işbirlikleri tarafından inşa edilmiştir. 2000'lerin ilk on yılında Tel Aviv ve Haifa şehirlerinde atık yönetimi ve kentsel dönüşüm (alışveriş merkezleri ve lojistik parkları) projelerinin ardından hafif raylı sistem ilk kez merkezi hükümet ile işbirliği yürütülerek inşa edilmiştir. 2008-2012 ekonomik krizi hafif raylı sistem projesini belli bir süre sekteye uğratmış ve devlet desteği ile tamamlanabilmiştir (Razin ve Hazan, 2013: 84).

Son 20 yıldır gerçekleştirilen kamu-özel sektör işbirlikleri ulaşım[25], enerji[26], su[27] ve inşaat[28] sektörlerinde yoğunlaşmıştır. Buna rağmen OECD ülkelerinin genelinde altyapı

[24] Şekil 3

[25]Route 431 (2006-2009), Fast lane to Tel Aviv (2007-2011), Highway 6 and Segments 3+7 (1999-2000)(2015-2019), (https://mof.gov.il/en/InternationalAffairs/InfrastructuresAndProjects/Projects/Documents/PPP_ProjectsInIsrael-en.pdf)

[26] Ibid. Ashalim thermo-solar facility Plot A-B (2014-2019), Ashalim PV 1 (2013-2017)

[27] Ibid. Ashkelion (2003-2005), Palmahim, Hadera (2005-2007), Sorek (2011-2013), Ashdod (2011-2015) Desalination Facilities

sistemlerinin %71'inin tüm süreçleri özel sektör tarafından gerçekleştirilmekteyken İsrail 2017 yılında bu oranı ancak %50'ye çıkarabilmiştir (Israel Ministry of Finance, 2019: 2).

Devlet destekli olarak gelişen özel sektör ve yetişen teknik personel İsrail'in gelişmekte olan bir ekonomiye sahip olduğu yıllarda dahi yıllık bütçenin büyük bir kısmının bilimsel yatırımlara aktarılmasının bir ürünü olarak görülmektedir. Bu sayede toplum genelinde ortaya çıkan karakteristik bir siber kültür, yetişmiş yetenekli personel ve son teknoloji teçhizat geliştirme kapasitesine sahip bir özel sektör yaratılabilmiştir. 2010 yılındaki OECD verilerine göre İsrail, Amerika ve Japonya'dan sonra dünyada en çok patentli ürüne sahip ülke olarak kayıtlara geçmiştir (Haan, 2011: 312). İsrail'in teknolojide bu denli yenilikçi olabilmesinin temel sebeplerinden biri tüm üniversitelerde gerçekleştirilen araştırmaların sonuçlarının aktif bir şekilde özel sektöre transfer edilmesinden kaynaklanmaktadır. Araştırma sonuçlarının şeffaf tutulması ile amaçlanan, şirketlerde staj yükümlülüklerine devam eden öğrencilerin, danışmanlık hizmeti veren akademisyenlerin ve çalışanların yeni gelişmelerden haberdar olmasının sağlanması ve kırılganlıkların azaltılması olarak planlanmıştır. Amaçlanan diğer çıktılar da şu şekilde sıralanmaktadır (Tabansky, 2013: 87):

- Üniversitelerin ders konuları ile özel sektörün iş alanının paralelliğinin sağlanması, (bilginin pratik kullanımı)

- Yıllık iş planlamasında rekabetin arttırılması,

- Lisans öğrencileri için bir nevi araştırma laboratuvarı etkisi yaratılması ve yaratıcılığın güçlendirmesi,

- Girişim kulüplerinin oluşturulması,

- Mezunlara yönelik hayat boyu faydalanma programları sayesinde girişimci sayısının ve niteliğinin arttırılmasıdır.

İsrail ölçeğimde, bilim komitesinden ayrılan bilim insanları zaman içerisinde kamu özel sektör işbirliklerinin varlığı için gerekli olan yerel siber güvenlik şirketlerini kurmuşlardır. Bilim komitesinde yetişmiş olan bilim insanları ve kamu özel sektör işbirliklerinin varlığı için gerekli olan yerel siber güvenlik şirketlerini kurmuşlarıdır. İsrail ölçeğinde bilim komitesinde yetişmiş olan bilim insanları zaman içerisinde kamu kadrolarından ayrılarak yerel teknoloji şirketleri kurmuşlar ve kamu özel sektör işbirliklerinin oluşturulabilmesi için yeterli siber kültür altyapısının yerleşmesi için farkındalık ve girişimcilik alanında çeşitli seminerler düzenlemişlerdir.

Ibid. National Police Academy (2012-2015), Ashdod Med Center (2012-2017), Teleprocessing Complex in Be'er Sheva (2018- p.e 2023)

[28] Ibid. National Police Academy (2012-2015), Ashdod Med Center (2012-2017), Teleprocessing Complex in Be'er Sheva (2018- p.e 2023)

Ülke içerisinde büyüyen bilişim sektörü siber güvenlik politikalarının kamu-özel sektör işbirlikleri kapsamında oluşturularak uygulanmasına imkân sağlayarak devlet-özel sektör arasındaki güven bağını güçlendirmiştir. Buna ek olarak toplum genelinde, devlet kurumlarında, özel şirket veri tabanlarında ve bilhassa kamu özel sektör işbirlikleri platformlarında ticari şifreleme programlarına ağırlık verilmesinin gerekliliği INCB tarafından vurgulanmıştır (Tabansky ve Israel, 2015: 22).

İnternet güvenliği alanında İsrail'in siber tehditler konusunda farkındalık sahibi olması ve kötü niyetli kullanıcıların tuzaklarına daha az düşmelerini sağlamak amacıyla 1994 yılında İsrail İnternet Birliği (IIA) bağımsız bir yapı olarak kurulmuştur. İsrail'in araştırma, eğitim, sosyal ve internet altyapılarının korunması için politikalar yürüten kuruluş, siber alanın aktif, istikrarlı ve erişilebilir kalması amacıyla güvenlik ve gizlilik konularında farkındalık seminerleri gerçekleştirmekte ve kendisi gibi kâr amaçlı olmayan kuruluşlar ile işbirlikleri yapmaktadır. IIA çevrimiçi sansür, siber-zorbalık gibi alanlarda projeler yürütmekte ve INCD'nin yıllık olarak yayınlamakta olduğu siber güvenlik metodolojileri kapsamında politikalarını yürütmektedir (INCD, 2018: 2).

3.2 Yeni Zelanda Örneği

1852 Anayasası ile İngiltere'nin hâkimiyetinden çıkan Yeni Zelanda teknolojik gelişmeleri yakından takip etmekte ve siber güvenlik anlamında önemli çabalar ortaya koymaktadır. Yeni Zelanda siber anlamda küreselleşmiş ve internete bağlanmış dünyanın imkânlarından yararlanarak, küçük bir devlet olmanın ve coğrafi konumunun dezavantajlarını bir anlamda ortadan kaldırmaktadır. Kritik altyapıların neredeyse tamamının özel sektör kontrolünde olduğu Yeni Zelanda kapsayıcı bir anlayışıyla siber güvenlik politikalarını şekillendirmektedir.

Teknolojik gelişmelerin ve küresel ticaretin küreselleşmeyi bir üst seviyeye taşıması, devletleri karşılıklı bağımlı hale getirmekle kalmamış aynı zamanda devlet, birey ve özel sektör üçgeninin de karşılıklı bağımlı hale getirerek güvenlik anlayışını dönüştürmüştür. Küreselleşmiş ve internete bağlanmış dünya Yeni Zelanda için küçük devlet olmanın ve coğrafi konumunun dezavantajlarını ortadan kaldıran etkenlerden biri olarak görülmektedir. Buna ek olarak, kritik altyapıların neredeyse tamamının özel sektör kontrolünde olduğu da hesaba katıldığı zaman güvenlik anlayışının kapsayıcı bir nitelik içermesi gerektiği sonucuna varılmaktadır. Yeni Zelanda'nın bulunduğu konum itibariyle özel sektör ve devlet kurumları operasyonlarının büyük bir kısmını siber alan üzerinden yürütmektedir. İnternet ve diğer dijital iletişim yöntemleri Yeni Zelanda'nın dünyanın geri kalanı ile diplomatik ve ticari ilişkiler yürütebilmesine olanak tanımaktadır. Devlet kurumları, bankacılık, finans, iletişim, ulaşım ve enerji sektörlerinden oluşan altyapı sağlayıcıları operasyonlarını günden güne siber alan üzerinden yürütmekte kapasitelerini arttırmaktadır. Resmi ve ticari işlemlerin siber alana taşınması hem insan kaynağı

ihtiyacının azaltılmasını, hem de bürokratik süreçlerin kısaltılmasını sağlamaktadır (Gordon, 2014: 31) .

1956 yılında kurulmuş olan Yeni Zelanda Güvenlik İstihbaratı Servisi[29] (SIS) gerçekleştirilen siber saldırıların 21. yüzyılın ikinci on yılı itibariyle arttığını belirtmektedir. 2011 yılında hükümete ve kritik altyapılara 90 adet saldırı düzenlenirken, bu sayı 2012 yılında 134'e yükselmiştir. Gerçekleştirilen saldırıların %60'ının denizaşırı lokasyonlardan kaynaklandığının tespit edilmiş olması, Yeni Zelanda'nın fiziki konumunun siber saldırılar karşısısında anlam ifade etmediğini gösterir niteliktedir (Burton, 2013: 227-228). Bu sebeple, bilgi ve iletişim teknolojilerinin dünyayı hızla dönüştürdüğünün farkına varan Yeni Zelanda devleti siber alana entegre bir devlet yapısı oluşturmak için 2000 yılında bir e-devlet girişimi başlatmıştır. Hizmetlerin internet ortamına taşınmasındaki temel amaçlar; daha verimli, daha şeffaf ve daha etkili operasyonların yürütülmesidir. Bunların yanı sıra, operasyoların daha etkin yürütülmesi, masrafların azaltılması ve bilgi kaynaklarının daha iyi kullanılarak toplumun demokratik süreçlere katılımının arttırılması amaçlanmaktadır (O'Neil, 2009: 2-3).

Fiziki anlamda hiçbir ülkeyle kara sınırı bulunmayan ve bulunduğu coğrafi konum itibariyle geçmiş yıllarda askeri tehditlerden endişe etmeyen Yeni Zelanda, 21. yüzyılın bireyden devlet düzeyine varan siber tehditleri karşısında kamu-özel sektör işbirlikleri çerçevesinde bütüncül politikalar geliştirmektedir. Hayatın her alanında işlevsellik gösteren siber alan kapsamında düşünüldüğünde, Yeni Zelanda'da vatandaşlarının en az %75'inin siber alanda günlük nedenlerle aktif olarak işlem gerçekleştirmesi, siber saldırılar karşısındaki kırılganlıkların ne derece yüksek olabileceği ihtimalini gündeme getirmektedir (New Zealand Government, 2011: 2). Siber tehditlerden korunmak ve siber güvenlik stratejilerini çeşitlendirmek isteyen Yeni Zelanda 2011 yılında Ulusal Siber Güvenlik Merkezi'ni (NCSC)[30] kurmuştur . Ulusal kritik altyapıların korunması ve gerçekleştirilen siber saldırıların tek bir merkez tarafından incelenip stratejiler geliştirilmesi Yeni Zelanda'nın siber güvenliğe verdiği önemi göstermektedir (Gordon, 2014: 32).

Mevcut siber tehditler devlet destekli espiyonaj, siber terörizm, fikir mülkiyetlerinin çalınması alanlarını kapsamaktadır. Yeni teknolojiler geliştirildikçe, siber alandaki risklerin ve fırsatların çeşitlenmesi sonucunda siber alana entegre olan aktörlerin politikalarının da aynı doğrultuda çeşitlenmesi gerekmektedir. Yeni Zelanda'nın siber güvenlik alanında hali hazırda uyguladığı ve uygulamayı planladığı stratejiler ve aksiyon planları şu şekildedir (Filinnova, 2018: 158):

[29] New Zealand Security Intelligence Service (SIS)
[30] National Cyber Security Center (NCSC)

- **Siber dayanıklılık:** Mevcut teçhizat ile bilgi altyapılarının milli çıkarlar doğrultusunda korunması ve siber tehditlere karşı dayanıklı hale getirilmesi, acil durum siber müdahale ekiplerinin[31] (CERTs) oluşturulması,

- **Siber kapasite:** Yeni Zelanda vatandaşlarının, iş sektörünün ve devlet kurumlarının siber tehditleri anlama ve kendilerini koruma kapasitesine sahip olması, küçük ve orta ölçekli şirketlerin ve ulusal altyapıların siber güvenlik kapasitelerini yükseltmelerinin sağlanması, siber güvenlik alanında çalışacak iş gücü yetiştirmek ve inovatif araştırmalarda bulunmak için eğitim politikalarının geliştirilmesi,

- **Siber suçlarla mücadele:** Siber suç teşkil eden müdahelelerin tümünün engellemesi, araştırılması ve uygun politikalar ile gelecek saldırıların önlenmesi, gerekli hukuki altyapının ve operasyonel müdahale ekiplerinin oluşturulması,

- **Uluslararası işbirliği:** Siber alanda gerçekleşen tüm aktivitenin barışçıl aktörlerin çıkarına hizmet etmesi için internet yönetişimi ve devlet davranışı normlarının inşa edilmesi yönünde politikalar uygulanması

Yeni Zelanda devleti yukarıda sıralanan stratejilerini gerçekleştirmek için kamu-özel sektör işbirliklerinin son derece önemli olduğunu vurgulamaktadır. Zira konumu itibariyle ülkenin ekonomisi, internet bağlantısının ve ağ yapılanmalarının işlevsel kalmasına ihtiyaç duymaktadır. Bu sebeple, özel sektörün ticari başarısının ardında yatan kritik bilgileri koruyabilmesi gerekmektedir. Siber güvenlik politikaları geliştirilirken bankalar, telekomünikasyon, iletişim, haberleşme ve yazılım şirketleri, sosyal medya, süpermarket hizmetleri, eğitim kurumları, STK'lar, meslek dernekleri ve devlet kurumları; kapsayıcı bir güvenlik stratejisi inşa edilerek korunmaktadır. Siber alana bağlı olan herhangi bir kurumun hizmet veremez duruma gelmesi, tüm sistemi savunmasız bırakacak sonuçlar doğurabilmektedir.

Siber suçluların ve devlet destekli aktörlerin kişisel bilgilere ve banka hesaplarına, fikri mülkiyetlere ve ulusal bilgi merkezlerine 7/24 siber saldırılar düzenlendiğini belirten hükümet yetkilileri milli güvenlik açısından bu adımı attıklarını belirtmişlerdir. Gerekli önlemler alınmadığı takdirde yaşanabilecek finansal zarara ve itibar kaybına tahammülleri olmadığını; buna ek olarak kritik altyapıların zarar görmesinin uzun vadede fiziksel saldırılardan daha yıkıcı olacağı da eklenmiştir. Siber güvenlik stratejileri belirlenirken ödün verilmeyecek ve daha iyi sonuçlar almak amacıyla hükümetin açıklamış olduğu beş prensip bulunmaktadır (New Zealand Government, 2019: 13):

[31] Computer Emergency Response Teams (CERTs)

- Güven inşa etmek ve sürdürmek,
- Toplum odaklı, saygılı ve kapsayıcı olmak,
- Çevik ve uyumlu olarak risk unsurlarını dengelemek,
- Daha iyi sonuçlar elde etmek için bileşik kuvvetlerimizden faydalanmak,
- Açık ve hesap verilebilir olmak

Yukarıda verilen prensipler, siber güvenlik stratejisinin çözülme zorunluluğu olan bir problem olarak değil, daha iyi sonuçlar almak için ortak sorumluluk projesi olarak görülmesi gerektiğini ifade etmektedir. Bu prensiplere ek olarak Yeni Zelanda, siber alanda barışı ve istikrarı daima savunacağını belirtmektedir. Uluslararası hukukun diğer operasyonel alanlarda geçerli olduğu gibi siber alanda da geçerli olduğunu, barışçıl ve stabil bir operasyonel alanın varlığını sürdürebilmek maksadıyla devletlerin siber alanda sorumlu davranması için normların geliştirilmesi ve uygulanması gerektiğini ifade etmektedir (New Zealand Government, 2019: 13).

