YENİ KÜRESEL TEHDİT: SİBER SALDIRILAR

SİBER GÜVENLİK VE POLİTİKA UYGULAMALARI

Editör
Dr. Öğr. Üyesi Fulya Köksoy

nobel

YENİ KÜRESEL TEHDİT: SİBER SALDIRILAR SİBER GÜVENLİK VE POLİTİKA UYGULAMALARI
Editör: Dr. Öğr. Üyesi Fulya Köksoy

Yayın No. :
Eğitim No. :
ISBN :
E-ISBN :
Basım Sayısı : 1. Basım, Eylül 2020

Genel Yayın Yönetmeni : Nevzat Argun -nargun@nobelyayin.com-
Yayın Koordinatörü : Gülfem Dursun -gulfem@nobelyayin.com-

Redaksiyon : Samet Tekin -samet@nobelyayin.com-
Sayfa Tasarım : Leyla Kurt -leyla@nobelyayin.com-
Kapak Tasarım : Mehtap Yürümez -mehtap@nobelyayin.com-
Baskı Sorumlusu : Yavuz Şahin -yavuz@nobelyayin.com-
Baskı ve Cilt : Atalay Matbaacılık / Sertifika No.: 15689-
Büyük Sanayi 1 Cad. Elif Sok. No.:7/236-237 İskitler / ANKARA

Kütüphane Bilgi Kartı

Köksoy, Fulya.
Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları / *Editör: Fulya Köksoy*
1. Basım. XXXII + 496 s. 16x23,5 cm. Kaynakça var, dizin yok.
ISBN:
E-ISBN:
1. Siber Güvenlik 2. Uluslararası Güvenlik 3. Güvenlik Politikaları

Genel Dağıtım

ATLAS AKADEMİK BASIM YAYIN DAĞITIM TİC. LTD. ŞTİ.
Adres: Bahçekapı mh. 2465 sk. Oto Sanayi Sitesi No:7 Bodrum Kat Şaşmaz-ANKARA - siparis@nobelyayin.com-
Telefon: +90 312 278 50 77 - **Faks:** 0 312 278 21 65
E-Satış: www.nobelkitap.com - esatis@nobelkitap.com / www.atlaskitap.com - info@atlaskitap.com

Dağıtım ve Satış Noktaları: Alfa Basım Dağıtım, Arasta, Arkadaş Kitabevi, D&R Mağazaları, Dost Dağıtım, Ekip Dağıtım, Kida Dağıtım, Kitapsan, Nezih Kitabevleri, Pandora, Prefix, Remzi Kitabevleri

BÖLÜM YAZARLARI

EDİTÖR: Dr. Öğr. Üyesi Fulya Köksoy
Batman Üniversitesi
fulyakoksoy@gmail.com
ORCID iD- https://orcid.org/0000-0002-6915-5620

YAZARLAR
BİRİNCİ KISIM
KAVRAMSAL VE TEORİK ÇERÇEVE

BÖLÜM 1: **KÜRESEL SİBER GÜVENLİK: KAVRAMSAL VE KURAMSAL BİR ANALİZ**

Prof. Dr. Nezir Akyeşilmen
Selçuk Üniversitesi
nezmen@yahoo.com
ORCID iD-https://orcid.org/ 0000-0001-8184-5280

Arş. Gör. İbrahim Kurnaz
Selçuk Üniversitesi
ibrahimkrnz.01@hotmail.com
ORCID iD- https://orcid.org/ 0000-0001-7228-6536

BÖLÜM 2: **ULUSAL VE ULUSLARARASI GÜVENLİĞİN BİR BİLEŞENİ OLARAK SİBER GÜVENLİK**

Doktora Adayı Kamil Tarhan
Malezya Uluslararası İslam Üniversitesi
kmltrhn.kt@gmail.com
ORCID iD- https://orcid.org/0000-0003-4668-7920

14. BÖLÜM

SİNGAPUR'UN SİBER GÜVENLİK POLİTİKASI

Aşkın İnci Sökmen Alaca

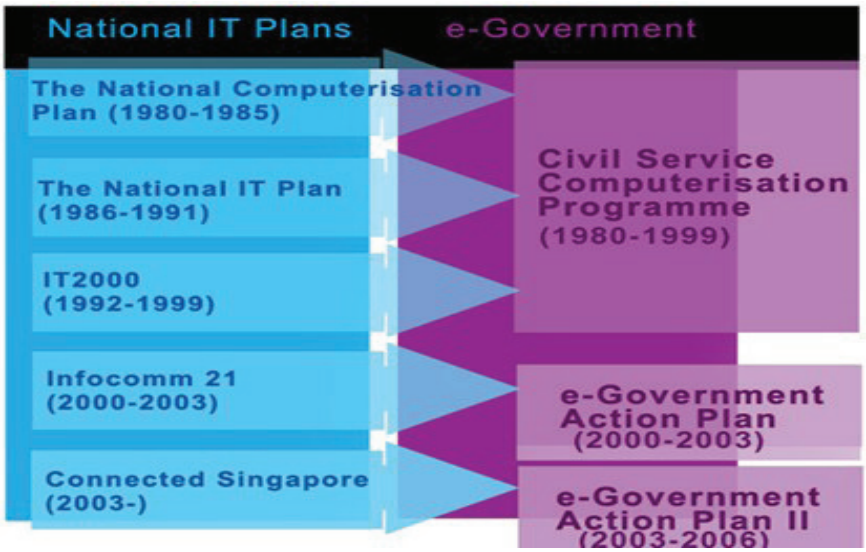
GİRİŞ

Singapur, Güney Doğu Asya'da jeostratejik öneme sahip bir bölgede yer alan, ada niteliğinde, şehir devlet ülkesidir. Altı milyona varan nüfusun büyük çoğunluğunu Han Çinlilerin oluşturduğu çok etnik yapılı toplum, deniz ticaretine dayalı gelişmiş bir ekonomik yapıya sahip ve uluslararası ilişkiler terminolojisinde "*küçük devlet* " statüsünde bir ülkedir. Tarihte bir deniz limanı işlevi gören ülke, günümüzde bir liman konteyner depo merkezi hâline gelmiştir. Aynı zamanda bölgesel finans merkezi olma hedefinde olan bir ülkedir. Yabancı yatırım ve ticaretle kalkınma modelini uygulayan ülke, aynı zamanda yüksek teknolojiyi benimseyerek dijital dönüşümü her alanda başarıyla gerçekleştirmiştir.

Singapur ulusal güvenliği içerisinde, dijital savunma kapsamında yer alan siber güvenlik politikaları bu makalenin konusunu teşkil etmektedir. Hükûmet tarafından kabul edilen siber güvenlik yasası, uygulamalar ve karşılaşılan siber saldırılara değinilecektir. Dünya genelinde model bir dijital toplum, şehir ve siyasal, askerî yapıya sahip ülkenin, siber güvenlik politikaları, diğer devletlere örnek teşkil edebileceğinden önem taşımaktadır.

Akıllı Ulus Olma

Akıllı ulus, teknoloji yardımıyla insanların yaşam kalitesinin en yüksek düzeyde ve daha kolaylaştığı bir toplum, siyaset ve ekonomik yapıya sahip ulus olarak tanımlanır. 1972 yılında ilk Dış İşleri Bakanı Sinnathamby Rajaratnam ülkeyi "*Küresel Şehir*" imajına dönüştürme kararı almasıyla, güncel teknolojiye dayalı yeni bir devlet yaratma ideali benimsendi. İlk olarak 1980-1990 yılı başları arasındaki dönemde, ülke sivil alanda bilgisayar kullanımını yaygınlaştırarak, yazılım ve hizmetleri konusunda bölgesel merkez olmak için faaliyetlerini artırdı. İkinci aşama olarak da 1990 ortaları ve 2010 başları arasında bilgi teknolojileri sanayisinin gelişmesiyle ülke hızlı internet altyapısına sahip oldu. Öte yandan, e- devlete geçiş üç yıllık planlarla 2000-2003 ve 2003-2006 yılları arasında gerçekleşmiştir. Aşağıdaki tabloda beş aşamalı bilgi teknolojilerinin ülkeye yerleştirilmesi görülmektedir.



Şekil 1: Singapur Ulusal IT Bilgi Teknolojileri Planları
Kaynak: (Chua, 2006: 8).

Tümüyle dijital dönüşümü başlatan karar, Kasım 2014 yılında Başbakan Lee Hsien Loong'un Singapur için *"Akıllı Ulus Girişimi*[1]*"* olmuştur (Prime Minister's Office Singapore, 2014). Akıllı ulus olma, fiziksel sınırları kısıtlı küçük bir ada devletinin, dijital alanda küresel ekonomik bağ-

[1] Singapur Akıllı Ulus Stratejisi için Singapur Akıllı Ulus Stratejisi için bkz. (Smart Nation and Digital Goverment Office in Singapore, t.y; Smart Nation Strategy Paper, 2018).

lantılarını güçlendirmesi; rekabetçi yapısını arttırmak için sağlık, ulaşım, şehir çözümleri, finans ve eğitim konularında teknolojik imkânlardan faydalanılması için zorunluluk olmuştur.

Akıllı bir ulus olabilmek için üç alanda, dijital ekonomi, dijital hükûmet ve dijital toplum inşa edilmesiyle mümkün hâle geldi. Teknoloji aracılığı ile Singapur'un akıllı ulusa dönüşümü, ülkenin Teknoloji Bakanlığı[2] (*The Government Technology Agency of Singapore- GovTech*) tarafından, ilk kamusal alanı dönüştürerek dijital hükûmete geçilmesiyle başladı. Sonrasında güçlü bilgi teknolojisi sistemi ve altyapıları kurularak kamu, özel ve bireysel vatandaşların ihtiyaçları karşılanmaya başlandı. Ülkenin bilim, teknoloji, matematik ve mühendislik alanında başarılı insan kaynağı da bu dönüşüm sürecinde yer alarak, süreci hızlandırdı.

Singapur'un hızlı dijital dönüşümü tarafsız bir değerlendirme ile de saptanmıştır. Amerikan merkezli ağ teknoloji şirketi, Cisco'nun 7 parametre üzerinden ülkeleri, dijital hazır oluşlarına göre 2019 *Küresel Dijital Hazır Oluşluk Endeksi* hazırlayarak karşılaştırmıştır. Holistik modele dayanan yedi parametre içerisinde; teknoloji altyapı kapasitesi, mevcut bu teknolojiyi ülkenin her yerine adapte etme, ülke ile dijital alanda kolay yatırım ve iş yapabilme imkânı, dijital alanda yetişmiş insan gücü, bu alandaki kamu ve özel sektör yatırımları, temel insan ihtiyaçları (temiz suya ve elektriğe erişim, ölüm oranı, yaşam süresi gibi) ve Start up[3] şirket sayısı yer almaktadır. Bu endekse göre dünya genelinde Singapur ilk sırada yer alan ülke olmuştur. Lüksemburg ikinci, ABD üçüncü, Rusya kırk beşinci ve Çin elli dördüncü sıradadır. Singapur'u ilk sıraya getiren, güçlü bir devlet desteği ile birlikte, kamu ve özel sektörünün iş birliği içinde dijital bir toplumun yaratılmasıdır (Cisco, 2019).

Dünya çapında Singapur'daki en önemli teknolojik-dijital toplumsal dönüşüm, bileşim teknolojisine dayalı "*akıllı şehirler*" yaratılarak, siyasal açıdan küçük bir balıkçı adasından, dijital şehir devletine dönüşmesidir. Akıllı şehir kavramının evrensel bir tanımı bulunmamaktadır. Genelde varlıkları ve kaynakları verimli şekilde yönetmek için kullanılan, bilgileri sağlamak amacıyla çeşitli türde, elektronik veri toplama sensörleri kullanan bir kentsel alan olarak ifade edilebilir. Ülkenin kritik altyapı tesisleri, şehirlerin tüm yaşamsal aktiviteleri (elektrik, su, gaz

[2] Daha detaylı bilgi için bkz. (The Goverment Technology Agency of Singapore, t.y).

[3] Start Up; yenilikçi bir ürün, süreç ya da servis sunan, sürekliliğe ve gelişmeye açık girişim fikirlerine denir. İlk 2010 yılında ABD'de ortaya çıkarak tüm dünyaya yayılan bir iş modeli akımıdır.

ve enerji, trafik, sağlık, güvenlik, ulaşım, afet yönetimi, çevre yönetimi gibi) yapay zekâ tabanlı bileşim sistemlerine entegre edilmiştir. Akıllı şehirlerin dayandığı en büyük teknoloji, nesnelerin interneti, sensörleri, bağlantı altyapısı ve verilerdir (Akıllı Şehirler, t.y). Hollanda'dan sonra dünyada ikinci ülke olarak insansız otomobiller, 2022 de faaliyete geçecektir. Sürücüsüz kamu araçlarının da toplum içinde kullanılması planlanmıştır. Yangın alanlarında robotik teknolojiye dayalı insanız araç ve ekipmanlar da kent afet yönetimine dâhil edilmiştir. Dünya genelinde Hollanda'dan sonra toplumsal yaşam alanı içerisinde otonom araç kullanmaya hazırlanan ikinci ülke Singapur olmuştur. İlk beş ülke içinde Singapur sonrası Norveç (3), ABD (4) ve İsveç (5) gelmektedir (CIO Middle East, 2019). Akıllı şehir dışında, dijital toplum projesi içerisinde, 2020 yılında tamamlanması düşünülen, Singapur halkına ait "*Ulusal Dijital Kimlik* " projesi kapsamında, ülke vatandaşlarının retina, ses, yüz, parmak izi bilgilerinin yer aldığı, biyometrik kimlik veri bankası oluşturulmuştur (Macaulay, 2019).

IMD Dünya Rekabet Merkezinin, inşalarını takip ettiği akıllı şehirlere dayanarak ilk kez hayata geçirilen, *IMD Akıllı Şehir 2019* İndeksine göre birinci sırada Singapur yer almaktadır. İlk on içindeki diğer şehirler sırasıyla İsviçre Zürih (2), İsveç Oslo (3), İsviçre Cenevre (4), Danimarka Kopenhag (5), Yeni Zelanda Auckland (6), Tayvan'ın başkenti Taipei (7), Finlandiya Helsinki (8), İspanya Bilbao (9) ve Almanya Düsseldorf (10) yer almaktadır (IMD, 2019: 7, 181-183).