3.2.1 Altyapı Sistemlerinin Oluşturulması

1991 yılında Yeni Zelanda Devlet Haberleşme Güvenliği Bürosu[32] (GCSB) kritik altyapı güvenliğini sağlamak ve diğer devlet kurumlarının sahip olduğu kategorize edilmemiş hassas bilgileri korumak amacıyla kurulmuştur. GCSB kuruluşundan itibaren uygulanacak politikalara rehberlik edilmesi, eğitim programları oluşturulması ve risk analizleri gerçekleştirilmesi için çeşitli platformlardan güncel bilgi toplanmıştır. Gerekli planlamanın gerçekleştirilmesinin ardından kurum kritik altyapıların korunmasını gündemine almış ve bu yönde politikalar izlemiştir. 2001 yılında GCSB hükümete daha kapsamlı bir siber güvenlik stratejisine ihtiyaç duyulduğunu belirterek yeni bir güvenlik merkezinin tesis edilmesine vesile olmuştur. Kritik Altyapıları Koruma Merkezi[33]'nin (CCIP) kurulması ile birlikte, odak noktası internet güvenliği olarak belirlenmiş ve fonksiyonları şu şekilde sıralanmıştır (Shore, Du, ve Zeadally, 2011: 1):

- 7/24 takip sistemi,

- Gözlem ve analiz,

- Teknik destek (Uzaktan erişim),

- Aracılık servisi eğitimi,

[32] Governemnt Communicaions Security Bureau (GCSB)
[33] Centre for Critical Infrastructure Protection (CCIP)

- Altyapı sağlayıcılarına, devlet kurumlarına ve Yeni Zelanda vatandaşlarına bir dereceye kadar hizmet

Zararlı yazılımlara, hizmet dışı bırakma saldırılarına[34], yazılımlarda yeni keşfedilen açıklara ve diğer bilgi güvenliği konularına müdahale etmede oldukça başarılı performans gösteren kurum bilhassa deniz aşırı meslektaşlar, kolluk kuvvetleri ve altyapı hizmeti sağlayıcılar ile kurulan bağlantıların kuvvetlendirilmesinde oldukça etkili olmuştur. CCIP, GCSB'nin merkez tesisinden operasyonlarını yürütmekte ve erken uyarı sistemleri ile halkı bilgilendirmeyi öncelikli politikalarından biri haline getirmiştir. Daha büyük ölçekte olan GCSB'nin işlevleri ise daha çok, istihbarat toplama ve gerekli birime iletme esasında olup günlük işleyişe doğrudan yüksek etki eden fonksiyonu bulunmamaktadır (Shore, Du, ve Zeadally, 2011: 2).

Yeni Zelanda hükümetinin siber güvenlik stratejileri özel sektörün ve devlet kurumlarının birlikte çalışmasını gerektirmektedir. Kâr odaklı işletmelerin ticari sistemlerine GSCB uzmanlarınca erişim sağlanması için taraflar arasındaki mevcut endişelerin giderilmesi, ortak çıkar odaklı politikaların oluşturulması ve her şeyden önce karşılıklı güven bağının sağlanması şart olmaktadır. Buna ek olarak, kritik altyapıları güvende tutabilecek çözümler sunabilmek adına hükümetin telekomünikasyon ve internet hizmeti sağlayan şirketleri düzenli olarak denetlemesi gerekmektedir. Zira özel sektör müşterilerine büyük oranda e-ticaret platformları aracılığıyla ulaşmakta ve siber güvenlik stratejileri oluşturulurken özel sektörün herhangi bir sebeple dışarıda bırakılması şirketlerin ve müşterilerinin büyük risk altında kalmasına sebep olabilmektedir (GCN, 2010). Yeni Zelanda'nın siber güvenliği gerekli kılan faktörleri devlet, toplum ve ticaret kapsamında aşağıdaki tabloda verilmiştir (Shore, Du, ve Zeadally, 2011: 4).

[34]Denial of Service (DoS) attacks

Tablo 4. Devlet, Toplum ve Ticari İşletmeler Kapsamında Siber Güvenlik Politikalarına İhtiyaç Duyulmasının Gerekçeleri

Kapsam	Faktör
Devlet	-Yeni Zelanda'nın egemenliğinin siber saldırılardan korunması, -Yeni Zelanda'nın kritik bilgilerinin siber casusluklardan korunması, -Yeni Zelanda'nın siber güvenlik alanında küresel işbirliği anlayışını savunması, -Devlet ve sanayinin telekomünikasyon teknolojilerine son derece bağımlı olması, -Yeni Zelanda'nın Uluslararası Telekomünikasyon Birliği (UTB) acil durum standartlarını desteklemesi, -Devletin çevrimiçi hizmetlerinin internet sağlayıcılarının güvenilir olmasını gerektirmesi,
Toplum	-Temel hizmetlerin işlevsellik garantisi -Yeni Zelandalıların temel konularda siber güvenlik konusunda farkındalık sahibi olması, -Elektronik toplumun siber suçluları caydırmak amacına uygun şekilde denetlenmesi, -Ticari işletmelerin güvenli e-ticaret hizmeti sunma görevi olması, -Devletin güvenli e-hizmetler sunma görevi olması,
Ticaret	-İnternete erişim ve servis sağlayıcıların istenmeyen içerik ve aktiviteyi kaldırma görevi olması, - İnternet erişimi sağlayıcıların küresel erişimin tahsis edilmesi görevi olması, - İnternet servisi sağlayıcıların sistem kontrolleri gerçekleştirerek yapısal ve yazılım tabanlı sorunları gidermesi, - E-ticaret servislerinin hata vermeden işlemlerin gerçekleştirilmesini sağlaması

Kaynak: Shore, M., Du, Y., ve Zeadally, S. (2011: 4). Public Private Partnership Model for National Cybersecurity. *Policy Studies Organization*, Vol 3, Iss 2, Article 8.

Devlet perspektifinden bakıldığında, siber güvenlik politikaları kritik bilgilerin ve bilgi sistemlerinin korunması için büyük önem arz etmektedir. Yeni Zelanda uluslararası düzeyde farklı işbirlikleri kapsamında sahip olduğu paydaşları ile istihbarat paylaşmaktadır. Bu bağlamda bir artı değer yaratması ve uluslararası anlamda itibar kaybını önleyebilmesi için dayanıklı bir siber güvenlik kapasitesine sahip olması gerekmektedir. Yeni Zelanda tehdit unsurlarından arındırılmış, güvenli bir siber alan sahibi olma çalışmalarını desteklemektedir. Zira güvenli bir siber alan Yeni Zelanda'daki özel sektörün ulusal ve uluslararası çapta faaliyet gösterebilmesi için önem teşkil etmektedir. Ayrıca Yeni Zelanda vatandaşlarının ve özel sektörünün devlet

hizmetlerinden çevrimiçi olarak yararlanırken güvende olmaları gerekmektedir. Aksi halde kullanıcıların kişisel bilgileri kötü niyetli bilgisayar korsanlarının eline geçebilmekte ve yeni tehditler doğabilmektedir.

Toplumsal düzeyde değerlendirildiğinde, temel hizmetlerin kesintiye uğraması tüm toplumsal hayatı felç edebilecektir. Bunu engellemek amacıyla şekillendirilen siber güvenlik politikalarına sahip olunması, vatandaşların temel hizmetlerden mahrum kalmamasına ve siber tuzaklara karşı daha bilinçli hale gelmesine katkı sağlamaktadır. Dayanıklı güvenlik duvarlarının ve farkındalık sahibi vatandaşların varlığı siber suçların daha az meydana gelmesini sağlamakta ve faillerin ortaya çıkarılmasını kolaylaştırmaktadır. Ayrıca bir tüketici/vatandaş olarak siber alana erişen kullanıcıların güvende olduklarını bildikleri takdirde nispeten daha refah içerisinde bir hayat sürme imkânına sahip olmaktadırlar.

Ticari işletmelerin odak noktası günden güne daha fazla tüketiciye ulaşma yöntemlerini belirlemek ve sonucunda kârlı bir işletmeye sahip olmaktır. Yeni Zelanda'nın konumu göz önüne alındığında siber alan işletmelerin büyüyebilmesi ve rekabet edebilmesi açısından önem teşkil etmektedir. Bilhassa internet erişimi ve servisi sağlayıcılarının bağlantıları güvenli hale getirmesi, bu hizmetten günlük olarak yararlanan kâr odaklı işletmelerin ve tüketicilerin güvende olabilmesini sağlamak için yapılmaktadır. Donanım ve yazılım tabanlı problemlerin çözülmesi ve e-ticaret uygulamalarının sorunsuz çalışmasının sağlanması ticari işletmelerin varlıklarını sürdürebilmeleri ve işletmelerini ayakta tutabilmeleri için gerçekleştirilmektedir.

Siber güvenlik politikalarının başarıya ulaşması için giderilmesi gereken kırılganlıklar ve kritik altyapıların düzenli olarak güncellenmesi görevleri NCSC'ye aittir. Devlete ait kritik bilgilerin ve sistemlerin korunması, çeşitli senaryolara yönelik planlama ve hızlı müdahale kapasitesi gerektirmektedir. Üzerine düşen görevleri en hızlı ve etkili şekilde yerine getirmek için NCSC üç alana öncelik vermiştir (NCSC, 2013: 17-19):

- Çevrimiçi güvenliğin teşvik edilmesi,

- Çevrimiçi altyapıların korunması,

- Acil siber müdahale ekiplerinin oluşturulması (CERTs),

Bu öncelik alanlarının belirlenmesindeki amaçlar; küçük işletmelerin ve bireylerin farkındalık seviyelerinin yükseltilmesi ve kritik altyapıların siber güvenlik kapasitelerinin arttırılması olarak planlanmıştır. NCSC 2013 yılında Yeni Zelanda'daki internet kullanıcısı kurum ve kuruluşların siber güvenlik alanında farkındalık sahibi olmasını sağlamak amacıyla eğitimler düzenlemiştir. NCSC'nin çalışmaları mevcut altyapı

sistemlerinin ve bilişim ağlarının siber saldırılara karşı dayanıklılık geliştirmesi açısından önem taşımaktadır (NCSC, 2013: 17-19).

Görevlerinden biri olarak NCSC siber güvenlik alanında yaşanan gelişmeler hakkında istihbarat toplamaktadır. NCSC'nin resmi rakamlarına göre Yeni Zelanda siber alan kaynaklı hırsızlık ve dolandırıcılık aktiviteleri sebebiyle yıllık 500 milyon dolar kayba uğramaktadır. 2011'de gerçekleştirilen bir anket çalışmasına göre Yeni Zelanda, rapor edilen siber-hırsızlık vakalarında 78 ülke arasından dördüncü olarak görülmektedir. 2012 yılında toplanan verilerde ise, yılda ortalama 133.000 Yeni Zelanda vatandaşının kimlik hırsızlığı mağduru olduğu ve bu sayının üçte birinin kimlik bilgilerinin çevrimiçi ortamlardan çalınması, üçte ikisinin de kredi veya banka kartı dolandırıcılıklarına maruz kaldıkları belirlenmiştir (Gordon, 2014: 33). Mağduriyetlerin büyük bir çoğunluğu istenmeyen elektronik postalar[35], hizmet engelleme saldırıları ve zararlı yazılımlar aracılığıyla gerçekleştirilmektedir. Gerçekleştirilen çalışmalar toplumun %70'inin siber alanda suç teşkil eden unsurlardan en az bir kere zarara uğradıklarını belirtmektedir. Buna ek olarak, özel sektörden sızdırılmış olan fikri mülkiyetlere fiyat biçilmesi güç olmakta hatta herhangi bir saldırıya uğradıklarının farkında olmadıkları durumlar gerçekleşebilmektedir. Diğer yandan, bu tip durumları bildirmek başlangıç olarak itibar, sonuç olarak ise müşteri kayıplarına sebep olabileceği için bildirilmesi konusunda işletmeler tarafından tereddüt yaşanmaktadır (Gordon, 2014: 34).

Yeni Zelanda'nın siber güvenlik stratejileri sahip olduğu kritik altyapı sistemlerine, devlet kurumlarına, özel sektörüne ve vatandaşlarına yönelik olarak gerçekleşebilecek siber saldırılara karşı dayanıklılık geliştirmeyi amaçlamaktadır. Telekomünikasyon sistemleri, su ve kanalizasyon hizmetleri, ekonominin işleyişi için gerekli kurumlar (bankacılık sistemleri), ticari veya bireysel hayatı sekteye uğratabilecek siber saldırılara karşı korunamaz ise, siber suçlar ve siber casusluk eylemleri sebebiyle yıllık 1 trilyon dolara kadar kayıp gerçekleşebileceği ifade edilmektedir (NCSC, 2013: 3-6).

2011 yılından itibaren yayınlanan güvenlik stratejileri genel itibariyle Yeni Zelanda'nın operasyonel yapısı ve konuyu ele alış biçimi hakkında önemli bilgiler sunmaktadır. 2015 yılında CERTs'in çalışmalarına verilen önem arttırılmış ve yılsonunda toplanılan veriler sayesinde ilk siber güvenlik zirvesi gerçekleştirilmiştir. Son 2 yıllık operasyon süresince 67 milyon dolarlık kayıp engellenmiş, NCSC'nin zararlı yazılımlardan arındırılmış ağlar oluşturması sağlanmış, Yeni Zelanda polisine, toplumuna, özel şirketlerine, devlet kurumlarına ve özel sektör çalışanlarına yönelik ihtiyaçları doğrultusunda eğitim

[35] Spam mail

seminerleri düzenlenmiştir. Zirvede öne çıkan diğer bir konu ise, siber saldırıların gerçekleşme yönteminin sistem kullanıcılarının farkındalık seviyelerinin düşük olmasından kaynaklandığı olmuştur. Telefon veya internet siteleri üzerinden sisteme erişim sağlayan suçlular kullanıcıların bilgilerini oltalama[36] yöntemi ile ele geçirerek amaçlarını gerçekleştirmektedir. Bu sebeple toplumun temel siber güvenlik eğitimleri alması Yeni Zelanda'nın farkındalık seviyesinin yükseltilmesi NCSC'nin başlıca hedefleri arasında yer almaktadır (New Zealand Government, 2019: 6).

3.2.2 İnsan Kaynağının Yetiştirilmesi

Siber alanda güvenlik inşa etme süreci altyapıların, sistem donanımlarının ve yazılımlarının güvenliğini sağlamak anlamına geldiği gibi, kullanıcıların da siber alanda karşılaşabilecekleri tehdit unsurlarından korunmalarını gerektirmektedir. Bilhassa bu sistemleri kullanan operatörler mevcut siber saldırıların hedefi olmaktadır. Siber alanda farkındalık sahibi olan bir insan kaynağına sahip olmak siber güvenlik stratejilerindeki en önemli adımlardan biri olarak görülmektedir. Bu minvalde Yeni Zelanda'da 2011 yılından itibaren aktif bir şekilde siber güvenlik eğitimine önem vermeye başlamıştır (New Zealan Government, 2019: 6).