Devlet ve toplumsal alanın dönüştürülmesi ile birlikte diğer önemli konu ekonomidir. Dijital ekonomiyi sadece sanayi, uluslararası ticaret bazlı değil, aynı zamanda Singapur'un, Güney Doğu Asya ve Pasifik bölgesinde bir dijital finans merkezi olma isteği vardır. *Akılı Finans Merkez* projesi kapsamında "*Fintech*" yani finansal dijital teknoloji konusunda da yatırımlarını artırmıştır. Bu amaçla Singapur Merkez Bankası (*Monetary Authority of Singapore*) tarafından oluşturulan, *Finansal Teknoloji ve İnnovasyon Grubu,* dijital kimlik, blok zinciri (*blockchain*), kripto paralar, regülâsyon teknolojisi, dijital para gibi bilişim tabanlı finans teknolojilerini, bir *Fintech İnnovasyon Laboratuvarında* geliştirmektedir (CSA, 2016: 15). Örnek vermek gerekirse Singapur Merkez Bankası'nın Singapur Bankalar Birliği ile birlikte 40 finansal ve finansal olmayan şirket ile yürütülen " *UBIN projesi*"[4], dijital para, blok zinciri (*blockchain*) kullanımı ve Dağıtılmış Defter Teknolojisi (*Distributed Ledger Technology*) üzerinde çalışmaktadır (Monetary Authority of Singapore, t.y). Siber saldırıların he-

[4] Detaylı bilgi için bkz. (Monetary Authority of Singapore, t.y).

definde ilk sırada finans ve bankacılık sektörleri gelmektedir. Bu nedenle Singapur siber güvenlik alanında finans teknolojileri açısından, ürünler geliştirmekte ve başarılı girişimleriyle bu alanda cazibe merkezi olmaya çalışmaktadır. Üyesi olduğu, 1994'te kurulan Güney Doğu Asya Uluslar Birliği (ASEAN) bünyesinde, bölgesel iş birliği ve finansal teknolojik ortak merkezi oluşturma çabalarına da öncülük etmektedir.

Dijital dönüşüm sonrası, "*Akıllı Ulus*" olarak nitelendirilen ülke, siber güvenlik konusuna ciddi önem vererek, benimsediği topyekûn ulusal güvenlik stratejisi içerisine dijital savunmayı da eklemiştir. Günümüzde siber savaş, savaş türleri içerisinde beşinci boyut olarak bir ülkeyi etkisiz kılabilir. Nesnelerin interneti (IoT teknolojisi), sensörler, akıllı telefonlar üzerinden veri akışı sağlanabilen ve kontrol edilebilen akıllı şehir sistemlerinin en büyük güvenlik tehdidi, bu dijital yapıya yönelik siber saldırılardır (Pandey ve diğer., 2019). Dijital savunma, akıllı şehirlere sahip, en gelişmiş teknolojiyi kullanan, dışa açık küresel ekonomi ve dünyayla entegre dijital platforma sahip olmasından dolayı bir zorunluluk olarak ortaya çıkmıştır.

Singapur ordusu, dijital modernizasyon çalışmaları sonucu, "*3. Jenerasyon*" modeli olarak günümüzde nitelendirilmektedir. Siber alandaki yeni gelişen saldırı biçimleri ile hibrit savaş modeline yönelik gerekli donanım ordu kabiliyetlerine eklenmiştir. Ordu içindeki siber komutanlık ise 7/24 siber ortamı izlemek, kritik altyapıları siber saldırılara karşı korumakla görevlidir. Uluslararası askerî teknoloji alanında ismi geçen bir ülke olmak için, yapay zekâ yazılımları, robot teknolojisi, büyük veri analizi ve veri madenciliği konularına büyük önem verilerek yatırımlar sürdürülmektedir (MINDEF Singapore, t.y). Ülkenin batısında inşası devam eden "*SAFTI City*" ordu personelinin artırılmış gerçeklik ve simülasyon modelleri üzerinden, şehirlerde konvansiyonel tehdit ve terörizme karşı, eğitim programlarını gerçekleştirmek üzere kurulmaktadır (Zhang, 2019).

Ülkenin polis teşkilatı da suç ve terörizmle mücadelede son dijital ürünler kullanmaktadır. Akıllı şehre dönüşmüş kentlerde, "*Polcam 2.0*" adı verilen kapalı devre kameralarla şehir takip edilirken yollar üzerinde bulunan "*hit and run* " dedektör sistemleriyle olayları hızlıca görüp müdahale etmeleri sağlanmaktadır. Polis arabaları içerisine yerleştirilmiş ekran, özel bir yazılımla ana veri bankasına bağlanarak hızlı bilgi edinmeyi sağlarken şehir navigasyonu üzerinden de trafik durumunu göstermektedir. Polislerin taktığı kasklarda ve gözlüklerde, "*Google Cam Gözlük*" teknolojisi yer almakta, merkezle iletişimi sağlayan ve karşıda duran bireyin

suçlu olup olmadığını belirten yüz tanıma veri bankası bulunmaktadır. Yine polislere özel tahsis edilen cep telefonları içerisinde "*AI Remote*" adı verilen aplikasyon programı; hırsızlık, gasp ve adam kaçırma olaylarında şüpheli şahısların teşhis edilmelerini sağlamaktadır. Kısaca sahada polise yardımcı olabilecek her türlü veri akışı ve donanım dijital olarak sağlanmıştır (Singapore Minister of Home Affairs, t.y).

Dünyada şehirlerini akıllı şehir olarak dönüştüren ilk ülke olarak sayılan Singapur'da; dijital şehirleri, ekonomisini, finansal yapısını, e devlet hizmetlerini ve siyasal seçim güvenliğini, siber alandan kaynaklanan tehditlerine karşı korumak birincil öncelik hâline gelmiştir. Siber alanda devlet sınırı olmayan, saldırı eylemlerinin kimin yaptığı net anlaşılamayan, tüm ülkeyi bir anda çökertebilecek tehditleri içeren, devlet, devlet dışı aktörler ve bireylerin faaliyet gösterebildiği bir alan olarak tanımlanmaktadır. Ülkeler siber güvenlik ve savunma alanında kabiliyetlerini artırdıkça, tehditlerde ona göre yeniden şekillenmektedir. Teknik bir konu olarak siber saldırı, bileşim sistemi kullanılarak yapılan her türlü hareketi içermektedir. Maliyetin düşük olması ve fark edilme zorluğu, siber saldırıları devletlerarasındaki mücadelelerde çekici hâle getirmiştir. İnsanların (hackerların) bu alandaki yetenekleri geliştikçe daha fazla ülkeye bu alanda zarar vermektedirler. Örnek vermek gerekirse akıllı şehirlerin dayandığı nesnelerin interneti teknolojisi, yeni tehditleri de beraberinde getirmiştir. Akıllı ulus kavramı çerçevesinde bilgi teknolojilerine dayanarak yeniden inşa edilen ülkenin, ulusal güvenliğinde birincil öncelikli konu ise sürdürülebilir, güvenli bir siber güvenlik yapısıdır. Bir sonraki bölümde ülkenin tarihsel olarak siber güvenlik politikalarını nasıl oluşturduğuna değinilecektir.

Siber Güvenlik Politikası

Ülkenin tarihsel bazda kamu politikaları içerisinde siber güvenlik yapılanması 2005 yılında başlamıştır. Ancak hukuksal anlamda siber güvenlik kavramının tanımlanması, 16 Mart 2018 yılında yürürlüğe giren, *Siber Güvenlik Yasası*'nda yer almıştır. Ulusal siber güvenlik mevzuatı oluşturmak amacıyla çıkarılan yasanın, ilk giriş bölümünde siber güvenlik "*devletin, sahip olduğu bilgi işlem altyapısı ve sistemine izinsiz giriş ya da saldırı gibi tehditlere karşı cevap vermek, korumak ve savunmak amaçlı gerekli önlemlerin alınması, kritik bilgi tabanlı altyapıların düzenlenmesi ve siber güvenlik hizmeti verenlerin ayarlanması*" olarak belirtilmiştir. Altı bölümden oluşan yasa içerisinde yer alan siber güvenlik terminolojisi bağlamında ilk bölümün ikinci kısmında neleri ifade ettiği açıklanmıştır. Burada yer

alan siber güvenlik kavramı, devletin sahip olduğu bilgi teknolojileri altyapısına yetkisiz giriş ya da saldırının önlenmesi olarak tanımlanmıştır. Devletin bu teknolojilerinin sürekli etkin ve işler olması, korunması ve verilere dayanan bilgi güvenliğinin sağlanmış olması bu kavram çerçevesinde belirtilmiştir. Bilgisayar sistemlerinin güvenliği, bilgi güvenliği ve operasyon güvenliği gibi geniş bir alan tanımlanmıştır (Singapore Status Online, 2018).