Auckland'da bulunan Unitec Teknoloji Enstitüsü (UTI) lisans, yüksek lisans ve doktora derecelerinde siber güvenlik eğitimi vermeye ilk başlayan üniversite olmuştur. Unitec'e ek olarak Auckland, Waikato ve WelTec, Massey ve AUT Üniversiteleri de bu girişime katılmışlardır. Eğitim tek başına siber alanda güvende kalmak için yetersiz kalmaktadır. Bu sebeple UTI, Japonya Ulusal Bilgi ve İletişim Teknolojileri Enstitüsü (NICT) ile işbirliği kurarak Siber Güvenlik için Sayısal Zekâ Merkezi'ni[37] açmıştır. Bu merkezde gerçek hayattan örnekler alınarak hazırlanan acil durum senaryolarıyla öğrenciler karşılaşabilecekleri tehdit senaryolarıyla önceden yüzleştirilip pratik yapmaları sağlanmaktadır. Son teknoloji siber güvenlik gözlem kapasitesi sayesinde Yeni Zelanda'da insan ve teknoloji sermayesi oluşturularak hem ülkeye hem de iş sektörüne siber güvenlik uzmanları yetiştirilmektedir. Merkezin amaçları şu şekilde belirtilmiştir (Fourie, ve diğerleri, 2014: 176-177):

- Siber güvenlik üssü olarak hizmet vermek,
- Siber güvenlik araştırmalarını yürütmek ve teşvik etmek,
- Yüksek verim alınabilecek bireyleri belirleyip siber güvenlik alanında eğitim vermek,
- Mezunların işverenler tarafından tercih edilebilir olmasını sağlamak,

[36] Phishing: Kullanıcının gönderilen e-postada mevcut olan erişim adresine tıklamasıyla kullandığı cihazın erişimi ve içinde bulunan bilgiler e-postayı gönderen suçluların eline geçmektedir.

[37] Computational Intelligence for Cyber Security (CICS)

- Toplumda farkındalık yaratmak için destek vermek,

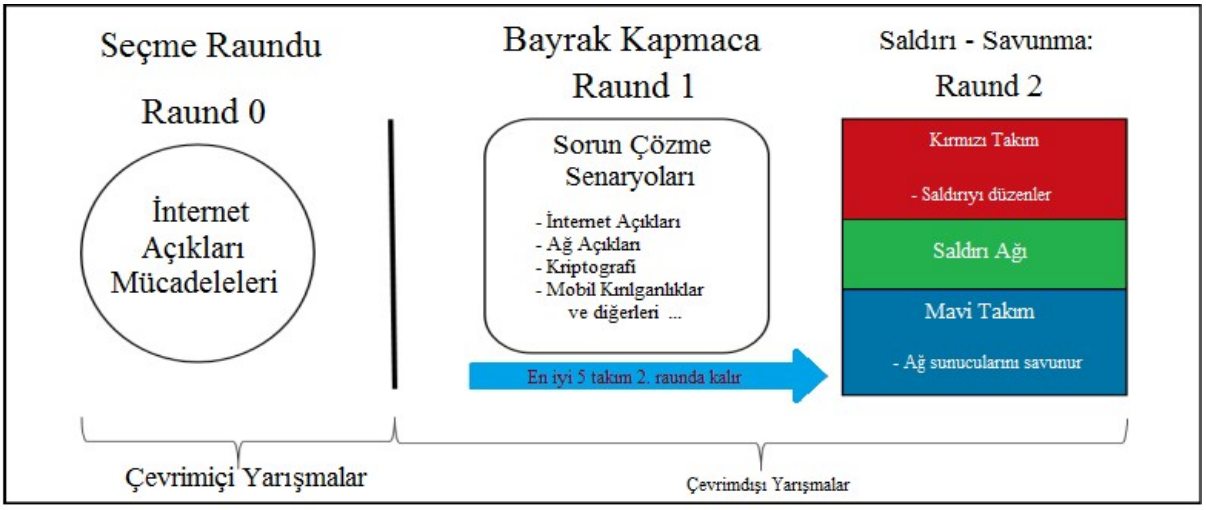
- Toplumun siber güvenlik alanında bilgi sahibi olması için çalışmalara sponsor olmak, yönlendirmek ve doğrudan seminerler düzenlemek,

Bahsi geçen araştırma merkezinin gelecek saldırıları önlemede etkili olacağı öngörülmüştür. Güvenli ve dayanıklı bir siber alan yaratma yönünde önemli bir adım olduğu düşünülmüş ve bu sebeple merkezin aktiviteleri Waikato Üniversitesi'nin de bir siber güvenlik laboratuvarı açmasına öncülük etmiştir.

Siber güvenlik alanında uzmanlaşmak isteyen bireylerin geçmesi gereken eğitimlerin sayısı ve düzeyi uzmanlaşılmak istenen alana göre değişiklik göstermektedir. Eğitim yöntemleri arasında görselleştirme ve simülasyonlar sıklıkla kullanılmaktadır. Bu sayede uzman adaylarının gerçek bir tehdit unsuruyla karşı karşıya kaldıklarında verebilecekleri tepkiler ve kriz anındaki işlevsellikleri ölçülebilmektedir. Birçok gerçek olay sonrasında, itibar kaybı endişesi yaşayan yöneticilerin sistemlerin ele geçirilmesini teknik arıza olarak açıklaması veya detay vermekten kaçınması sebebiyle sistem açıklarının düzeltilmesi güçleşmektedir. Daha şeffaf bir oluşum hedefleyen bilim insanları Yeni Zelanda Siber Güvenlik Meydanokumalarını[38] (NZCSC) hayata geçirmiştir. Meydanokumalara katılmak isteyen adaylar, çeşitli deneyim ve eğitime sahip kişiler lise ve üniversite öğrencilerinden oluşabildiği gibi, özel sektörde çalışan uzmanların da katılım sağlanabilmektedir (Jeffery, ve diğerleri, 2017). Şekil 5'te görülen şema meydan okumalardaki senaryolardan birine örnek teşkil etmektedir (Jeffery ve diğerleri, 2017: 1124).

[38] New Zealand Cyber Security Challenge (NZCSC)

Şekil 4. Siber Güvenlik Yarışma Platformları Tasarımı



Kaynak: Jeffery, G., Ryan, K., Ko, L., Kho, J., Saidah, S., Mark, A., Apperly, M. (2017: 1124). Visualizing the New Zealand Cyber Security Challenge for Attack Behaviours. *IEEE Computet Society*, 1123-1130.

Meydan okumalarda ilk aşama katılımcı sayısının azaltılması ve takımların belirlenmesi amacıyla seçme raundu ile başlamaktadır. İnternet sitelerinde mevcut kırılganlıklardan faydalanılarak sitelerin ele geçirilmesi veya söz konusu internet sitesinin ne tür kırılganlıkları olduğunu tespit etmeye yönelik pratik çalışmalar aracılığıyla adaylar belirlenmektedir. Bu raundu başarı ile tamamlayan takımlar bir dizi sorun ile karşı karşıya bırakılarak analiz ve pratik becerileri ölçülmektedir. Çeşitli kırılganlık problemlerini çözmeleri veya kırılganlıkları mevcut olan sistemlere sızmaları istenen takımların en iyi sürelere ve becerilere sahip beş tanesi ikinci raunda kalmaya hak kazanmaktadır. İkinci raunda katılan takımlar kırmızı ve mavi takım olarak ikiye ayrılmakta ve sırasıyla sistemlere saldırma veya savunma konumunda bulunmaktadırlar. Bu uygulamanın sonunda galip gelen takım için eğitim ve kariyer olanakları sunulmakta, aynı zamanda bu başarılar belgelendirilerek siber güvenlik alanında yetenekli bireylerin görünürlükleri arttırılmaktadır.

Yeni Zelanda siber güvenlik politikalarını şekillendirirken yetenekli ve tecrübeli siber güvenlik uzmanlarına ihtiyaç duymaktadır. Gerekli işgücünün yetişmesi için izlenmesi gereken adımlar şu şekilde sıralanmıştır (New Zealand Government, 2019: 12):

- Siber güvenlik uzmanlarının istihdam edilebileceği devlet kurumları, altyapı hizmet sektörleri ve ticari işletmelerin sayılarının arttırılması için teşviklerde bulunulması,

- Siber güvenlik uzmanlarına yönelik rollerin ve fırsatların desteklenmesi,

- Yeni Zelanda'da yükselmeye başlayan siber güvenlik endüstrisinin teşvik edilmesi,

- Özel sektörde mevcut işletmelerin bünyelerinde siber güvenlik uzmanlarını istihdam edebilecekleri merkezler bulundurmaya teşvik edilmesi ve yönetici pozisyonlarına yükseltilmelerinin önemi hakkında farkındalık oluşturulması,

- Birinci kalite siber güvenlik araştırmaları gerçekleştirilmesi için akademinin ve araştırma topluluklarını teşvik edilmesi,

- Akademinin ve özel sektörün yüksek kalite siber güvenlik araştırmalarında bulunmaları için desteklenmesi

Siber güvenlik alanında uzman personele sahip olmak için farklı eğitim seviyesine sahip bireyler için farklı seviyelerde eğitim programları geliştirilmesi gerekmektedir. Örnek olarak, hali hazırda siber güvenlik sektöründe çalışan ancak hala belirli konularda eğitime ve pratiğe ihtiyacı olan bireyler için kısa süreli eğitim programları düzenlenmektedir. Ayrıca CCIP siber güvenlik alanında kısa süreli eğitimleri dahi sertifikalı hale getirerek eğitim alanlarının resmi olarak görünürlüğünü arttırmaktadır. Üniversitelerden mezun olan kişiler istihdam edildikleri takdirde tam anlamıyla işlevsel personeller olarak işe başlamaktadır. İşverenlerin yeni personele çok fazla yatırım yapması gerekmediği için çok daha verimli çalışma ortamları yaratılabilmektedir. Kimi üniversitelerin siber güvenlik alanında lisansüstü derece vermeye başlaması, bu sektörde istihdam edilen personelin hem kendi alanlarında yükselebilmesine hem bakış açılarını genişletebilmesine, hem de personelin göreceli olarak daha az zaman ve para harcayarak kendilerini geliştirebilmesine olanak tanımıştır. Eğitimde bir üst basamak olarak yüksek lisans derecelerini tamamlayan personele doktora imkânları da sunulmakta ve bu sayede ileri seviye araştırmaların yapılabilmesine, siber güvenlik endüstrisi dâhilinde araştırma merkezlerinin kurulmasına ve daha çok istihdam alanı yaratılmasına imkân sağlanmaktadır (Fourie, ve diğerleri, 2014: 178-179).

2013 yılında insan kaynağı yetiştirme çalışmalarına hız kazandırmak amacıyla Bir İşgücü Stratejisi[39] yürürlüğe konmuştur. Devlet kurumları içerisinde mevcut kariyer imkânlarının çeşitlendirilmesi ve çalışanların refah seviyelerinin iyileştirilmesi üzerine ne tür çalışmalar yapılabileceği hakkında çalıştaylar organize edilmiştir (Wellington Regional Strategy Office, 2016: 26). En geniş kapsamda GCSB ve SIS içerisinde yürütülen çalışmalar sonucunda insan kaynakları faaliyetleri tek çatı altına toplanarak iç ve dış yönetim faaliyetleri iyileştirilmiştir. Bu kurumlarda kariyer sahibi olmak isteyen çalışanların varabilecekleri noktalar belirlenerek çalışanların kariyer fırsatlarının farkında olması sağlanmıştır (GCSB, 2014: 21).

Yeni Zelanda'da özel sektör %90 oranında küçük işletmelerden oluşmaktadır. 20 veya daha az çalışana sahip bu işletmelerin yüksek uzmanlık becerilerine sahip siber güvenlik

[39] One Workforce Strategy

uzmanlarını istihdam etmeleri pek mümkün olmamaktadır. Bunun yerine kısa süreli eğitimleri tamamlayarak sertifika sahibi olmaya hak kazanmış personelleri tercih etmektedirler. Yüksek lisans ve doktora derecelerinden mezun olan kişiler yüksek kabiliyete sahip olmakta ve siber güvenlik alanında seçtikleri kariyerlerde ilerlemekte veya mevcut kariyerleri ile siber alanda kullanabildikleri yeteneklerini birleştirerek çalışmalar yürütebilmektedirler. Lisansüstü derecelere sahip kişiler aynı zamanda kendi firmalarını kurarak yeni istihdam yaratabilmekte ve Yeni Zelanda'nın siber alanda daha aktif rol oynamasını sağlamaktadırlar. Diğer opsiyonlar arasında ise; bu bireylerin deniz aşırı ülkelerde, devlet bünyesinde, araştırma tesislerinde veya üniversitelerde istihdam edilmeleri ve gelecek nesillerin yetişmesinde önemli rol oynamaları söz konusu olmaktadır (Fourie, ve diğerleri, 2014: 180).

3.2.3 Çok Boyutlu ve Entegre Politikaların Şekillendirilmesi

Siber güvenlik politikaları oluşturulurken sürece dâhil edilmesi gereken birden çok parametre bulunmaktadır. Yeni Zelanda gibi küçük bir devlet için devletlerarası ilişkiler ve özel sektörün işleyişinin sekteye uğramaması, siber alana sorunsuz erişim kabiliyetine sahip olarak gerçekleşmektedir. Zira diğer devletler siber alana erişimin kesintiye uğraması durumunda operasyonlarını geleneksel kanallardan yürütebilme olanağına sahip olmakta ancak Yeni Zelanda, konumunun uzak ve ekonomik hacminin küçük olması sebebiyle diğer devletlere kıyasla siber alana daha fazla ihtiyaç duymaktadır. Mevcut tehditlerden korunması amacıyla Yeni Zelanda vatandaşlarının ve küçük işletmelerin siber güvenlik alanındaki farkındalıklarının yüksek tutulması, devlet kurumlarının güvenliğinin sağlanması ve kritik altyapıların korunması için stratejiler geliştirmektedir (Luiifj, Besseling, Spoelstra, ve de Graaf, 2013: 3).

GCSB, birçok operasyonda Yeni Zelanda Savunma Kuvvetleri[40] (NZDF) birimlerine destek sunmaktadır. Siber teknolojilerin yardımıyla NZDF birimlerine yönelik gerçekleştirilebilecek tehdit unsurlarının tespit edilmesi ve etkisiz hale getirilmesi sağlanmaktadır. Askeri operasyonlardaki desteğin yanı sıra, GCSB'nin rolü istihbarat toplama ve paylaşma alanlarında yoğunlaşmıştır. Üye olduğu işbirliği projeleri Yeni Zelanda'nın küçük bir devlet oluşunu ve sahip olduğu siber güvenlik kapasitesi ve istihbarat ağı, bulunduğu coğrafi konumu önemsizleştirmektedir. İstihbarat toplama ve dağıtma çabaları Yeni Zelanda'nın siber saldırı gerçekleştirme niyetinde olan aktörleri caydırma, saldırganları belirleme ve gerektiği koşullarda misilleme gerçekleştirebilme kapasitesine sahip olmasını sağlamaktadır. GCSB ve SIS siber güvenliğe en çok katkıda bulunan iki kurum olarak görülmekte ve toplamış oldukları istihbaratı işbirliği içerisinde bulunulan istihbarat servisleriyle paylaşmaktadır. Bu paylaşımın karşılığında Yeni Zelanda vermiş olduğu istihbaratın yaklaşık beş katını elde etmektedir (GCSB, 2013).

[40] New Zealand Defence Forces (NZDF)

Beş Gözlü İstihbarat Sistemi[41] (FVEY) adı verilen işbirliği projesinin içerisinde Yeni Zelanda'nın yanı sıra ABD, Kanada, Avusturalya ve Birleşik Krallık yer almaktadır. Her ne kadar mevcut sistemin en fazla fayda elde edeni Yeni Zelanda olarak görülse de, beşliyi oluşturan hiçbir ülke tek başına bu ölçekteki küresel istihbarat ağını sürdürebilecek kaynaklara sahip olmamakla beraber, istihbarat ağından elde edilen caydırıcılık kozunu da kaybetmek istememektedir.