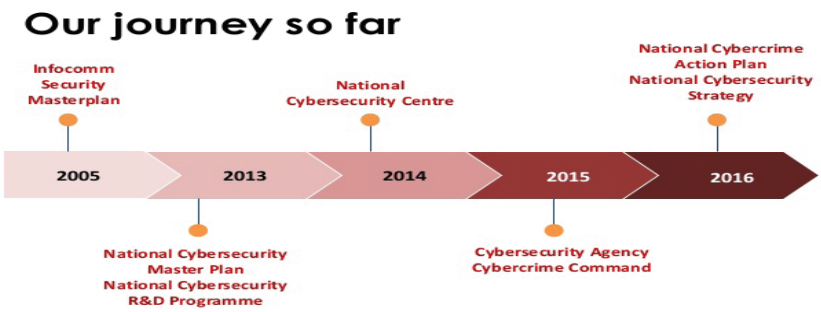
2018 de hukuksal bazda siber güvenlik ve suçlarının belirlenmesinden önce, iki ve dört yıllık yol gösterici master planlar kapsamında siber güvenlik kamu politikaları oluşturulmuştur. İlk olarak *Infocomm*[5] *Güvenlik Master Planı* (2005-2007), ikincisi (2008-2012) yılında hazırlanarak, devletin siber güvenlik faaliyetlerini güçlendirmeyi ve bilgi teknoloji altyapılarının korunması hedeflenmiştir. 2009 yılında kurumsal olarak Singapur Infocomm Teknoloji Güvenlik Birimi oluşturulmuştur. Bu birimin amacı siber saldırılara ve siber istihbarata karşı önlem almaktı. 2013 yılında ise ilk *Ulusal Siber Güvenlik Master Planı* kabul edilmiştir. Bu planda devlet dışında da özel şirketler ve bireyleri de kapsayacak şekilde, siber eko sistemi genişletilmiştir. Temel vizyonda ise ülkeyi siber alanda güvenli bir merkezî ağ konumuna getirmek söz konusu olmuştur. Aynı yılda ülkenin siber güvenlik kapasiteni güçlendirmek için araştırma ve geliştirmeye önem verilerek, *Ulusal Siber Güvenlik Araştırma Geliştirme Programı* başlatılmıştır. Hâlen bu program sürmektedir. 2014 yılında *Ulusal Siber Güvenlik Merkezi* açılarak tehditleri takip, gerçekleşen saldırıları bertaraf etme ve savunmayı güçlendirme faaliyetlerine yoğunlaşılmıştır.

Siber güvenlik alanında en önemli gelişme, açılan güvenlik merkezinin, bir yıl sonra ülkenin siber güvenlik politikalarını icra edecek, merkezî koordinasyon birimine dönüştürülmesidir. 2015 yılında Başbakanlığa bağlı, Singapur İletişim ve Ulaştırma Bakanlığı tarafından yönetilen *Siber Güvenlik Ajansı*[6] (*Cyber Security Agency*) kuruldu. Ajansın temel amacı, ülke ulusal güvenliğinin bir parçası olarak siber alanı korumak, dijital ekonomiyi güçlendirmek ve halkın dijital yaşamını güvenli şekilde gerçekleştirmesini sağlamaktır. Operasyon merkezi

[5] Infocomm - Infocommunications**;** bilgi iletişimi anlamına gelmektedir. Ortak bir internet ya da dijital teknoloji temelinde her türlü elektronik iletişimi içeren, bilgi işleme ve içerik işleme işlevleriyle, telekomünikasyonun doğal olarak genişletilmesidir. Bilgi teknolojileriyle iletişim teknolojilerinin birleşmesidir. Telefon hatları, kablosuz internet ve bilgisayarlar, özel yazılımlar, görsel işitseller bu konu içerisinde sayılır.

[6] Detaylı bilgi için bkz. (CSA, t.y).

olarak, düzenli olarak siber tehditleri izlemek, kritik iletişim altyapılarını korumak, kapasiteyi artırmak, sürekli siber savunma yeteneklerini geliştirmek ve saptanan 11 sektörün kritik bilgi teknolojisi altyapısını korumakla yükümlüdür. Bu sektörler; kamu hizmetleri, elektronik haberleşme, enerji hatları, hava - deniz yolları ve kara ulaşımı, kamu sağlığı, bankacılık ve finans, su şebeke yönetimi, güvenlik ile afet yönetimi ve medyadır (CSA-Cyber Security Agency- Singapore, t.y). Aşağıdaki tabloda ülkenin siber güvenlik politikalarının gelişim süreci görülmektedir.



Şekil 2 : Singapur Siber Güvenlik Politikaları Gelişimi
Kaynak: (CSA, 2016: 7).

Şekil 2'den görüldüğü gibi bu ajansın hazırladığı, ülkenin siber güvenlik stratejisini belirleyen belge, 2016 yılında Singapur Uluslararası Siber Haftasında, Başbakan Lee Hsien Loong tarafından açıklanmıştır. *Singapur Siber Güvenlik Strateji* belgesine göre, ülkenin siber güvenlik politikası dört ana ilkeye dayanmaktadır. Bu ilkeler (CSA, 2016: 4-5);

1. Esnek bir siber altyapı inşa etmek,
2. Güvenli bir siber alan yaratmak,
3. Canlı bir siber güvenlik eko sistemi geliştirmek,
4. Uluslararası iş birliklerini güçlendirmek.

Esnek bir siber altyapı olarak nitelendirilen, kamu otoritesinin, özel sektör operatörleri, servis sağlayanlarla ve kritik on bir sektörün yetkilileriyle çalışma biçimini ifade etmektedir. Dört konuda esnek çalışma üzerinde durulmaktadır. İlki kritik altyapı sistemlerinin korunması için

gerekli donanımı sağlamak, risk analizleri yapmak, acil durum eylem planları oluşturmak ve bu sektör çalışanlarının siber güvenlik tehditleri konusunda farkındalığını geliştirmektir. Belirlenen on bir kritik sektör için koruma programı oluşturulmuştur. Üretilecek yeni siber güvenlik ürünlerinde temel ilke, maksimum seviyede güvenlik (*Security by Design* kavramı) sağlayabilecek bir özelliğe sahip olması şarttır. Oluşan siber tehdide hızlı tespit ve erken müdahale edebilmek ikinci konuyu oluşturmaktadır. Bunu gerçekleştirebilmek için strateji belgesinde *Ulusal Siber Olaylara Müdahale Timleri* oluşturulması kararlaştırılmıştır. Anlık oluşan saldırılara karşı, hızlı operasyonel cevap verme, siber güvenlik açısından önem taşıyan bir konudur. Üçüncü konu siber güvenlik yönetimi ve siber güvenlik mevzuatının sürekli geliştirilmesi ve son olarak da kamu operatörlerini ve sistemlerini azami şekilde güvenli hâle getirmektedir (CSA, 2016: 9).

Singapur hükûmeti, risklerin ve tehditlerin hızla değiştiği siber alanda, bu tehditlere hızla cevap verebilmek için, *Ulusal Siber Güvenlik Tehditlerini Karşılama Planı* hazırlamıştır. Bu planda ilk olarak öncelikle ulusal güvenliği tehdit eden, diğer devletlerin siber saldırılarına karşı, e-devlet, askerî ve kritik altyapı projelerinde devlet sırlarının korunması, siber ortamda üretilen bilginin/verinin güvenli şekilde muhafaza edilmesi, erişilebilirliğinin güvence altına alınması yer almaktadır. Ulusal güvenlik teorisi kapsamında güçlü bir savunmanın yanında, saldırgan eylemlere karşı caydırıcı olmak da birincil önceliktir. Siber güvenlik ve savunma alanında caydırıcılık, siber ortamda bir güvenlik duvarı oluşturma, veri kaçaklarını önleyecek bariyer geliştirme, web uygulama güvenliği, saldırganın eylemini hızlı tespit ve erken müdahale ile geri çevirmek, saldırganı tanımlayarak cezalandırmaktır. Planda bu nedenle ilk sırada devlet uygulamaları konulmuştur. İkinci olarak kritik altyapı sektörleri ve üçüncü olarak da spesifik operatörlere yönelik saldırılara hazırlık yer almaktadır. Bu plan Siber Güvenlik Ajansı ile diğer sektör yetkililerinin yakın çalışmasını öngörmektedir (CSA, 2016: 16).

Siber güvenlik strateji belgesinde öne çıkan diğer önemli bir husus, uluslararası iş birliklerinin güçlendirilmesidir. Dijital ortamda ülkelerin birbirlerine ekonomik, bilgi, haber ağı üzerinden bağlı hâle geldiği küresel ağ toplumunda, bir ülke tek başına siber tehditleri bertaraf ederek savunmasını güçlü kılamaz. Siber tehdit istihbaratı edinimi ve paylaşımı ülkeler arasında kilit rol oynarken karşılıklı ikili anlaşmalarla teknolojik yönden siber güvenlik kapasitelerinin geliştirilmesi de önem kazanmıştır. Siber alanda teknolojik ve tehdit istihbaratı bilgi paylaşımı amaçlı Singapur hükûmeti, birçok ülkeyle mutabakat zap-

tını (*Memorandum of Understanding*), Siber Güvenlik Ajansı aracılığı ile gerçekleştirilmektedir. Bu ülkeler, ilk olarak Fransa (2015) ile başlamış, Birleşik Krallık (2015), ABD (2016), Hollanda (2016), Avustralya (2017), Japonya (2017), Almanya (2017), Hindistan (2018), Kanada (2018), Güney Kore (2019), Yeni Zelanda (2019) ile devam etmiştir. Nesnelerin İnterneti teknolojisinin (IoT) güvenliği konusunda Hollanda Ulusal Siber Güvenlik Merkezi ile ortak bir yayın[7] çıkarılırken İngiltere ile bu konuda teknolojik iş birliğine gidilmiştir. Kâr amacı taşımayan, küresel siber eko sistemini daha da güvenilir kılmak için oluşturulmuş *Cyber Green*[8] organizasyonunda Japonya, İngiltere ile birlikte Singapur da yer almaktadır. Bu organizasyon dünya siber ağı içerisindeki, siber riskler ve zayıf serverlar konusunda yayınlar yapmaktadır. Singapur, ASEAN üyelerine bu organizasyonun portalına erişim imkânı sağlayarak, güvenliklerini karşılaştırarak bir değerlendirme yapma imkânı vermektedir (CyberGreen, t.y).

İkili iş birlikleri askerî alanda da sürerken, 2018 yılında Estonya ile yapılan iş birliği çerçevesinde, Estonya Savunma Kuvvetleri Cyber Range (EDFCyR), Singapur Savunma Bakanlığı ve Singapur Silahlı Kuvvetlerine siber güvenlik eğitim desteği sağlamaktadır. Ayrıca Uluslararası alanda, siber suçları takip amaçlı, üretim sağladığı siber istihbaratı, üyesi olduğu, Interpol (Uluslararası Kriminal Polis Teşkilatı) ile paylaşarak, karşılıklı bilgi alışverişi yapmaktadır. Singapur aynı zamanda Interpol'ün tüm üyeleri için siber suçlar konusunda uluslararası operasyonlarını gerçekleştirdiği, *Innovasyon için Küresel Kompleks* merkezine ev sahipliği yapmaktadır. Böylece bu merkez üzerinde diğer Interpol üyeleriyle siber suçlara karşı sınır ötesi operasyonlarda yer almaktadır (CSA, 2016: 45).Ülkenin siber güvenlik politikasında böylece, siber tehdit istihbarat paylaşımı kapsamında "*bilgi güçtür*" ve uluslararası iş birlikleriyle "*hep beraber daha güçlüyüz*" vizyonun hâkim olduğu görülmektedir.

Bulunduğu Güney Doğu Asya bölgesinde, siyasi ve güvenlik konularında üye ülkeler arasında karşılıklı diyaloğu geliştirmek amaçlı kurulan ASEAN örgütünün, gelişen uluslararası olaylara paralel ajandasında siber güvenlik de yer almaktadır. Uluslararası örgütün siber kapasitesini geliştirmek amaçlı, operasyonel, teknik, yasal, siber politikaların oluşturulması ve diplomatik konulardaki girişimlere Singapur da katkı

[7] Yayın konusunda daha detaylı bilgi için bkz. (Staalduinen ve Joshi, 2019).

[8] Bkz. (Cyber Green, t.y).

sağlamaktadır. 2012 yılında örgüt bünyesinde Bilgisayar Acil Müdahale Timi oluşturulmuştur. Karşılıklı diyalog ve iş birliğinin geliştirilmesi amaçlı üye ülkeleri birbirine bağlayan, ASEAN Güvenlik Eylem Konseyi Network'u (ANSAC) oluşturulmuştur. Diğer yandan, farklı zamanlarda ASEAN bölgesel forumlar gerçekleştirerek siber güvenlik ve siber suçlar konuları görüşülmektedir. Ayrıca *ASEAN- Singapur Siber Güvenlik Mükemmeliyet Merkezi* Nisan 2020'de açılarak, diğer üye ülkelerle bu alanda faaliyetlerin geliştirilmesine çalışmaktadır. Siber alanda uluslararası düzene dayalı kuralların oluşturulması amacıyla ASEAN üyeleri, 2015 yılında hazırlanan Birleşmiş Milletler Hükûmet Uzmanları Raporuna, on bir bağlayıcı olmayan norm önermiştir. Uluslararası hukukta siber güvenlik alanında bağlayıcı olan sözleşmeler ve statüler yanında, bağlayıcılığı olmayan rehber kurallara Singapur'un üyesi bulunduğu ASEAN örgütü ile katkıda bulunduğu görülmektedir. Ayrıca Singapur, siber alanda norm geliştiren, politikalar oluşturan, ulusal ve uluslararası siber hukuk mevzuatı çalışmaları yapan, siber caydırıcılık ve siber suç konusunda bölgesel ve uluslararası iş birliğine önem veren bir ülke olarak görülmektedir (CSA, 2016: 45-46).