Uluslararası alanda güvenlik işbirlikleri oluşturmak amacıyla Yeni Zelanda 2012 yılında NATO ile Bireysel Ortaklık ve İşbirliği Programına[42] (IPCP) katılmıştır. Siber güvenlik konularında danışmanlık ve işbirliği konusunda alınan destek ülkenin siber güvenlik politikaları geliştirebilmesi ve uygulayabilmesindeki en önemli faktör olarak görülmektedir. Ancak 2010 yılı itibariyle kurulan işbirlikleri Yeni Zelanda'nın siber güvenlik kapasitesinin mevcut tehditler karşısında yetersiz kalmasına neden olmuş ve gerçekleştirilen siber saldırılara karşı olan dayanıklılık 21. yüzyılın ikinci on yılı itibariyle yetersiz kalmaya başlamıştır. 2011 yılında özel sektörün üçte ikisinin son bir yıl içinde düzenli olarak siber saldırılara maruz kaldığını ve toplam 70.000 Yeni Zelanda doları finansal kayıplarının olduğunu rapor etmişlerdir. 2012 yılında Yeni Zelanda'nın resmi 'Work and Income' adlı internet sitesinde mevcut olan müşteri bilgileri siber korsanlar tarafından sızdırılmıştır. Buna ek olarak 2013 yılında zamanın başbakanı John Key'in şahsi internet sayfası da dâhil olmak üzere siyasi parti web sitelerine, bir düzine kadar dağıtılmış hizmet dışı bırakma saldırısı[43] düzenlenerek toplumun gözünde siyasi partileri itibarsızlaştırma propagandası düzenlenmiştir. Diğer taraftan GCSB'nin mevcut personelinin güncel siber tehditler karşısında yetersiz kalması sebebiyle hükümet dayanıklılık alanında yatırımları arttırmış ve siber güvenlikten sorumlu kurumların bütçelerini yıllık 45 milyon Yeni Zelanda dolarından yıllık 97 milyon Yeni Zelanda dolarına yükseltmiştir (GCSB, 2013). Buna ek olarak, siber güvenlik alanında yetişmiş personelin kısıtlı iş imkânları sebebiyle deniz aşırı ülkelerde kariyerlerine devam etmeleri, ülkedeki altyapıların korunması için gerekli stratejilerin geliştirilememesine yol açmıştır. Başarılı siber güvenlik uzmanlarının daha yüksek maddi gelir elde etmek amacıyla genellikle deniz aşırı ülkelerde kariyer sahibi olmaları her ne kadar ülke imajına katkıda bulunsa da, ülke güvenliğinden sorumlu uzmanların yetersiz oluşu sebebiyle mevcut siber güvenlik politikaları başarısızlığa uğramıştır. Bu durumun önüne geçmek için çeşitli üniversitelerde araştırma laboratuvarları ve akademik programlar teşvik edilerek uzman eksikliğinin giderilmesi için çalışmalar yürütülmektedir.

2014 yılında siber güvenlik kapasitesini arttırmak amacıyla CORTEX adlı proje hayata geçirilmiştir. Bir yazılım paketi olarak tasarlanan ve kritik öneme sahip ulusal altyapıların

[41] The Five Eyes
[42] Individual Partnership Cooperation Programme (IPCP)
[43] Dağıtılmış Hizmet Dışı Bırakma Saldırıları (Distributed Denial of Services) birkaç farklı lokasyondan aynı anda gerçekleştirilerek internet sayfasının aşırı yüklenmesine ve geçici olarak hizmet verilememesine sebep olmaktadır.

korunmasında kullanılan CORTEX sisteme zarar verme potansiyeli olan zararlı yazılımları tespit ederek ve etkisiz hale getirerek oldukça kapsamlı bir beyaz solucan programı olarak kullanılmaktadır. Bilhassa deniz aşırı bölgelerden gönderilen virüslerin ve zararlı yazılımların tespit edilmesi ve engellenmesi Yeni Zelanda'nın ekonomik ve siber güvenliği açısından önem teşkil etmektedir. CORTEX'in koruma alanları şu şekilde sıralanmaktadır (GCSB, 2017):

- Fikri hakların çalınması (özgün çalışmalar, teknik tasarımlar ve ticari açıdan hassas teklif dokümanları),

- Müşteri bilgilerinin çalınması (kredi kartı ve kimlik bilgileri)

- Özel konuşma ve yazışmaların yok edilmesi veya sızdırılması,

- Online ortamlarda mevcut olan verilerin fidye karşılığı serbest bırakılmak üzere şifrelenmesi,

- Ağ bağlantılarına veya internete bağlı sistemlere saldırılar düzenlenerek hizmetlerin aksatılması

CORTEX ağından faydalanan kurumlar sırasıyla; CERT NZ[44], Başbakanlığa bağlı Siber Politika Ofisi, Yeni Zelanda Polis Gücü, SIS, İçişleri Bakanlığı gibi resmi kurumlara ek olarak NetSafe[45], Internet Task Force[46] ve Connect Smart[47] gibi özel sektör ortaklarından oluşmaktadır. Siber Politika Ofisi ulusal güvenliğe yönelik bir tehdit gördüğü takdirde özel sektörden kurumlar da CORTEX yazılım paketinden faydalanabilmekte ve Yeni Zelanda'nın siber güvenlik alanındaki dayanıklılığı bu programın devlet ve özel sektör bünyesinde aktif olarak kullanılması ile arttırılmaktadır

CORTEX'in operasyonel hale gelmesinden sonra siber saldırıların çıkış noktasının belirlenmesi ve tehditlerin ortadan kaldırılması hususunda ciddi ilerlemeler kaydedilmiştir. Örnek olarak 2019 GCSB yıllık raporuna göre dönem içerisinde 339 saldırı meydana gelmiş ve 131 saldırının (tüm saldırıların %38'ine tekabül eden oran geçen yıllardaki devlet destekli saldırılar ile paralellik göstermektedir) devlet destekli siber korsanlar tarafından gerçekleştirildiği ortaya çıkartılmıştır. CORTEX sayesinde dönem içerisinde toplam 27,7 milyon Yeni Zelanda doları tutarında finansal kayıp engellenmiştir (GCSB, 2019: 19). Yeni Zelanda'nın dijital stratejileri ülkedeki özel sektörün ticari faaliyetlerinin sekteye uğramaması için son derece önem arz etmektedir.

[44] Yeni Zelanda Acil Durum Siber Müdahale Ekipleri
[45] Netsafe Yeni Zelanda'da aktif olan bağımsız, kar gütmeyen bir çevrimiçi güvenlik kuruluşudur (https://www.netsafe.org.nz/aboutnetsafe/).
[46] Yeni Zelanda İnternet Timi kâr gütmeyen bir kuruluştur ve siber güvenlik kapasitesini arttırmak amacıyla Yeni Zelanda halkının internet güvenliğini sağlamaktadır (https://nzitf. org.nz/about-1).
[47] Güvenli Bağlantı İşbirliği Yeni Zelanda'da mevcut işletmelerin, okulların ve vatandaşların çevrimiçi ortamda güvende olmaları amacıyla başlatılmış devlet kurumları, STK'lar ve özel sektörden katılımcılar içeren bir girişimdir CERT NZ'nin hayata geçirilmesinden itibaren yürürlükten kaldırılmıştır (https://dpmc.govt.nz/our-programmes/special-programmes/connect-smart).

Tablo 5. 2018 Yılı İtibariyle Siber Dolandırıcılık Sayısı ve Kayıplar

Kategori	Rapor Edilen Olay Sayısı	Toplam Kayıp	Ortalama Kayıp
İlişki ve Güven Temelli Dolandırıcılıklar	68	8,717,578 $	128,200 $
Yatırım Dolandırıcılıkları	121	7,150,682 $	59,097 $
Ödül ve Hibe Dolandırıcılıkları	67	2,459,223 $	37,704 $
Kimlik Dolandırıcılıkları	23	339,989 $	14,782 $

Kaynak: NetSafe. (2018). *Annual Report.* Auckland, NZ: NetSafe.

Tablo 5'te görüldüğü üzere devlet kurumlarının, özel sektörün ve STK'ların yoğun çabalarına rağmen siber suç unsurları farklı yöntemler geliştirerek var olmaya devam etmektedir. Bilhassa bireylerin ve hedef alınan özel sektör temsilcilerinin çalışanlarının cihazları, Tablo 5'te görülmekte olan yöntemlerden en az biriyle ele geçirilerek hassas bilgiler ele geçirilebilmektedir. Ülke içinde siber güvenlik alanında hizmet veren tüm kurum ve kuruluşlar bu sebeple mevcut aktivitelerini yıllık raporlar aracılığıyla tamamen şeffaf bir biçimde (bütçe planlamaları ve harcamalar, başarılı olunan veya başarısızlıkla sonuçlanan projeler, gelecek planlamaları vb.) toplum ile paylaşmaktadırlar. Yeni Zelanda'nın politikaları; ortak çıkar ve karşılıklı hesap verilebilirlik ilkeleri doğrultusunda, karşılıklı güven ilişkisinin esas olduğu işbirlikleri aracılığıyla yürütülmektedir.

Özel sektörde siber güvenlik kapasitesinin arttırılması amacıyla çeşitli stratejiler belirlenmiştir. Yeni Zelanda'nın özel sektör yapısı çoğunlukla küçük şirketlerden oluştuğundan kompleks sistemleri yönetecek bilgi ve tecrübeye sahip uzmanlar istihdam edilememektedir. Buradan hareketle özel sektöre, siber güvenlik alanında başarılı stratejiler üretmek için ortak hareket planları yapmaları gerektiği tavsiye edilmektedir. Siber saldırıların ve açıkların paylaşılması, kullanılan mevcut sistemlerin kırılganlıklarının belirlenmesi ve akabinde ortak eylem planları oluşturulması sonucunda güvenlik kapasitesinin arttırılabileceği düşünülmektedir. Özel sektöre verilen tavsiyelerin içerisinde; saldırılara karşı dayanıklı çok katmanlı bir güvenlik duvarı oluşturulması, güncel virüs programlarının kurulması, tüm şirket hesaplarının mutlaka şifre korumalı hale getirilmesi ve yanlış giriş sonucu sistemlerin geçici olarak kullanım dışı kalmasının sağlanması yer almaktadır. Buna ek olarak, tüm bilgilerin günlük olarak yedeklenmesi, kablosuz bağlantı şifrelemesinin yükseltilmesi gibi oldukça temel ve faydalı maddeler içermektedir (Fourie, ve diğerleri, 2014: 9).

Siber güvenlik alanında farkındalık oluşturmak ve aktif vatandaşlara sahip olmak amacıyla 2019 Siber Güvenlik Stratejileri yıllık raporunda uygulanmakta olan adımları Yeni Zelanda hükümeti şu şekilde sıralamıştır (New Zealand Government, 2019: 12):

- Pratiğe yönelik, düzenli ve hedefleri belli farkındalık oluşturma programları ile tüm toplumun siber dayanıklılığa sahip olması,

- Siber suçları rapor etmenin tüm toplum nezdinde kolaylaştırılması ve ilgili devlet kurumlarından ve STK'lardan yardım alınmasının sağlanması,

- Eğitici araçlara erişim imkânının arttırılması ve toplumun siber saldırılara karşı dayanıklılığının güçlendirilmesi,

- Kolay zarar görebilecek yaşlı ve genç vatandaşların siber suçların kurbanı olmalarını önlemek amacıyla okullarda ve bakım evlerinde seminerler düzenlenmesi,

- Tüm kurumlar ve sektörler bazında yürütülen araştırmaların sonuçlarının tamamen şeffaf bir biçimde paylaşılması

Yönetişim anlamında kapsamlı ve çok paydaşlı bir yaklaşımla şekillendirilen sürecin devlet-toplum işbirliği çerçevesinde geliştirildiği görülmektedir. Bu kapsamda farkındalık oluşturulması, eğitim ve uzmanlık gibi noktalar üzerinde durularak siber alanın hayatın her alanındaki önemine ve bu çerçevede devletle vatandaşların işbirliğine vurgu yapılmaktadır.

Devletin toplumu korumak için belirlediği bu maddelere ek olarak, toplumun internet ortamında güvende olabilmesi için tüm vatandaşların internete erişirken uymaları gereken temel kurallar bulunmaktadır. Bu kurallardan bazılarına örnek olarak; erişim için seçilen parolanın mutlaka harf, rakam ve noktalama işareti içermesi ve güçlü parolalar yaratılması, aynı parolanın birden fazla yere erişim için kullanılmaması ve kullanılan parolaların en fazla üç aylık periyotlarda yenilenmesi, tüm cihazların mutlaka parola ile şifrelenmesi ve yabancı cihazlardan erişimin mümkün olduğunca kısıtlanması, yabancı adreslerden yönlendirilen e-postaların açılmaması, çevrimiçi tekliflerin ve reklamların birkaç kaynaktan doğrulanması, üye olunan internet sitelerinde mutlaka kişisel bilgilerin sınırlandırılması verilmektedir. Her ne kadar temel kurallar olsa da bilişim teknolojilerinin yaygınlaşmasından çok önce doğmuş (50>) ve bilişim teknolojilerinin yaygınlaşmasından sonra dünyaya gelmiş nesiller (16<) en yüksek tehlike içerisinde olan grupları oluşturmaktadır. Bu sebeple Yeni Zelanda devleti ve işbirliği içerisinde bulunduğu özel sektör temsilcileri toplumsal farkındalık çalışmaları yürütmektedir (Fourie, ve diğerleri, 2014: 182).

3.2.4 Özel Sektör ile İşbirliklerinin Çeşitlendirilmesi

Kamu-özel sektör işbirlikleri geleneksel ve modern güvenlik tehditlerini engellemek için sıklıkla kullanılmaktadır. Liberal ekonominin hâkim olduğu ülkelerin büyük bir çoğunluğunda özel sektör ulusal kritik altyapı sistemlerinin yarıdan fazlasını, kimi ülkelerde neredeyse tamamını elinde bulundurmaktadır. Devletin yalnızca yönlendirici aktör olarak rol aldığı ve özel sektörün daha otonom hareket edebildiği kamu-özel sektör

işbirliği çalışmaları mevcut işbirliklerinin verimliliğini arttırmakta ve sonuç olarak güvenlik kapasitesinin arttırılabilmesine vesile olmaktadır.

Bilgi toplamak, depolamak ve bilgiyi gereken noktalara aktarmak yirmi yıl öncesine kıyasla sıklıkla gerçekleştirilebilecek kadar kolaylaşmıştır. Ancak bu bilgilerin toplanması, depolanması ve aktarılmasın süreçlerinde gerçekleşebilecek siber saldırıların engellenmesi amacıyla politikalar uygulanması da çağın gereklerinden olmuştur. Devlet kurumlarının üstlendiği siber güvenlik yaklaşımları her ne kadar kapsayıcı olsa da, özel sektörün; altyapılara, bilgilerin niteliğine ve maliyet analizlerine bakış açıları daha verimli projeler üretilmesine olanak sağlamaktadır. Kamu-özel sektör işbirlikleri, devletin işleyişinin daha verimli hale getirilmesi için kimi kamu hizmetlerinin özel sektörden alanında uzman kurumlara delege edilmesi yöntemiyle gerçekleştirilebilen, devletin, özel sektörün ve vatandaşların tamamının ortak çıkarını gözeterek oluşturulan işbirliği projelerinden oluşmaktadır.