Sadece kamu politikaları arasına alarak savunma amaçlı değil, siber güvenlik alanında üretilen ürünleri dış dünyaya pazarlayarak ekonomik gelir elde etmek de ülkenin hedefleri arasındadır. 2018 sonu verilerine göre Singapur siber güvenlik endüstrisinin net değeri, 500 milyon dolardır. Bu değerin 2022 yılı sonunda 1.1 milyar dolar olması beklenmektedir (Yılmaz, t.y). Singapur hükûmeti bu alanda şirketleri destekleyici ve kolaylaştırıcı olmakta, üniversiteler ile ortak eğitim programları ve projeler düzenleyerek yetişmiş nitelikli insan gücü ve ürünlerin gelişmesini sağlamaktadır. Küçük bir devlet olmasına rağmen, siber alanda elde ettiği başarılar, yine bu alanda öne çıkan İsrail, Estonya gibi küçük devletlerle birlikte, *baskın bir güç* olarak teknoloji konusunda ön plana çıkmasını sağlamıştır. Ülke genelinde farklı zamanlarda yapılan bu alandaki uluslararası konferanslar (2016'dan başlayıp her yıl yapılan *Singapur Uluslararası Siber Haftası*[9] *- Singapore International Cyber Week* gibi), siber güvenlik alanında çalışan dünya genelindeki uzmanların ülkeyi yakından görmelerini, uluslararası-bölgesel yeni networkların kurulması ve siber güvenlik alanında ortak iş birliklerini sağlamaktadır. Bu husus Singapur için gündemdeki konuları tartışılabilen ülkelerin siber güvenlik deneyimlerini aktardıkları platformlar olarak, kendi bilgi ve deneyimlerini paylaştığı bir ortam yaratmaktadır.

[9] Detaylı bilgi için bkz. (Singapore International Cyber Week, t.y).

Singapur'un tüm bu siber güvenlik yapılanmasının, başarılı ya da yetersiz kaldığını ölçebildiğimiz kriterler de vardır. BM Bilgi ve İletişim Teknolojileri özel ajansı, Uluslararası Telekomünikasyon Birliği (ITU) tarafından yayımlanan, dünya genelinde 164 ülkeyi, beş ana başlık altında değerlendiren *Küresel Siber Güvenlik Endeksi* bulunmaktadır. Bu başlıklar; siber güvenlik hukuksal mevzuatı, teknik açıdan siber güvenlik kapasite inşası, organizasyon yapısı, bu alanda istihdam ettiği insan kaynağı, ulusal ve uluslararası çapta iş birlikleridir. Singapur, 2018 verileri bulunan bu indekste Asya Pasifik bölgesinde birinci iken küresel sıralamada ise altıncı sırada yer almıştır (Global Security Index, 2018: 58). İlaveten 2018 yılında başlatılan, ülkenin internette gezinti yapma konusunda kamu-özel sistem ayrımı, Singapur ordusu tarafından başlatılan, bilgi sistemlerindeki açıkları bulma programı ve sanayi kesimine yönelik siber kontrol sistemleri rehberi de onu ilk sıralara taşıyan uygulamalarıdır.

Singapur'un siber güvenlik ve savunma da etkili bir yapılanma kurup kurulmadığını ölçen diğer bir faktör ise bir sonraki bölümde ele alınacak, karşılaşılan siber tehdit saldırıları, bu saldırılara yapılan müdahale ve sona erdirme hızıdır.

Karşılaşılan Siber Güvenlik Tehditleri

Ulusal güvenlik içerisinde yer alan siber güvenlik tehditleri, askerî ve kamusal ağlara zararlı yazımların bulaştırılması, devlet sırlarının açığa çıkarılması ve sürekli veri sızdırma, web uygulama güvensizlikleri, kablosuz ağların getirdiği güvenlik açıkları, kimlik bilgilerinin çalınması, kritik su-elektrik-enerji ve nükleer santrallere yapılan siber saldırılar, fidye yazılım saldırıları gibi çok geniş bir eylemi içermektedir. Singapur'da benzer saldırılara maruz kalmış bir ülke olarak, her yıl siber güvenlik ajansı tarafından yayımlanan, ülkenin siber alandaki faaliyetleri ülke ve dünya kamuoyu ile paylaşmaktadır.

2020 de yayımlanan bir sene önceki raporunda, öncelikle Çin'in Wuhan kentinde başlayan Covid-19 Pandemi küresel krizinin, siber alanda yeni tehditler yaratıldığına değinilmiştir. Dünya genelinde sokağa çıkma yasaklarıyla evden çalışma, eğitim gibi tüm yaşamsal faaliyetlerin en çok gerçekleştiği yer siber alan olmuştur. Bu alanda kişisel veri hırsızlığı, fidye yazılımlar, web sayfasını devre dışı bırakma, mobil ve internet cihazlarla casus yazılımlar yükleme, bilgisayar oyunları aracılığı ile casus yazılım yükleme, covid-19 ile ilgili sahte web sayfaları açarak algı yönetimi yapma, ülke vaka sayılarını uzaktan değiştirme, aşı çalışmalarının çalınması (ABD-İngiltere), Dünya Sağlık Örgütüne yönelik siber saldırılar, sosyal

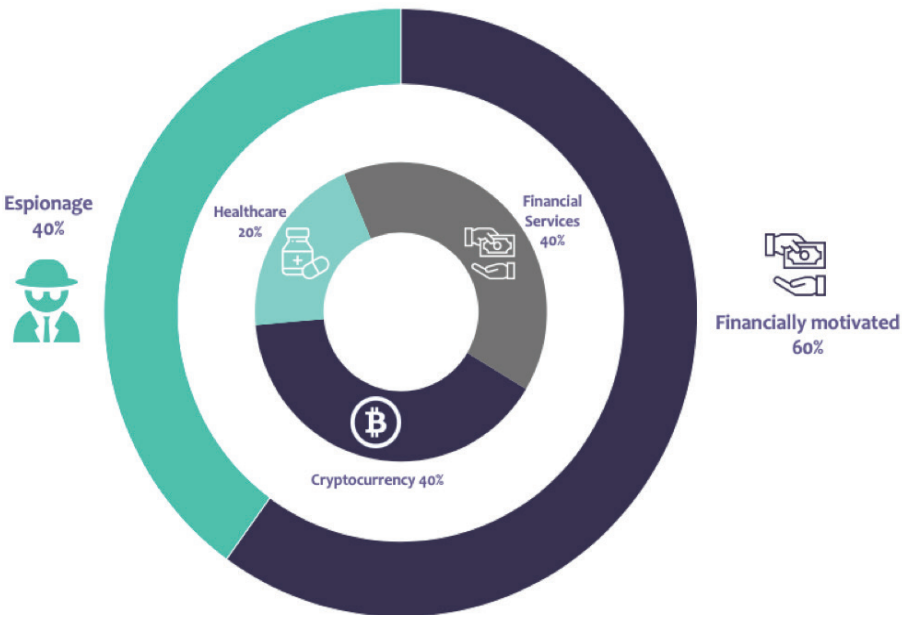
medya verilerinin çalınması gibi örnekler bu dönemde en çok karşılaşılan siber eylemlerdir (Singapore Cyber Landscape 2019, 2020: 48-49). Bu olaylardan biride Singapur da gerçekleşmiştir. Millî eğitim diğer birçok ülkede olduğu gibi, merkezi ABD'de bulunan, Çin kökenli bir işadamı tarafından kurulan, "*Zoom programı*" üzerinden devam ederken 9 Nisan 2020 coğrafya dersinde, iki bilgisayar korsanı siber saldırı düzenleyerek eğitimin yarıda kesilmesini sağlamıştır. "*Zoom Bombing*" adı verilen, çevrim içi platformların açıklarını bularak, bunlara sızan ve yapılan toplantı, ders gibi görüşmeleri hedef alan bu saldırılar, Singapur'da uzaktan eğitimde zoom programından vazgeçilmesiyle sonuçlanmıştır. Veri güvenliği ve veri açıkları bakımından yetersiz görülen bu program, ABD Senatosu, Alman Dış İşleri Bakanlığı, Tayvan ve Avusturya Savunma Bakanlığı tarafından da kullanılmaktan vazgeçilmiştir (Siber Bülten, 2020).