Devlet kurumları siber güvenlik alanında yol gösterici rol oynamakta ve özel sektör ile işbirlikleri kurmakta ve ortak çıkar anlayışı üzerinden politikalarını yürütmektedir (New Zealand Government, 2019: 9). Yeni Zelanda devleti siber güvenlik altyapısını oluştururken özel sektörün, STK'ların ve günlük hayatta siber alana erişen tüm vatandaşlarının güvenliğini gündemine alarak çalışmalar gerçekleştirmektedir. GCSB yol gösterici bir lider konumunda bulunarak ulusal siber güvenlik altyapısının kurulması esnasında; sorumlulukların paylaşımı, risk yönetimi ve aktif uluslararası işbirlikleri süreçlerini kapsayıcı bir yaklaşım ile yönetmektedir. CORTEX programının hayata geçirildiği 2014 yılı öncesinde siber saldırılar bilhassa 2011-2014 yılları arasında artış göstermiş olsa da, yeterli teknik altyapı tüm ortaklar ile sağlandıktan sonra GCSB son yıllardaki yıllık raporlarında 'aşılamaz siber güvenlik kalkanı' söylemini kullanmaya başlamıştır (GCSB, 2019: 19).

Söz konusu işbirliğinin kurulabilmesi için birtakım şartlar getirilmiştir. Şartlar kamu-özel sektör işbirliklerinin verimini arttırmak amacıyla hazırlanmıştır (The Treasury of the New Zealand Government, 2015: 9):

- Uzun süreli projeler olmaları (20-30 yıl),

- İşbirliği projesinin çıktılarının önceden belirlenmesi,

- Topluma hizmet sağlayacak yeni bir tesis inşası veya mevcut bir tesisin geliştirilmesi projesi olması,

- Hizmetin belli bir kısmının özel sektör tarafından gerçekleştirilmesi,

- Risk faktörlerini ve yönetim görevlerini en iyi üstlenebilecek tarafa sorumlulukların transferi,

- Mülkiyetin devlete, finansmanın özel sektör ortağına ait olması,

- İşbirliği sonucunda yapılan incelemeler ile proje başlangıcındaki çıktıların uyuşması sonucunda devletin kendi tarafına düşen yükümlülükleri gerçekleştirmesi

Kamu-özel sektör işbirliklerinin Yeni Zelanda devleti nezdinde tasarlanması; inşa edilmesi, finansman sağlanması, bakımının yapılması ve işletilmesi adımlarını takip etmektedir. Bu yöntem sayesinde tesiste çıkabilecek herhangi bir sorun özel sektörün işletim süresi boyunca ortaya çıkmakta ve giderilmektedir. Özel sektör ve devlet arasında gerçekleştirilen ilk kamu-özel sektör işbirliği, 2012 yılında Auckland şehrinde bir ilk ve ortaokul tesislerinin yapılmasında kullanılmıştır. Bu projeyi takip eden işbirlikleri içerisinde çeşitli okul, hastane, hapishane gibi birçok tesis bulunmaktadır. Devletin bu tip işbirlikleri aracılığıyla özel sektör ile ortaklıklar kurmasının temel sebepleri arasında; hizmet kalitesinin özel sektör tarafından sağlanan hizmetlerde daha yüksek olması, ticari amaçlar doğrultusunda tasarlanmış tesislerin daha çok kazanç getirmesi ve sözleşmeden cayılması durumunda finansal riskin özel sektöre ait olması gösterilmektedir. Özel sektörün inşa veya revize edilecek tesis hakkında daha fazla bilgi ve tecrübe sahibi olması da kamu özel sektör işbirliklerinin gerçekleştirilmesi için bir diğer sebep olarak verilmektedir (The Treasury of the New Zealand Government, 2015: 14).

Devletin ve özel sektörün ortak çabalarına ek olarak kâr gütmeyen kuruluşlar da Yeni Zelanda toplumunun farkındalık seviyesinin yükselmesinde ve kritik altyapıların korunmasında önemli rol oynamaktadırlar. Örnek olarak, özel sektörün ve Yeni Zelanda vatandaşlarının internete erişimlerinde güvende olmalarını sağlamak amacıyla Netsafe adlı kâr gütmeyen bir kuruluş hizmet vermektedir. Bütçesi çeşitli bakanlıklar ile yapmış olduğu işbirlikleri çerçevesinde oluşturulmakta ve yıllık raporlar ile hesap verilebilirliği görülebilmektedir. Netsafe 7/24, 364 gün yardım hatları üzerinden teknik destek sağlamakta ve siber alanda karşılaşılabilecek her türlü suç unsuruna karşı mücadele vermektedir (NetSafe, 2018: 12).

Bağımsız bir topluluk ve hayır kuruluşu olarak kendini tanıtan Netsafe gönüllülük esaslarına göre çalışmaktadır. Buna ek olarak 157 ulusal ve uluslararası üyeye sahip olup, yönetim kadrosu tüm üyelerin katılımıyla seçilmekte ve yönetişim prensipleriyle idare edilmektedir. Netsafe eğitim bakanlığı ile işbirliği içinde bulunmakta ve okullarda temel siber güvenlik eğitimi vererek farkındalık oluşturmaktadır. Yürüttüğü sosyal sorumluluk ve toplumu bilinçlendirme projeleri sayesinde 2018 yılında Cannes Lions Uluslararası Yaratıcılık Festivali'nde ödüllerinden gümüş ve bronz madalya kazanmıştır. İnternet dolandırıcılıkları ve oltalama yöntemlerine karşı geliştirilen Re: Scam adlı yapay zeka programı ile farklı bir etkinlikte ise altın madalya kazanmıştır. Ayrıca dünya çapında siber güvenlik alanında AR-GE çalışmalarının sayısını arttırmak amacıyla öğrencilere ve işletmelere burs ve hibe dağıtmaktadır. Adalet Bakanlığı ile yürütülen bir işbirliği projesi ile elde edilen bulgulardan bazıları şu şekilde sıralanmaktadır (NetSafe, 2018: 14-15):

- Yetişkin toplum internet üzerinden bilgi edinmek konusunda temel bilgiye sahip olmakla beraber toplumun beşte biri internet ortamında güvende kalmak için ne tür seçenekleri olduğunu bilmemektedir.

- Toplumun yaklaşık olarak üçte biri geçmiş bir yıl boyunca en az bir istenmeyen e-posta almıştır (istenmeyen e-postalar basit reklam içeriklerinden tehdit mesajlarına uzanan geniş bir yelpaze oluşturmaktadır).

- Her on kişiden biri istenmeyen dijital iletişim sebebiyle sosyal hayatında sorunlar yaşamaktadır.

Güncel olarak yürütülen siber güvenlik stratejileri kritik altyapıların korunmasına yönelik kamu yararı ve ortak çıkar prensiplerine dayalı olarak yürütülmektedir. Bu yaklaşım telekomünikasyon altyapıları üzerinde devlet kontrolünün yok denecek kadar az olmasından ileri gelmektedir. Zira bu altyapıların kontrolü yüksek oranda özel sektörün elinde bulunmaktadır. Yeni Zelanda'da mevcut olan telekomünikasyon şirketleri yetkilendirme yöntemi ile kamu özel sektör işbirliklerini idare etmektedir. Telekomünikasyon şirketlerinin rekabet edebilmesi için hükümet şirketlerin kurabileceği altyapı sistemlerine (baz istasyonu, sinyal dağıtıcı sistemler vb.) sınırlama getirerek tekelleşmeyi önlemeyi amaçlamıştır (Shore, Du, ve Zeadally, 2011: 4-5).

Siber güvenlik alanında özel sektör ile kurulan işbirlikleri, Yeni Zelanda devleti, özel sektörü ve vatandaşları arasındaki güven bağını kuvvetlendirerek ortak çıkarlar doğrultusunda daha az müdahaleci politikaların yürütülmesine imkân tanıyacağı öngörülmektedir. Siber alana olan bağımlılık siber alanın daha güvenli hale getirilmesi amacıyla politikalar yürütülmesini gerektirmiş ve sonucunda siber alana entegre çalışan ve dünyanın çeşitli konumlarına mal ve hizmet ulaştırabilen bir özel sektör yaratmıştır. Özel sektör ile yürütülen işbirlikleri kapsamında Yeni Zelanda vatandaşlarının siber güvenlik bilinci STK'ların uygulamakta olduğu farkındalık projeleri sayesinde yükseltilmiş ve siber suçlardan dolayı ortaya çıkan mağduriyetin en aza indirilmesi yönünde politikaların gerçekleştirilmesi esnasında devlet bütçesinden yapılan harcamaların azaltılması sağlanmıştır.

SONUÇ

21. yüzyılın güvenlik ortamı, aktörleri, araçları ve tehditleri itibariyle bir dönüşüm içerisindedir. Güvenlik aktörlerinin çeşitlendiği, güvenlik konularının çok boyutlu bir hal aldığı günümüzde insan eliyle oluşturulmuş siber alan güvenlik ajandasının öncelikli konularından biri konumuna gelmektedir. Gerek güvenlik ortamının geçirdiği dönüşümün açıklanmasında gerekse siber alan başta olmak üzere güvenlik politikalarının şekillendirilmesinde geniş bir perspektife ihtiyaç duyulduğu aşikârdır. Zira siber güvenlik politikalarının inşasında çok paydaşlı politika uygulamaları elzem hale gelirken, kamu-özel sektör işbirliği büyük bir önem arz etmektedir. Söz konusu işbirliğine imkân verecek dinamiklerin ve politika uygulamalarının anlaşılması, siber güvenlik konusunda geleceğe yönelik projeksiyonların sunulmasında ciddi bir noktaya işaret etmektedir.

Bu tez çalışmasında, araştırma soruları kapsamında devletlerin siber güvenlik altyapılarını şekillendirme süreçlerinde özel sektör ile geliştirdikleri işbirliklerinde etkili olan faktörler incelenmiştir. Güvenlik çevresinin çeşitlenen ve derinleşen tehdit unsurları itibariyle düşünüldüğünde, ancak özel sektör ile işbirliklerinin çeşitlendirilmesi ve bütüncül bir yaklaşımın geliştirilmesiyle etkili politikaların elde edilebileceği sonucuna ulaşılmıştır. Bu çerçevede tarihsel süreç boyunca güvenlik kavramının geçirdiği dönüşümün güvenlik arayışlarına etkisi ile devletlerin güvenlik stratejilerini oluştururken ne tür değişkenleri baz aldıkları araştırılmıştır. Çalışmanın hipotezlerinden biri olarak, Soğuk Savaş sonrası dönemde güvenlik ajandasının genişleyerek bireysel, toplumsal, siyasi ve çevresel güvenlik politikalarını içerecek şekilde çeşitlendiği ve derinleştiği ortaya konmuştur. Soğuk Savaş sonrası dönemde siber alanın operasyonel alanlardan biri haline gelmesiyle tehdit unsurlarının sonsuz bir düzlemde çeşitlenerek siber güvenliğin başlıca güvenlik konularından biri haline geldiği gözlemlenmiştir. Siber alan kapsamında, karşılıklı bağımlılıkların artışı ve mevcut kırılganlıkların farklı alanlarda ulusal güvenliği tehdit edebilecek sonuçlar doğurmasıyla, siber güvenlik tehditlerinin ne derece ciddi bir aşamaya ulaştığı ve devletlerin tek başlarına politika geliştirmekte yetersiz kaldığı savunulmuştur.

İnsan eliyle üretilmiş beşinci operasyonel alan olarak karşımıza çıkan siber alanda insan üstü bir tempoyla hareket imkanı ve alanı kazanan aktörlerin artması, devletlerin bu alana entegre olurken öngörülemeyen tehdit unsurları ile karşı karşıya kalmalarına sebebiyet vermektedir. Bu doğrultuda, bu tez çalışmasında siber alanda yaşanan gelişmelerin güvenlik anlayışını ve devletlerin bu konuya yönelik yaklaşımını nasıl dönüştürdüğü sorusuna cevap aranmıştır. Gerek aktörlerin kimlikleri ve kapasitesi, gerekse devletlerin bu alanda sahip oldukları kırılganlıklar, siber güvenlik politikalarının geleneksel yaklaşımların ötesine geçilerek daha geniş ve çok boyutlu bir yaklaşım ile şekillendirilmesini elzem kılmıştır. Güvenliği çok boyutlu bir yaklaşımla ele alan Kopenhag Ekolü çerçevesinde siber güvenlik politikalarının çok taraflı ve çok boyutlu bir

şekilde tesis edilmesi üzerinde durulmuş, siber güvenlik politikalarının şekillendirilme sürecinde özel sektör ile geliştirilen işbirlikleri bu çerçevede incelenmiştir.

Küreselleşmenin ve karşılıklı bağımlılığın karmaşıklaşan yapısı devletlerin kırılganlıkları, kullandıkları araçları ve politika uygulamaları kapsamında etkili olmakta ve siber güvenlik politikalarının bu kapsamda geliştirilmesinin gerekliliğini ortaya koymaktadır. Coğrafi operasyonel alanlar kapsamında, klasik araçlarla kara, deniz ve hava sınırlarının korunması, güvenlik politikalarının dar bir alanını teşkil eder hale gelmiştir. Nitekim sahip olunan teknolojik araçlar ve bilişim sektörünün geldiği noktanın bir ürünü olarak siber alanın ortaya çıkması ve tüm dünyayı birbirine bağlaması sonucunda, mesafeler önemini yitirmiş ve coğrafi konumlarından ötürü dezavantajlı durumda olan aktörlerin hareket kabiliyetlerinin artmasına olanak sağlanmıştır. Zira coğrafi olarak deniz aşırı konumlardan komut verilerek siber alan üzerinden gerçekleştirilen eylemler geleneksel yöntemlere kıyasla oldukça yıkıcı etki yaratabilmekte, kimliği belirsiz aktörler - özellikle de birey düzeyinde - asimetrik güce sahip olabilmektedir. Siber saldırılar aracılığıyla askeri, ekonomik, siyasi ve sosyal altyapıların zarara uğratılmasıyla buradaki unsurlar ulusal güvenliğe tehdit oluşturulabilmektedirler. Örneklendirmek gerekirse; kritik altyapıların işlevselliğinin zarara uğratılması, toplumun ve devletin işleyişinin sekteye uğramasına, hatta toplumda paniğe ve sonuç olarak devletin itibar kaybına neden olabilmektedir. Buna ek olarak, ekonomik sistemlerin zarar görmesi, ticari işletmelerin maddi kayba uğramasına ve uzun vadede ülke ekonomisinin çıkmaza sürüklenmesine sebebiyet verebilmektedir.

Siber alanda öngörülemeyen tehdit unsurlarının varlığı, siber güvenlik altyapılarının maliyetlerinin yükselmesine ve devletlerin tek başına siber güvenlik politikalarını şekillendirmelerini güçleştirmektedir. Bu çerçevede, siber güvenlik politikalarının uygulanması sürecinde aktörlerin rollerini hangi kapsamda değerlendirmek gerektiği sorusu akla gelmektedir. Zira siber güvenlik duvarlarının aşılması ve diğer siber güvenlik protokollerinin başarısız olması durumunda devletlerin ulusal ve uluslararası alandaki itibarlarına zarar verme potansiyeline sahip hassas bilgiler açığa çıkarılabilmekte, son teknoloji ürünü askeri ve ticari ürün tasarımlarının çalınabilmesi veya sızdırılabilmesi mümkün olabilmektedir. Sistem kırılganlıklarının yanı sıra, sistem kullanıcılarının siber alana erişim esnasında uymaları gereken standartların belirlenmesi de gerekmektedir. Zira kullanıcıların kaynağı bilinmeyen bir e-postayı açması sonucunda sistemi korumak amacıyla alınmış olan tüm tedbirlerin geçerliliğini yitirmesi söz konusu olabilmektedir. Bu kapsamda, tüm paydaşların güvende olacağı bir siber alan meydana getirmek amacıyla, ortak çıkarlar doğrultusunda geliştirilecek olan siber güvenlik politikalarının ne derece elzem olduğu ortaya çıkmaktadır.

Bilişim ve haberleşme teknolojilerinin dinamik, kompleks ve dağınık yapılara sahip olmaları sebebiyle, siber güvenlik politikalarının şekillendirilme süreci esnasında risk ve tehdit unsurlarının belirlenmesi oldukça kapsamlı çalışmalar gerektirmektedir. Bu

doğrultuda siber güvenlik politikalarının şekillenmesinde etkili olan başlıca unsurlar incelenmiştir.

Değişen ve dönüşen tehdit unsurları kapsamında devletler, siber güvenlik stratejilerini şekillendirirken devlet dışı aktörlerden kaynaklı olarak ortaya çıkabilecek risk unsurlarını da politikalarına dâhil etmek zorunda kalmışlardır. Siber alanda ortaya çıkan risk ve tehdit unsurlarını oluşturan aktörler yalnızca devletlerle sınırlı kalmamaktadır. Siber alan yapısı gereği gerekli teçhizata, bilgiye ve tecrübeye sahip her boyuttan aktörün bir tehdit unsuru haline gelebilmesine olanak sağlamaktadır. Bunun sonucunda var olabilen asimetrik tehditler siber güvenlik politikalarının kapsamlı olarak şekillendirilmesini gerektirmektedirler. Devletlerin siber güvenlik politikalarını şekillendirirken; kritik altyapılarının korunması, insan kaynağının yetiştirilmesi ve toplumda farkındalık yaratılması ihtiyaçları söz konusu olmaktadır. Bu süreçlerin daha verimli ve etkili bir şekilde yürütülmesi amacıyla devletler yönetişim mekanizmaları aracılığıyla özel sektör ile işbirlikleri kurmaya başlayarak çok boyutlu ve kapsayıcı politikalar oluşturabilmeye başlamışlardır. Siber güvenlik politikalarının şekillendirilmesinde rol alan özel sektör temsilcilerinin devlet kurumları tarafından belirlenen standartlara eksiksiz olarak uyması gerekmektedir. Yönetişim yelpazesinde tanzim etme yöntemine denk düşen bu uygulama siber güvenlik stratejilerinin dayanıklılığı açısından serbest piyasa kontrolüne henüz devredilemeyecek kadar hassas planlamalar gerektirdiğinin kanıtı niteliğinde görülmektedir.

Devlet kurumları haricinde internete bağlı olan diğer tüm sistemleri ve bireyleri korumaya yönelik olan girişimler özel sektörü ve vatandaşları, kanunlar ve işbirlikleri aracılığıyla yönlendirme sürecini gerektirmektedir. Tüm bürokratik ve ticari süreçlerin siber alana entegre edilmiş olması süreçlerin daha hızlı işlemesini ve daha etkili bir şekilde yönetilebilmesini sağlamaktadır. Diğer taraftan, bu süreçlerin siber alana taşınmış olması yeni kırılganlıklar yaratmakta ve siber güvenlik politikalarının kapsamlı bir biçimde geliştirilmesini zorunlu kılmaktadır. Mevcut sistemlerin sayısı, çeşitliği ve niteliği koruma faaliyetlerinin tek başına devlet bütçesi tarafından karşılanmasını güçleştirmekte, bürokratik süreçlerin uzunluğu karar alma mekanizmalarının yavaş işlemesine sebep olmakta ve alternatif çözümler üretilmesi için politikaların geliştirilmesini gerekli kılmaktadır.

Bu tez çalışmasında kamu-özel sektör işbirlikleri çerçevesinde şekillenen siber güvenlik politikalarının temel unsurlarının neler olduğu sorgulanmıştır. Bu çerçevede; ülkede faaliyet gösteren, alanında bilgi ve tecrübe sahibi özel sektör ve STK'lar ile işbirlikleri kurulması aracılığıyla, bürokratik süreçlerin kısaltılabileceği görülmüştür. Altyapı tesislerinin inşası, finanse edilmesi, işletmesi, denetlenmesi ve izinsiz erişim aktivitelerinden korunması süreçlerinin özel sektör tarafından yürütülmesinin siber güvenlik kapasitesinin ve dayanıklılığının arttırılması açısından önem arz ettiği sonucuna varılmıştır. Yönetişim mekanizmalarının siber güvenlik politikalarının şekillendirilme

aşamasında kullanılması; devlet bütçesinin farklı yatırımlar amacıyla kullanılabilmesini, özel sektörün kâr odaklı bakış açısının siber güvenlik politikalarına uyarlanabilmesini ve toplumun daha hızlı ve etkili bir şekilde bilinçlendirilebilmesini sağlamaktadır.

Siber güvenlik politikalarının geliştirilmesi kapsamında değerlendirildiğinde, özel sektörün çeşitli alanlarda gelişebilmesi amacıyla devletin özel sektöre alan yaratması ve teşvikler vermesi kamu-özel sektör işbirliklerinin kurulabilmesi açısından önem arz etmektedir. Devlet bütçesinin ve gözetim mekanizmalarının yetersiz kaldığı noktalarda, ortak amaçlar doğrultusunda siber güvenlik politikalarının şekillendirilebilmesi için kamu-özel sektör işbirliklerine ihtiyaç duyulmaktadır. Özel sektörün gelişmesine destek verilerek devletin sınırlı kaynaklarının farklı yatırımlar gerçekleştirmek amacıyla kullanılabilmesi sağlanmaktadır. Teknolojik gelişmelerin geldiği noktada; daha kapsamlı, çeşitli boyutlarda ve güçte aktörlerin katkıda bulunduğu, ulusal ve uluslararası işbirliğine dayalı bir güvenlik anlayışının oluşturulması siber alana askeri, ekonomik, siyasi, toplumsal ve sosyal anlamda entegre olmayı gerektirmektedir. Siber alanın sunmuş olduğu imkânlar sayesinde görece olarak küçük devletlerin etkili politikalar izleyerek daha büyük ölçekli devletler ile paralel faydalar sağlayabildiği görülmektedir. Siber güvenliğin çok boyutlu yapısının ve yönetişim mekanizmalarının etkinliğinin devletlerin siber güvenlik politikalarını şekillendirme süreçlerine nasıl bir etki oluşturacağının daha iyi anlaşılması amacıyla örnek olarak İsrail ve Yeni Zelanda devletleri seçilmiştir.

İsrail ve Yeni Zelanda devletleri, siber alan içerisinde birleştirici ve bütünleştirici politikalar uygulamakta, küresel güvenlik çalışmalarına destek olmakta ve işbirliği içerisinde oldukları ortaklarını da daha dayanıklı hale getirme çabası içerisinde bulunmaktadırlar. Her iki devletin verimli ve başarılı politikalarının çok paydaşlı anlayışlar ile şekillendirildiği ve bu durumun kamu-özel sektör işbirliklerinin artan önemini kanıtlar bir nitelik arz ettiği hipotezi bu çerçevede tartışılmıştır. Zira haiz olunan tehdit unsurları kapsamında her iki devlet de insan kaynağı yetiştirme ve özel sektör bünyesinde siber güvenlik alanında aktif olarak çalışan şirketlerin ortaya çıkmasına imkân sağlayan politikalar izlemektedirler. İsrail zorunlu askeri hizmet süresince genç vatandaşlarına girişimcilik eğitimleri verirken, Yeni Zelanda üniversiteler bünyesinde bu çalışmaları yürütmektedir. Ayrıca iki devlet de uluslararası anlamda stratejik ortaklıklar kurdukları devletlerin birçoğundan uzak mesafelerde bulunmalarına rağmen sahip oldukları kapasite ve özellikle de siber alandaki itibarları sayesinde kendilerini gösterebilmektedirler.

Bu iki örneğin göreceli olarak küçük devletler olarak nitelendirilebilmesine rağmen, siber güvenlik stratejilerini çok boyutlu güvenlik yaklaşımları çerçevesinde şekillendirmeleri sayesinde siber alanda daha büyük ölçekli ekonomilere, daha stratejik coğrafi konuma ve daha köklü devlet geleneğine sahip devletlere paralel hatta üstün faydalar edinebildikleri görülmektedir. Bu kapasitelerine ek olarak; yüksek teknolojili ürün geliştirebilmekte, istihbarat toplayabilmekte, işbirlikleri kapsamında bu kaynakları ihraç edebilmekte,

alanında uzman personel yetiştirebilmekte ve farkında bir toplum yaratmak amacıyla epistemik topluluklar oluşturabilmektedirler. Çıkarılan yasalar doğrultusunda, özel sektörün siber alana entegre faaliyetler gerçekleştirirken devlet kurumları ile işbirliği içerisinde olması, çok paydaşlı bir yöntem çerçevesinde kapsamlı politikalar geliştirilmesi, devlet ve özel sektör arasındaki güven bağını kuvvetlendirme anlamında etkili olmakta ve siber güvenlik politikalarının devlet, altyapı, toplum, birey güvenliği ve ticari güvenlik alanlarını kapsayan yöntemler doğrultusunda geliştirilmesi için gerekli ortamın oluşmasında önemli rol oynamaktadır.

İsrail tehdit unsurlarıyla çevrelenmiş bir coğrafyada bulunması itibariyle askeri güvenlik politikalarına her zaman öncelik vermiştir. Sahip olduğu askeri birimlerin sayısı ve ölçeği hususlarında dünyada itibar kazanmış olan İsrail, siber tehditlere karşı tedbirler alırken çok boyutlu politikalar izlemektedir. Kritik altyapıların korunmasının gerekliliği ve ulusal güvenliğe yönelik siber risk unsurlarının ortaya çıkması sonucunda İsrail, siber güvenliğini kurumsal bir çerçevede şekillendirmekte ve bunun yanı sıra sınırlı insan kaynağının etkili kullanılmasını sağlamaktadır. Bu sayede sonraki jenerasyonların siber güvenlik alanındaki farkındalık seviyelerinin arttırılması ve siber güvenlik uzmanlarının yetiştirilmesi yönünde atılımlar yapılmaktadır. İnsan kaynağının yetiştirilmesi ve verimli kullanılmasına ek olarak, özel sektör tarafından gerçekleştirilen AR-GE projelerine devlet tarafından aktarılan kaynaklar, sivil yatırımlara verilen önemi göstermektedir. Yıllık GSYİH'nin belli bir kısmının her yıl söz konusu AR-GE çalışmalarına aktarılmakta olması ve OECD ülkeleri arasında son yıllarda özel sektör AR-GE çalışmalarına aktarılan GSYİH yüzdeleri bakımından ilk sıralarda yer alması, İsrail'in siber güvenlik alanında ve yüksek teknolojili ürün geliştirme konusunda başarılı politikalar uygulamakta olduğunu göstermektedir. Ayrıca siber güvenlik alanındaki liderlik iddialarını destekleyici nitelikte olduğu görülmektedir. Bahsi geçen yatırımlar aracılığıyla, siber güvenlik alanında operasyonlar yürüten ticari işletmeler uluslararası platformlarda İsrail'in görünürlüğünü arttırmakta ve özel sektörün bu alanda daha fazla gelişmesi için yeni girişimcileri cesaretlendirmektedir. Mevcut tehdit unsurları sebebiyle, siber güvenlik politikalarının devlet standartları doğrultusunda şekillendiği tanzim etme yöntemi ile yürütülmekte ve buna ek olarak tehdit unsurlarının giderilmesi amacıyla İsrail, uluslararası siber güvenlik hukuku yaratma ve uluslararası normlar oluşturma çabaları içerisine girmektedir. Bu çabaların sonuç vermesi ve siber alanın daha güvenli bir operasyonel alan haline gelmesi durumunda İsrail'in daha az müdahaleci politikalar izleyebileceği öngörülmektedir.

Yeni Zelanda örneği incelendiğinde ise, coğrafi konumu itibariyle dünyanın geri kalanından uzakta bulunması nedeniyle bilhassa askeri, siyasi ve ticari faaliyetlerde etkinlik kazanılması amacıyla politikaların şekillendirildiği ve bu doğrultuda siber alanın aktif kullanımı üzerinde durulduğu görülmektedir. Uluslararası ortaklıkları ve siber alana entegre yürütülen politikaları sayesinde Yeni Zelanda kendisinden daha büyük ölçekli ekonomilere sahip olan ve daha avantajlı coğrafi konumlarda bulunan devletler ile işbirlikleri kurabilmektedir. Yeni Zelanda yıllık olarak siber güvenlik alanındaki

yatırımlarını, maruz kalınan siber saldırıları ve önlenen finansal kayıpları raporlamakta ve şeffaf bir biçimde kamuoyu ile paylaşmaktadır. Yürütülen politikaların ve alınan sonuçların şeffaf bir şekilde paylaşılması, hem devlet hem de özel sektör düzeyinde çözüm arayışlarında alternatifler oluşturulmasını sağlamakta ve ortak çıkarlar doğrultusunda politikalar oluşturulmasına imkân tanımaktadır.

Çeşitlenen tehdit unsurları ve artan hassasiyetler sebebiyle Yeni Zelanda, kamu kurumlarında ve özel sektör bünyesinde istihdam edilmiş olan vatandaşlarının siber güvenlik alanında farkındalık sahibi olmaları amacıyla politikalar geliştirmeye başlamıştır. Özel sektörün ve Yeni Zelanda vatandaşlarının esas olarak deniz aşırı konumlardan kaynaklanan siber saldırılar sonucu meydana gelen mali kayıpları ilerleyen yıllarda siber müdahale ekiplerinin oluşturulmasını gerekli kılmış ve sonucunda siber güvenlik politikaları daha etkili şekillerde uygulanabilmeye başlanmıştır. Ancak Yeni Zelanda'nın siber güvenlik alanındaki esas atılımı 2014 yılında, kritik bilgilerin yer aldığı kamu ve özel sektörün kontrollerinde bulunan bilgi merkezlerine CORTEX adlı yazılımın entegre edilmesi aracılığıyla gerçekleştirilmiştir. Siber güvenlik kapasitesini büyük ölçüde arttıran CORTEX uygulaması ulusal güvenliğe tehdit oluşturabilecek kritik bilgilere sahip tüm kamu ve özel sektör operasyonlarına dâhil edilmiş ve siber dayanıklılıklar iyileştirilmiştir. Siber alanın güvenli bir operasyonel alan olması Yeni Zelanda için hayati bir önem arz etmektedir.

Siyasi ve ekonomik politikaların kesintiye uğramadan gerçekleştirilebilmesi amacıyla Yeni Zelanda siber alanı güvenli hale getirebilmek için önemli yatırımlarda bulunmakta ve bu alandaki uluslararası işbirliklerine destek vermektedir. Özel sektörde aktif operasyon yürüten şirketlerin mal ve hizmetlerini deniz aşırı konumlara ulaştırmaları, kendi aralarında rekabet edebilmeleri ve kâr sağlayabilmeleri açısından elzemdir. Siber alana bağımlı operasyonlar yürüten ticari işletmelerin varlığı, Yeni Zelanda'nın siber güvenliğe önem vermesinin başlıca nedenlerinden birini teşkil etmektedir. Özel sektör ve STK'lar ile yürütülen işbirlikleri Yeni Zelanda'nın kapsayıcı politikalar oluşturabilmesine olanak tanırken, karşılıklı güven bağının oluşumunu sağlayarak zaman içerisinde işbirliklerinin derinleşmesine imkân vereceğinin işaretini vermektedir.