Ülkenin karşılaştığı en büyük siber saldırı, geniş çaplı kimlik veri hırsızlığıdır. 2018 yılında, dünyada kamusal sağlık sistemine yönelik siber saldırı tek örnek olarak gerçekleşmiştir. Verilerin içerisinde Başbakan Lee Hsien Loong'un kişisel sağlık bilgilerinin de yer aldığı, SingHealth kamu sağlık sisteminden hackerlar, 1.5 milyon kişinin verilerini kopyalayıp, 160 bin hastanın ilaç dağıtım kayıtlarını ele geçirmiştir (Bilgi Güvende, 2018). Tüm ülkenin sağlık güvenlik sistemine yönelik gerçekleştirilen, medikal istihbarat amaçlı veri hırsızlığının, Symantec firması tarafından, "*Whitefly*" adı verilen devlet destekli istihbarat grubu tarafından gerçekleştirildiği saptanmıştır (Moon, 2019). Hâlâ üzerinde kafa yorulan küresel Covid-19 pandemisi öncesi, ülkelerin sağlık verilerinin çalınması, ulusal güvenlikleri için büyük bir risk taşımaktadır. 2019'da yine bir kimlik verileri sızdırma olayı ülkede gerçekleşmiştir. Savunma Bakanlığı'nın ve Singapur Silahlı Kuvvetleri'nin toplam 2400 personelinin bilgileri, gönderilen bir e-mail aracılığıyla oltalama (*phishing*) yapılarak iki aracı firma yüzünden sızdırılmıştır (Chong, 2019). Kuzey Kore'nin gerçekleştirdiği düşünülen bu tarz kimlik avları konusunda ise ülkeler uyarılmaktadır.

2019 da ülkede gerçekleşen siber suç oranlarında bir önceki yıla göre, %51,7 artış ile 9.430 olay gerçekleşmiştir. Bu ise tüm suçlar içerisinde dörtte birinden fazlasını oluşturmaktadır. Online chat sitelerinde ağırlıkla gelişen bu olaylar içerinde, sahte e ticaret siteleri ile dolandırıcılık da geniş yer almaktadır. Zararlı yazılım yükleme anlamına gelen oltalama 47.500 kere gerçekleşirken hedef alınan sektörler sırasıyla teknoloji, bankacılık ve finans sektörleri ile e mail servis sağlayıcılarıdır. En çok hedef alınan devlet kurumları ise sınır kapılarında yer alan göçmen büroları, Çalışma Bakanlığı ve Singapur polis departmanıdır. Web sayfalarına yönelik toplam saldırı 873, tespit edilen 35 fidye yazılımı, temelinde DDosS (da-

ğıtık servis dışı bırakma), botnet saldırıları ise (büyük zombi pc ağı) 2300 kez gerçekleşmiştir. Fidye yazılımların hedefinde turizm, hava ulaşımı, imalat ve lojistik sektörlerinin hedef alındığı görülmektedir. Kimlik avı vakaları 2018'de 16.100 URL (internet adresi) iken 2019 da 47.500 URL'ye ulaşmıştır (Singapore Cyber Landscape 2019, 2020: 4-5).

Şekil 3'teki tüm veriler sonucunda, Singapur siber tehdit alanı bir bütün olarak gösterilmiştir. En büyük oran %60 ile parasal kazanç amaçlı, %40 finansal hizmet veren banka ve döviz bürolarına yönelik saldırılar, %40 kripto paralar ve kripto para ile gerçekleşen ticari alanlar, %20 sağlık sistemine yönelik saldırılar ve %40 ülkenin jeostratejik konumu nedeni ile istihbarat toplama amaçlı gelişen eylemlerden oluşmaktadır.



Şekil 3: 2019 Singapur Siber Tehdit Alanı
Kaynak: (Peh, 2019).

Singapur'da 2019 da gerçekleşen siber saldırı olayları içerisinde cep telefonlarının hacklenmesine yönelik olaylarda da artış olmuştur. Askerî ve sivil kurum ağlarına zararlı yazımların bulaştırılmasında mobil cihazların ele geçirilmesi ise önem taşımıştır. Hacklenen mobil cihazların günlük işlemleri takip edilerek istihbarat toplanmıştır. "*Pegasus*" adı verilen, hem IOS hem de Android işletim sisteminde çalışan, zararlı yazılım aralarında Singapur'un da bulunduğu 45 ülkede mobil istihbarat gerçekleştirmiştir (Cimpanu, 2018).

Nisan 2021 yılında gerçekleşmesi planlanan Singapur genel seçimleri öncesinde, Siber Güvenlik Ajansı seçime katılacak siyasi partileri, siber tehditler ve dış devletlerin seçimlere müdahale konusunda uyardı. Dünya genelinde 2017'de Fransız Başkanlık ve Alman Federal seçimlerinde, 2018'de Amerikan Başkanlık ile İtalyan genel seçimlerinde gündeme gelen siber tehditler ve seçim güvenliği konusu artık tüm devletleri de endişelendirmektedir. Özellikle parti liderlerine ait özel hayatla ilgili veri hırsızlığı, mail hesaplara izinsiz erişim ve yabancı devletlerin algı operasyonlarının gerçekleşebilme ihtimali karşısında dikkatli olunması gerekliliği belirtilmiştir. Seçim güvenliği, yeni bir siber tehdit alanı olarak böylece siber güvenlik alanına dâhil edilmiştir (Yu, 2020).

Yapay zekâ teknolojilerinin gelişmesiyle bilişim saldırılarının özellikle dijital para hırsızlığı, fidye yazılımları, kritik altyapılara yönelik siber saldırıların, mobil tehditlerin, internete bağlı cihazların ve bulut tabanlı depolama platformlarının hedef alınmasında, bu teknolojinin kullanılarak gerçekleştirileceği öngörülmektedir. Bu nedenle siber güvenliğinde yapay zekâ tabanlı yazılım esnekliğini, ağ saldırı tespitini, zararlı kod-url-botnet saptanmasını, spam filtreleme, kullanıcı doğrulama, tehdit analizini hızlı yapabilen ve saldırılara cevap verebilen yazılımlar ve erken tespit gibi yöntemlerin geliştirilmesi gerektiği vurgulanmaktadır. Nesnelerin interneti ise giyilebilir sağlık teknolojilerini kullanan bireylerin bio hacking saldırısına uğramalarına neden olabilir. APT olarak adlandırılan " Gelişmiş Sürekli Tehdit- *Advanced Persistent Threats*" ya da " Hedef Odaklı Saldırılar", siber savaş silahları, olarak devletlerin kamu kurumlarını, kritik altyapılarını ve büyük şirketleri hedef almaktadır. Bu saldırılardan en bilineni 2010 yılında İran'da nükleer santrale yapılan Stuxnet siber saldırısıdır. Siber savunmada özellikle karar, destek, farkındalık ve bilgi yönetimi konusunda, algoritma yapay zekâ yazılımlarının kullanımının yaygınlaştırılması, Singapur siber güvenlik hedefleri arasındadır.

SONUÇ

Uluslararası siber güvenlik ülke karşılaştırmalarında ilk sıralarda yer alan, küçük bir ada ülkesi Singapur planlı bir biçimde büyük küresel aktörlerin karşısında, teknolojik yönden kendini geliştirerek akıllı bir ulus inşa etmeyi başarmıştır. Dijital devlet yapılanmasının en güzel örneklerinden olan ülke, küresel ısınma sonrası yükselen deniz seviyesiyle tümden batma tehlikesi altında olsa da dış politika ve ekonomik ilişkilerde diplomasi, uluslararası hukuk ve yeni girişimlerle norm yapma süreçlerinde önderlik etmektedir.