Siber güvenlik politikalarının şekillendirilmesi sürecinde kamu-özel sektör işbirliklerinin artan önemi İsrail ve Yeni Zelanda devletlerinin uygulamakta oldukları politikalar kapsamında analiz edildiğinde; günümüz güvenlik ortamının dinamiklerinin devletlerin siber alandaki tüm paydaşların ortak çıkarını gözeterek politikalarını şekillendirmeleri gerektirdiği sonucuna varılmaktadır. Kamu-özel sektör işbirliklerinin altyapı tesisleri kurulması esnasında üstlendiği rollerin devlet ve özel sektör arasında bir güven bağı oluşturduğu, bu tez çalışmasının diğer bir hipotezini oluşturmaktadır. Bu doğrultuda kamu-özel sektör işbirliklerinin özel sektörün kâr odaklı politikaları ile devletin güvenlik politikalarının ortak çıkarlar doğrultusunda sentezlenmesini gerektirdiği ve başarılı politikaların devlet ve özel sektör arasında bir güven inşa etmekte olduğu sonucuna

varılmıştır. İnşa edilen güven ortamı daha az müdahaleci politikaların uygulanabilmesi için ortam hazırlamakta ve yönetişim prensipleri kapsamında ve ortak çıkarlar doğrultusunda şekillenen siber güvenlik politikalarının uygulanabilmesine imkân tanımaktadır. Ayrıca her iki örnek devletin yetişmiş uzmanları istihdam edilebilecekleri siber güvenlik merkezlerini kurmaları ve AR-GE tesislerinin arttırılması yönünde girişimlerde bulunmaları beyin göçünü azaltmakta ve insan kaynağının etkili kullanılabilmesi açısından fayda sağlamaktadır. Çok boyutlu politikaların uygulanması siber alandaki kırılganlıkların giderilmesi konusunda önemli rol oynamaktadır. Siber alanda katılımcı, çok paydaşlı ve birleştirici politikalar izlenmesi uzun vadede etkili politikaların şekillendirilmesi açısından önem arz etmektedir.

Bu tez çalışmasında kamu-özel sektör işbirlikleri aracılığıyla şekillendirilen siber güvenlik politikalarının konu edilmesi aracılığıyla, İsrail ve Yeni Zelanda devletlerinin izlediği politikalar incelenmiş ve yapılmış olan analizler doğrultusunda literatüre katkıda bulunulması amaçlanmıştır. Belirtilen hususlar çerçevesinde, Türkiye Cumhuriyeti'nin siber güvenlik politikalarının şekillendirilmesi konusundaki tartışmalara ve literatüre katkı sağlanacağı ve perspektif sunulabileceği düşünülmektedir.

KAYNAKÇA

Acharya, A. (2017, March). After Liberal Hegemony: The Advent of a Multiplex World Order. *Ethics and International Affairs*, S. 271-285.

Ağır, B. S. (2011). Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı. *Güvenlik Stratejileri*, Sayı: 22 Sayfa: 100.

Aksu, M., ve Turhan, F. (2012). Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik. *Uluslararası İşletme Fatültesi Dergisi, 4*(2), 69-80.

Andrijcic, E., ve Horowitz, B. (2006). A Macro Economic Framework for Evaluation of Cyber Security Risks Related to the Protection of Intellectual Property. *Risk Analysis*(4), 907-923. Doi:10.1111/J.1539-6924.2006.00787.x

Areng, L. (2016). Role of Military in Cybersecurity. C. Samuel, ve M. Sharma içinde, *Securing Cyberspace: International and Asian Perspectives* (S. 124-134). New Delhi: Pentagon Press.

Assaf, D. (2008). Models of Critical Information Infrastructure Protection . *International Journal of Critical Infrastructure Protection*, 6-14.

Atkinson, J. B. (2008). *The Prince.* Indianapolis/Cambridge: Hackett Publishing Company, Inc.

Balki, S. (2014, May 11). *Biggest Cyber Attacks in History*. List25.Com: https://list25.com/25-biggest-cyber-attacks-in-history/ adresinden alındı.

Barkay, T. (2009). Regulation and Voluntarism: A Case Srudy of Governance in the Making. *Regulation And Governance*(3), 360-375.

Baylis, J. (2008). Uluslararası İlişkilerde Güvenlik Kavramı. *Uluslararası İlişkiler, 5*(18), S. 69-85.

Ben Gurion University of the Negev. (2017, October 30). *The First International Cyber Security Smart Mobility Analysis and Research Test Range, in Partnership with BGU*. Cyber Security Workshop for Future Smart Mobility: https://in.bgu.ac.il/en/pages/news/smart_mobility.aspx adresinden alındı.

Berg, H.-P. (2017). Cyber Security of Critical Infrastructures Such as Nuclear Facilities. *Energetika*, 141-145.

Betz, D. J., ve Stevens, T. (2011). Chapter Two: Cyberspace and Sovereignty. *Adelphi Series, 51*(424), 55-74.

Betz, D., ve Stevens, T. (2011). Chapter One: Power and Cyperspace. *Adelphi Series, 51*(424), 35-54. Doi:10.1080/19445571.2011.636954

Booth, K. (1991, October). Security and Emancipation. *Review of International Studies*(17), 313-326. https://www.jstor.org/stable/20097269 adresinden alındı.

Booth, K. (1997). Security and Self Reflection of a Fallen Realist . *Critical Security Studies: Concepts and Cases* , s. 83.

Booth, K. (2007). *Theory of World Security.* London: Cambridge University Press.

Bossong, R., ve Wagner, B. (2016, October 16). A Typology of Cybersecurity and Public-Private Partnership in the Context of the EU. *Crime Law Soc Change*(67), s. 265-288. Doi:10.1007/S10611-016-9653-3

Börzel, T. A., ve Risse, T. (2002). Public-Private Partnerships: Effective and Legitimate Tools of International Governance. *The Reconstitution of Political Authority in the 21st Century* (S. 1-23). Florence: University Of Toronto.

Brown, G. (2011). Why Iran Didn't Admit Stuxnet Was an Attack. *JFQ*(63,4th Quarter), s. 70-73.

Bures, O. (2016, October 21). Contributions of Private Businesses to the Provision of Security in the EU: Beyond Public-Private Partnerships. *Crime Law Soc Change*(67), s. 289-312. Doi:10.1007/S10611-016-9650-6

Burton, J. (2013). Small States and Cyber Security: The Case of New Zealand. *Political Science, 65*(2), 216-238. Doi:10.1177/0032318713508491

Burton, J. (2018). *Cyber Deterrence: A Comprehensive Approach.* NATO Cooperative Cyber Defence Centre of Excellence (CCD COE).

Buzan, B. (1983). *People, States and Fear.* Brighton: North Carolina Press.

Buzan, B. (1991). *People, States and Fear: An Agenda for International Security in the Post-Cold War Era.* Harvester Wheatsheaf.

Buzan, B. (2004). From International to World Society. *English School Theory and the Social Structure of Globalisation*, S. 48.

Buzan, B., Weaver, O., Ve De Wilde, J. (1998). *Security: A New Framework for Analysis.* London: Reinner Publishers.

Cambridge University Press. (2020). *Cambridge Advanced Learner's Dictionary and Thesaurus*. 03 06, 2020 tarihinde Cambridge Dictionary: https://dictionary.cambridge.org/tr/sözlük/ingilizce/sui-generis adresinden alındı.

Carr, M. (2016). Public-Private Partnerships in National Cyber Security Strategies. *International Affairs*, 43-62.

Cavelty, M. D. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Stuies Review*(15), 105-122.

Charney, S. (2009). *Rethinking the Cyber Threat: A Framework and Path Forward*. Microsoft Corp.: http://www.microsoft.com/downloads/en/details.aspx?displaylang=envefamilyıd=062754cc-be0e-4bab-a181-077447f66877 adresinden alındı.

Choucri, N., Ve Clark, D. D. (2012). *Integrating Cyberspace and International Relations: The Co-Evolution Dilemma.* Explorations in Cyber-International Relations. Cambridge: MIT Press.

Clarke, R. A., ve Knarke, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do about It. *New York:Ecco*, 11-21.

Clayton, M. (2010, Sep 21). Stuxnet Malware is Weapon out to Destroy... Iran's Bushehr Nuclear Plant? *Christian Science Monitor*.

Cohen, M. S., Freilich, C. D., ve Siboni, G. (2015, Dec 29). Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*, S. 1-15. Doi:10.1093/isp/ekv023

Cornish, P. (2015). Governing Cyberspace through Consrtuctive Ambiguity. *Global Politics and Strategy, 57*(3), 153-176. Doi:10.1080/00396338.2015.1046230

Couchri, N., ve Goldsmith, D. (2012). Lost in Cyberspace: Harnessing the Internet, International Relations and Global Security. *Bulletin of the Atomic Scientists, 68*(2), 70-77. Doi:10.1177/0096340212438696

Couchri, N., Madnick, S., ve Ferwerda, J. (2014, Oct 22). Institutions for Cyber Security : International Responses and Global Imperatives. *Information Technology for Development, 20*(2), S. 96-121. Doi:10.1080/02681102.2013.836699

Cox, R. W. (1981). Social Forces, States And World Orders: Beyond International Relations Theory. *Millennium: Journal of International Studies*, vol.10 no.2 126-155.

CSI/FBI. (2003). Computer Crime And Security Survey. Langley, ABD.

Cyberspark. (2017, October 30). *Israeli Cyber Innovation Arena*. Cyberspark Industry Initiative: http://cyberspark.org.il adresinden alındı

Çetinkaya, Ş. (2012-13, Aralık-Ocak-Şubat). Güvenlik Algılaması ve Uluslararası İlişkiler Teorilerinin Güvenliğe Bakış Açıları. *21. Yüzyılda Sosyal Bilimler* (2), 241-260.

Davis, P. K. (2014). *Toward Theory for Dissuasion (Or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy.* Santa Monica, Los Angeles, CA: Rand Corporation. https://www.rand.org/pubs/working_papers/wr1027.html adresinden alındı.

Dedeoğlu, B. (2008). *Uluslararası Güvenlik Ve Strateji.* İstanbul: Yeni Yüzyıl Yayınları.

Demir, S. (2009). Avrupa Güvenlik Mimarisinin Tarihsel Gelişimi ve Türkiye'nin Bu Güvenlik Mimarisindeki Yeri. *Stratejik Araştırmalar Enstitüsü Güvenlik Stratejileri Dergisi, Sayı 9*.

Dewar, R. S. (2014). Triptych of Cyber Security: A Classification of Active Cyber Defence. *6th International Conference on Cyber Conflict* (S. 7-21). Talinn: NATO CCD COE Publications.

Doh, J. P., Teegen, H., ve Mudambi, R. (2004). Balancing Private and State Ownership in Emerging Markets' Telecommunications Infrastructure: Country, Industry and Firm Influences. *Journal Of International Business Studies*, 233-250.

Dunn-Cavelty, M., ve Suter, M. (2009). Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure. *International Journal Of Critical Infrastructure Protection*(2), 179-187. www.elsevier.com/locate/ijcip adresinden alındı.

Encyclopedia Mypedia. (2013). *Mimir Türk Ansiklopedisi/Hukuk ve Devlet/Askeri*. 03 22, 2020 tarihinde Encyclopedia Mypedia: https://mimirbook.com/tr/e1dd4f94d9f adresinden alındı.

Erdoğan, İ. (2013). Küreselleşme Olgusu Bağlamında Yeni Güvenlik Algısı. *Akademik Bakış, 6*(12), 5-8.

Erenow. (2016). *Ancient History and Civilisation/Ancient Greece/ Page 9*. 10 13, 2019 tarihinde Erenow: https://erenow.net/ancient/ancient-greece-from-prehistoric-to-hellenistic-times/9.php adresinden alındı.

Fourie, L., Sarrafzadeh, A., Shaoning, P., Kingston, T., Hettema, H., Ve Watters, P. (2014). The Global Cyber Security Workforce- An Ongoing Human Capital Crisis. *The Global Business And Technology Association*, 173-184.

Fowler, S. (2014, July 18). *Hamas and Israel Step Up Cyber Battle for Hearts and Minds.* BBC News Middle East: https://www.gvsd.org/cms/lib02/pa01001045/centricity/domain/610/2014articlesonpropagandawarwitharab-ısraeliconflict.pdf adresinden alındı.

Freilich, C. D. (2006, Autumn). National Security Decision-Making in Israel: Processes, Pathologies and Strengths. *Middle East Journal, 60*(4), 635-663.

Freilich, C. D. (2013). National Security Decision-Making in Israel: Improving the Process. *Middle East Journal, 67*(2), 257-266. Doi:10.3751/67.2.16

GCN. (2010, 02 15). *Lack of Trust Still Hinders Public/Private Security Efforts*. Government Computer News: http//gen.com/articles/2010/02/15/cybereye-public-private-partnerships.aspx adresinden alındı.

GCSB. (2013). *Annual Report.* Wellington, NZ: Government Communication Security Bureau.

GCSB. (2014). *Annual Report.* Wellington, NZ: New Zealand Government Communications Security Bureau.

GCSB. (2017). *Cortex Frequently Answered Questions*. GCSB Information Assurance: https://www.gcsb.govt.nz/our-work/information-assurance/cortex-faqs/ adresinden alındı.

GCSB. (2019). *Annual Report.* Wellington, NZ: Government Communications Security Bureau.

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict And Security in Cyberspace.* Lausanne: EPFL Press.

Goodman, W. (2010, Fall). Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly*, S. 102-135.

Goodyear, M., Goerdel, H. T., Portillo, S., ve Williams, L. (2010). Cybersecurity Management in the States: The Emerging Role of Chief Information Officers. *Sthrengthening Cybersecurity Series*, 1-44.

Gordon, R. (2014). Privacy, Security and the Cyber Dilemma: An Examination of New Zealand's Response to the Rising Threat of Cyber-Attack. *Master' S Thesis*. Wellington, New Zealand: Victoria University of Wellington.

Grauman, B. (2014). Cybersecurity: The Vexed Question of Global Rules. *Security and Defense Agenda*, 1-104.

Greathouse, C. B. (2014). Cyber War and Strategic Thought: Do Classic Theorists Still Mater? J.-F. Kremer, ve B. Müller içinde, *Cyberspace and International Relations* (s. 21-40).

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

Haan, U. D. (2011). The Israel Case of Science and Technology Based Entrepreneurship: An Exploration Cluster. S. A. Mian içinde, *Science and Technology Based Regional Entrepreneurship: Global Experience in Policy and Program Development* (s. 306-326). Cheltenham, UK: EE Publishing.

Haimes, Y. Y., Ve Longstaff, T. (2002). The Role Of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism. *Risk Analysis: An International Journal*(22), 439-444.

Hare, F. B. (2017, December 26). Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy? *Asian Security*. Doi:10.1080/14799855.2017.1414803

Harel, A. (2013, Oct 12). *Israel's Next War.* Haaretz. adresinden alındı.

Harknett, R. J., ve Stever, J. A. (2009). The Cybersecurity Triad: Governemnt, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal Of Homeland Security and Emergency Management, 6*(1), 1-16. Doi:10.2202/1547-7355.1649

Hensen, L., ve Nissenbaum, H. (2009, March 26). Digital Disaster, Cyber Security and the Copenhagen School. *International Studies Quartely*(53), S. 1155-1175.

Howard, M., Ve Paret, P. (1984). *On War* (Cilt 1). Princeton, New Jersey: Princeton University Press.

Huang, K., Ve Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences* (S. 6398-6407). Hawaii: HICSS. https://hdl.handle.net/10125/60074 adresinden alındı.

INCD. (2018). *Cybersecurity Framework Success Story.* Jerusalem: INCD.

International Court Of Justice. (1996). *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion.* Court Verdict, I.C.J.

Jeffery, G., Ryan, K., Ko, L., Kho, J., Saidah, S., Mark, A., Apperly, M. (2017). Visualizing The New Zealand Cyber Security Challenge For Attack Behaviours. *IEEE Computet Society*, 1123-1130.