Aynı çabayı siber güvenlik alanında da gösteren Singapur, bulunduğu kritik stratejik bölgede ABD-Çin rekabeti arasında kalırken nüfusu içinde bulunan %76'lık Han nüfusla ona rakip bir kalkınma modeli olarak da durmaktadır. Çin'in yeniden modernizasyonunda örnek aldığı ülke, günümüzde yabancılara ciddi istihdam sağlayarak dijital alandaki insan işgücü potansiyelini iyi değerlendirmektedir. Küresel aktör rekabetinin kendi ülkesine de yansıması sonucu devlet destekli istihbarat operasyonuyla önemli kritik sağlık ve askerî kimlik verilerinin çalınması olayını tecrübe eden Singapur, covid-19 pandemi sürecinde yeni çıkan tehditlere de maruz kalmış ve daha dirençli bir siber güvenlik kapasitesi inşa etmek için yapay zekâ tabanlı yatırımlarını artırmıştır. Sonuç olarak, dijital dönüşüm ve siber güvenlik politikalarının oluşturulması bakımından, siber güvenlik çalışmaları içerisinde incelenmesi gereken bir ülke olarak uzun yıllar kalacağı görülmektedir.

KAYNAKÇA

Akıllı Şehirler, (t.y.), https://www.akillisehirler.gov.tr/akilli-sehir-nedir/, (06.08.2020).

Bilgi Güvende, (2018), " Singapur'un En Büyük Sağlık Grubu Siber Saldırıya Uğradı", https://bilgiguvende.com/singapurun-en-buyuk-saglik-grubu-siber-saldiriya-ugradi/, (10.08.2020).

Chong, C., (2019), "2 Vendors for MINDEF, SAF hit by Malware; Personal Data of 2400 Staff Could Have Been Leaked", https://www.straitstimes.com/singapore/healthcare-training-provider-hmi-institutes-server-infected-by-ransomware, (10.08.2020).

Chua, C., (2006), "The Singapore e-Government Experience", IDA Singapore, https://www.carecprogram.org/uploads/Day1-SIN-eGovernment-Experience.pdf, (07.08.2020).

Cimpanu, C., (2018), "Lawful Intercept Pegasus Spyware Found Deployed in 45 Countries", https://www.zdnet.com/article/lawful-intercept-pegasus-spyware-found-deployed-in-45-countries/, (10.08.2020)

CIO Middle East, (2019), " Singapore Ranked Second Most Prepared Country in the World to Adopt AVs", https://home.kpmg/sg/en/home/media/press-releases/2019/02/singapore-is-second-most-prepared-nation-in-the-world-to-adopt-autonomous-vehicles.html, (07.08.2020).

Cisco, (2019), "Digital Readiness Index 2019", https://www.cisco.com/c/m/en_us/about/corporate-social-responsibility/research-resources/digital-readiness-index.html#/Basic%20Needs, (06.08.2020).

CSA (Cyber Security Agency) Singapore, (t.y.), https://www.csa.gov.sg/, (08.08.2020).

CSA, (2016), "Singapore's Cybersecurity Strategy", file:///C:/Users/user/Downloads/SingaporeCybersecurityStrategy%20(1).pdf, (08.08.2020).

CyberGreen, (t.y), https://thegfce.org/initiatives/cybergreen/, (10.08.2020).

IMD Smart City Index, (2019), file:///C:/Users/user/Downloads/smart_city_index_digital.pdf, (08.08.2020).

Global Security Index, (2018), "ITU Publications", https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf, (10.08.2020).

MINDEF (Ministry of Defense) Singapore, (t.y), "3G SAF" https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/3g-saf, (07.08.2020).

Monetary Authority of Singapore, (t.y.)," Project Ubin : Central Bank Digital Money Using Distributed Ledger Technology", "https://www.mas.gov.sg/schemes-and-initiatives/project-ubin, (08.08.2020).

Moon, A., (2019), "State Sponsored Espionage Group Whitefly Behind Singapore Cyberattack : Report", https://www.reuters.com/article/us-singapore-cyberattack-symantec/state-sponsored-espionage-group-whitefly-behind-major-singapore-cyberattack-report-idUSKCN1QN1S4, (10.08.2020).

Pandey, P., Golden, D., Peasley, S. ve Kelkar, M., (2019), " Making Smart Cities Cyber Secure", **Deloitte Insights**, https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html, (08.08.2020).

Peh, Y. X., (2019), " Singapore Cyber Threat Landscape Report (H1 2019) ", https://www.digitalshadows.com/blog-and-research/singapore-cyber-threat-landscape-report-h1-2019/, (10.08.2020).

Prime Minister's Office Singapore, (2014), "Transcript of Prime Minister Lee Hsien Loong's Speech at Smart Nation Launch on 24 November", https://www.pmo.gov.sg/newsroom/transcript-prime-minister-lee-hsien-loongs-speech-smart-nation-launch-24-november, (08.08.2020).

Siber Bülten, (2020), " Zoom'da Sorunlar Bitmiyor, Singapur Uygulamayı Yasakladı", https://siberbulten.com/dijitalguvenlik/zoomda-sorunlar-bitmiyor-singapur-uygulamayi-yasakladi/, (09.08.2020).

Singapore International Cyber Week (SICW), (t.y), https://www.sicw.sg/, (08.08.2020).

Singapore Cyber Landscape -2019, (2020), "CSA Publishing", file:///C:/Users/user/Downloads/SingaporeCyberLandscape2019.pdf, (10.08.2020).

Singapore Minister of Home Affairs, (t.y), " Innovating to Keep Singapore Safe and Secure", https://www.mha.gov.sg/about-us/innovating-to-keep-singapore-safe-and-secure, (07.08.2020).

Singapore Status Online, (2018), " Cyber Security Act 2018 ",https://sso.agc.gov.sg/Acts-Supp/9-2018/, (07.08.2020).

Smart Nation and Digital Government Office in Singapore, (t.y), https://www.smartnation.gov.sg/, (06.08.2020).

Smart Nation Singapore Strategy Paper, (2018), https://www.smartnation.gov.sg/docs/default-source/default-document-library/smart-nation-strategy_nov2018.pdf?sfvrsn=3f5c2af8_2, (06.08.2020).

Staalduinen V. M. ve Joshi, Y., (2019), " The IoT Security Landscape, TNO", file:///C:/Users/user/Downloads/IoT%20Security%20Landscape%20Report%20(1).pdf, (09.08.2020).

The Government Technology Agency of Singapore (GovTech), (t.y), https://www.tech.gov.sg/, (08.08.2020).

Zhang, M. L., (2019) "The State of the Art Safti City Open From 2023 Features Transport Hub For Realistic Military Training ", **The Strait Times**, https://www.straitstimes.com/singapore/state-of-the-art-safti-city-to-open-from-2023-will-feature-transport-hub-and-targets-with, (07.08.2020).

Yılmaz; M., (t.y), " Dünyada ve Türkiye'de Siber Güvenlik Gerçekleri-1, İstatistikler, Analizler ve Öngörüler", **Cube Incubation**, https://www.cubeincubation.com/blog/dunyada-ve-turkiyede-siber-guvenlik-gercekleri-1-istatistikler-analizler-ongoruler, (10.08.2020).

Yu, E., (2020), "Singapore Warns Political Parties of Cyber Security Threats and Election Interference ", **ZD Net,** https://www.zdnet.com/article/singapore-issues-advisories-warning-political-parties-of-cybersecurity-threats-election-interference/, (10.08.2020).