Kibaroğlu, P. D. (2014, Kasım 05). Kitle İmha Silahlarının Yayılması Sorunu. *Kitle İmha Silahlarının Yayılması Sorunu*, 7-16. İstanbul, Türkiye: Genel Kurmay Başkanlığı Harp Akademileri Komutanlığı.

Korab-Karpowicz, W. (2006). *How International Relations Theorists Can Benefit By Reading Thucydides.* The Monit.

Korns, C. S. (2009, (3rd Qtr.)). Cyber Operations: The New Balance. *Joint Force Quarterly* (54), 97-100.

Kramer, F. D., Starr, S. H., ve Wentz, L. (2009). *Cyber Power and National Security.* National Defense University Press.

Krause, K., ve Williams, M. C. (1997). *Critical Security Studies.* Minneapolis: University of Minnesota Press.

Kremer, J. (2014, October 30). Policing Cybercrime or Militarizing Cybersecurity? Security Mindsets and the Regulation of Threats from Cyberspace. *Information and Communications Technology Law, 23*(3), s. 220-237. Doi:10.1080/13600834.2014.970432

Küçüksolak, Ö. K. (2012). Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Okulu Çerçevesinde Tartışılması. *Turan Stratejik Araştırmalar Merkezi Dergisi, 4*(14), s. 202-208.

Küçüksolak, Ö. K. (2016). İnsan Güvenliği Kavramının Gelişimi. *Turan-Sam Uluslararası Bilimsel Hakemli Dergisi, 8/KIŞ*(29), 148-160.

Küçüksolak, Ö. K. (2018). Cyberspace: The Fifth Domain of Escalating Security Challenges. *Current Debates in International Relations and Law, 24*(15), 25-42.

Küçükşahin, A. (2006, 04). Güvenlik Bağlamında, Risk ve Tehdit Kavramları Arasındaki Farklar Nelerdir ve Nasıl Belirlenmelidir? *Güvenlik Stratejileri Dergisi, 04*, 7-40. https://www.ceeol.com/search/article-detail?id=38698 adresinden alındı.

Küçükşahin, A., ve Akkan, T. (2007). Değişen Güvenlik Algılamarı Işığında Tehdit ve Asimetrik Tehdit. *Dergipark*, 41-66.

Levi-Faur, D. (2012). From 'Big Government to Big Governance'. D. Levi-Faur, ve D. Levi-Faur içinde, *the Oxford Handbook of Governance* (S. 28-43). Oxford, İngiltere: Oxford University Press.

Libel, T. (2016, March 29). Explaining the Security Paradigm Shift: Strategic Culture, Epistemic Communities and Israel's Changing National Security Policy. *Defence Studies, 16*(2), s. 137-156. Doi:10.1080/14702436.2016.1165595

Libicki, M. C. (2009). *Cyberdeterrence and Cyber War.* Santa Monica, California: Rand Corporation.

Limba, T., Pleta, T., Agafonov, K., ve Damkus, M. (2017, June). Cyber Security Management Model for Critical Infrastructure. *Entrepreneurship and Sustainability Issues, 4*(4), s. 559-573. Doi:10.9770/Jesi.2017.4.4(12)

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 365-404. Doi:10.1080/09636412.2013.816122

Luiifj, H., Besseling, K., Spoelstra, M., ve De Graaf, P. (2013). Ten National Cyber Security Strategies: A Comparison. *CRITIS*, 1-17. Doi:10.1007/978-3-642-41476-3_1

Manly, M. (2015). Cyberspace's Dynamic Duo: Forging a Cybersecurity Public Private Partnership. *Journal of Strategic Security, 8*(5/9), s. 85-98. Doi:10.5038/1944-0472.8.3S.1478

Martin, T. R. (1996). *Ancient Greece: From Prehistoric to Hellenistic Times.* New Heaven: Yale University Press.

Ministry of Finance. (2019). *PPP Projects in Israel* . Jerusalem : Ministry of Finance.

Morgan, S. (2015, Dec 20). *Cybersecurity Market Reaches $75 Billion in 2015: Expected to Reach $170 Billion by 2020*. Forbes: http://www.forbes.com/sites/stevemorgan2015/12/20/cybersecurity%e2%80%8b-%e2%80%8bmarket-reaches-75-billion-in-2015%e2%80%8b%e2%80%8b-%e2%80%8bexpected-to-reach-170-billion-by-2020/#2715e4857a04b4f46d21a2191 adresinden alındı.

NCSC. (2013). *Annual Report.* Wellington: New Zealand National Cyber Security Center.

NCSC. (2013). *The Economic Impact of Cybercrime and Cyber Espionage Report.* Wellington: Centre for Strategic and International Studies.

Netsafe. (2018). *Annual Report.* Auckland, NZ: Netsafe.

Nevill, L. (2016). Challenging Opportunities for the Asia-Pasific's Digital Economy. C. Samuel, ve M. Sharma içinde, *Securing Cyberspace: International and Asian Perspectives* (s. 221-230). New Delhi: Pentagon Press.

New Zealan Government. (2019). *New Zealand's Cyber Security Strategy: Enabling New Zealand to Thrive Online.* Wellington: Crown.

New Zealand Foreign Affairs and Trade. (2020, 02 14). *Cyber Security*. New Zealand Foreign Affairs and Trade: https://www.mfat.govt.nz/en/peace-rights-and-security/international-security/cyber-security-issues/ adresinden alındı.

New Zealand Government. (2011). *New Zealand's Cyber Security Strategy.* GCSB. Wellington, NZ: Prime Minister's Office. www.med.govt.nz/cyberstrategy adresinden alındı

New Zealand Parliament. (2017, Jun 30). *New Zealand's First Constitution Act Passed 165 Years Ago*. New Zealand Parliament: https://www.parliament.nz/en/get-involved/features/new-zealand-s-first-constitution-act-passed-165-years-ago/ adresinden alındı.

Nye Jr., J. S. (2010). *Cyber Power.* Harvard Kennedy School. Cambridge, MA: Belfer Center for Science and International Affairs.

OECD. (2020). *Gross Domestic Spending on Rved Total % of GDP, 2000-2019.* OECD Data: https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm adresinden alındı.

O'Neil, R. (2009). E-Government: Transformation of Public Governance in New Zealand? . *Phd Dissertation* . Wellington, New Zealand: Victoria University of Wellington.

Özdemir, Ö., ve Özdemir, E. (2018, 04 16). Suriyeli Kadınar ve İnsani Güvenlik. *Güvenlik Stratejileri*(27), 9-11.

Peters, G. B. (2012). Governance as Political Theory. D. Levi-Faur içinde, *The Oxford Handbook of Governance* (s. 43-55). Oxford: Oxford University Press.

Ponemon Institute LLC. (2018, July). 2018 Cost of Data Breach Study, Global Overview. *IBM Security*, s. 1-34.

Powell, R. (2003). Nuclear Deterrence Theory, Proliferation and National Missile Defence. *International Security, 27*(4), 86-118. Doi:10.1162/016228803321951108

Prebble, J., Stephens, M., ve Haradasa, T. (2019). On the Constitution of New Zealand: An Introduction to the Foundations of the Current Form of Government. *Victoria University of Wellington Legal Research Papers: Sir Kenneth Keith: Collected Papers*, 1-7.

Prime Minister's Office (2011, August 7). *Advancing National Capabilities in Cyberspace: Government Decision 3611.* Prime Minister's Office: http://www.pmo.gov.il/english/primeministersoffice/divisionsandauthorities/cyber/documents/advancing%20national%20cyberspace%20capabilities.pdf adresinden alındı.

Qi, H., ve Kotz, D. M. (2019, May 25). The Impact Of State-Owned Enterprises On China's Economic Growth. *Review Of Radical Political Economics*, s. 1-19.

Raska, M. (2015). *Confronting Cybersecurity Challenges: Israel's Evolving Cyberdefence Strategy.* S. Rajaratnam School of International Studies. Singapore: Nanyang Technological University.

Razin, E., ve Hazan, A. (2013). Municipal-Private Partnerships in Israel: From Local Development to Budgetary Bypass. P. K. Pradhan, J. Bucek, ve E. Razin içinde, *Geography Of Governance: Dynamics for Local Development* (s. 77-88). Bratislava: International Geographical Union Commission on Geography of Governance(IGUC/GOG).

Rue, R., ve Lawrance Pfleeger, S. (2009, July/August). Making the Best Use of Cybersecurity Economic Models. *The IEEE Computer and Reliability Societies*, s. 52-60.

Sandıklı, A., ve Emeklier, B. (2011). Güvenlik Yaklaşımlarında Değişim ve Dönüşüm. *21. Yüzyılda Yeni Güvenlik Anlayışı ve Yaklaşımları*, (S. 3-68). Kocaeli.

Sarbu, S. (2017, Ocak). The Cyber Threat and the Problem of Information Security. A Critical Analysis of the Concepts of Cyper-Power and Cyber-Space. *Annals- Series On Military Sciences*, 126-138. https://www.ceeol.com/search/article-detail?id=547609 adresinden alındı.

Schaferhoff, M., Campe, S., ve Kaan, C. (2009). Transnational Public-Private Partnerships in International Relations: Making Sense of Concepts, Research Frameworks and Results. *International Studies Review*, S. 11, 451-474.

Schmidt, A. (2014). Hierarchies in Networks: Emerging Hybrids of Networks and Hierarchies for Producing Internet Security. J.-F. Kremer, ve B. Müller içinde, *Cyberspace and International Relations: Theory, Prospects and Challenges* (s. 181-202). Düsseldorf: Springer Science+Business Media.

Shackelford, S. J. (2013). Toward Cyberspace: Managing Cyberattacks through Polycentric Governance. *American University Law Review, 62*(5), 1273-1364.

Shackelford, S. J. (2020). *Governing New Frontiers in the Information Age: Toward Cyber Peace.* Cambridge, United Kingdom: Cambridge University Press.

Shaheen, S. (2014). Offense-Defense Balance in Cyber Warfare. J. F. Kremer, ve B. Müller içinde, *Cyberspace and International Relations* (S. 77-93). Bonn: Springer.

Sheldon, J. B. (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*, 95-112.

Shore, M., Du, Y., ve Zeadally, S. (2011). Public Private Partnership Model For National Cybersecurity. *Policy Studies Organization*, S. Vol 3, Iss 2, Article 8.

Simon Fraser University. (2013). *Human Security Report Project.* Vancouver: Human Security Press.

Singer, P. W., ve Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press.

Sørsensen, E., ve Torfing, J. (2005). Democratic Anchorage of Governance Networks. *Scandinavian Political Studies*(28), 195-218.

Stevens, T. (2012, April 13). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy, 33*(1), s. 48-170. Doi:10.1080/13523260.2012.659597

Strassler, R. B. (1996). *A Comprehensive Guide to the Peloponessian War* (Cilt 1). (R. B. Strassler, Dü., ve R. Crawley, Çev.) New York: Free Press.

Tabansky, L. (2013, July-September). Cyberdefence Policy of Israel: Evolving Threats and Responses. *International Journal of Cyber Warfare and Terrorism, 3*(3), 80-87. Doi:10.4018/İjcwt.2013070106

Tabansky, L., ve Israel, I. B. (2015). *Cybersecurity in Israel.* Tel Aviv: Springer.

Tabansky, Y. (2013, September). Critical Infrastructure Protection: Evolution of Israeli Policy. *Journal of Cyber Warfare and Terrorism, 3*(3), 80-87.

Tangör, B. (2012). Kuramsal Tartışmalar Işığında İnsan Güvenliği ve Politikaları. *Uluslararası Hukuk ve Politika, 8*(30), 59-92.

The Treasury of The New Zealand Government. (2015). *Public Private Partnership Programme: The New Zealand PPP Model and Policy: Setting the Scene.* Wellington, NZ: The New Zealand Government.

Thomas, C. (2000). *Global Governance, Development and Human Security: The Challenge of Poverty and Inequality.* London: Pluto Press.

Thomas, C. (2010, Aug 09). Global Governance, Development And Human Security: Exploring the Links. *Third World Quarterly, 22*(2), 159-175. Doi:10.1080/01436590120037018

Thomas, N., ve Tow, W. T. (2002). The Utility of Human Security: Sovereignity and Humanitarian Intervention. *Security Dialogue, 33*(2), s. 177-192.

Thompson, D. (1990). *Europe since: Napoleon* (16 B.). London, England: Penguin Books.

UNODC. (2019, Februrary). *The Role Of Cybercrime Law*. UNODC: Promoting a Culture Of Lawfulness: https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrimelaw.html#:~:text=cybercrime%20law%20identifies%20standards%20of,infrastructure%2c%20in%20particular%3b%20protects%20human adresinden alındı.

Vacca, A. W. (2011, Dec 02). Military Culture and Cyber Security. *Survival: Global Politics and Strategy*, s. 159-176.

Walden, I. (2003). Computer Crime. C. Reed, ve J. Angel içinde, *Computer Law 5th Edition.* Oxford: Oxford University Press.

Walden, I. (2005). Crime and Security in Cyberspace. *Cambridge Review of International Affairs*, 51-68. Doi:10.1080/09557570500059563

Warfield, D. (2012, May 14). Critical Infrastructres: IT Security and Threats from Private Security Ownership. *Information Security Journal: A Global Perspective, 21*(3), s. 127-136. Doi:10.1080/19393555.2011.652289

Wellington Regional Strategy Office. (2016). *Cyber Security Skills Report.* Wellington: Greater Wellington Regional Council.

Westcott, N. (2008). *Digital Diplomacy: The Impact of the Internet on International Relations.* Oxford Internet Institute.

Worthington, I. (2014). *By the Spear: Philip II, Alexander the Great, and the Rise and Fall of the Macedonian Empire.* Oxford: Oxford University Press.

Yücel, D. M. (2016, Güz). Hukuk ile Savaş Arasında Hobbes, Rousseau, Vatel ve Clausewitz. *Felsefe ve Sosyal Bilimler Dergisi*(22), s. 41-59.

ÖZGEÇMİŞ

Engin SAVÇIN 1992 yılında Sakarya'nın Adapazarı ilçesinde doğmuştur. İlk ve orta öğrenimini Ahmet Akkoç İlköğretim Okulu'nda tamamladıktan sonra lise eğitimini Adapazarı Şehit Üsteğmen Selçuk Esedoğlu Anadolu Lisesi'nde tamamlamıştır.

Yalova Üniversitesi Uluslararası İlişkiler (%100 İngilizce) bölümünde lisans eğitimine 2010 yılında başlayan Savçın, 2012/2013 eğitim öğretim döneminde Uluslararası İlişkiler Bölüm Başkanlığı'nın başlattığı 'Gönüllü Araştırma Görevliliği' programı kapsamında bir yıl süreyle görev almış ve araştırma görevlisi hocalarınca verilen görevleri yerine getirmiştir. 2013/2014 eğitim-öğretim yılı bahar dönemini Erasmus programı kapsamında Slovakya'nın Bratislava şehrinde bulunan 'Comenius University in Bratislava'da tamamlamıştır.

2015 yılında Yalova Üniversitesi Uluslararası İlişkiler (%100 İngilizce) Bölümü'nden mezun olan Savçın 2017 yılında Yalova Üniversitesi Sosyal Bilimler Enstitüsü'nde yüksek lisans eğitimine başlamıştır. Aynı zamanda özel bir kurumda İngilizce Öğretmeni olarak görev yapmakta olan Savçın, 2020 yılında Dr. Öğretim Üyesi Övgü KALKAN KÜÇÜKSOLAK danışmanlığında 'Devletlerin Siber Güvenlik Politikalarının Şekillendirilmesi Sürecinde Kamu-Özel Sektör İşbirliğinin Artan Önemi: İsrail ve Yeni Zelanda Örnekleri' başlıklı tez çalışmasını tamamlamıştır.