



Dijital Egemenlik ve Dayanıklılık

Çalışma Grubu **Sonuç** Raporu
(Eylül 2024)

ÖNSÖZ

Dijital çağın hızla geliştiği günümüzde, dijital egemenlik, bağımsızlık ve dayanıklılık kavramları ulusal güvenliğin ve sürdürülebilir kalkınmanın ayrılmaz bir parçası hâline gelmiştir. Dünyanın dört bir yanında devletler ve kurumlar, dijital alandaki varlıklarını güçlendirmek ve korumak adına kapsamlı stratejiler geliştirmektedir. Özellikle son yıllarda yaşanan küresel olaylar, dijital egemenliğin ve dayanıklılığın önemini bir kez daha gözler önüne sermiştir.

Ülkemizde de bu alanda önemli çalışmalar yürütülmektedir. Ulusal veri merkezlerinin kurulması, yerli ve millî yazılımların geliştirilmesi, siber güvenlik altyapılarının güçlendirilmesi gibi eylemler, dijital bağımsızlığımızı sağlama yolunda atılan önemli adımlardır. Bu çabalar, dijital dünyada daha bağımsız, güvenli ve sürdürülebilir bir yapı oluşturmak için hayati öneme sahiptir.

Türkiye 3. Bilişim Şûrası çalışmalarında Derneğimize tevdi edilen görev kapsamında hazırlanan bu rapor, dijital egemenlik ve dayanıklılığın artırılması konusunda kapsamlı bir çalışma sunmaktadır. Bu çalışma kapsamında konu; teknolojik gelişmelerden yönetim önerilerine, veri egemenliğinden kriptolojiye, kritik dijital altyapı güvenliği yönetiminden toplumsal dijital dayanıklılığa kadar geniş bir yelpazede ele alınmıştır.

Raporun hazırlanmasında konu başlığı, olabildiğince derinliğine analiz ihtiyacını göz önünde bulundurmak suretiyle çalışılmıştır. Uzun zamandır bu alanda böylesine kapsamlı bir çalışma yapılmamış olması, raporun önemini bir kat daha artırmaktadır. Dijital dünyada bağımsız ve güçlü bir ülke olma yolunda atılacak adımların belirlenmesinde bu raporun rehberlik edeceğine inanıyoruz.

Çalışmanın hazırlanmasında desteklerini esirgemeyen Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı, sivil toplum kuruluşları ve katkıları için tüm katılımcılara şükranlarımızı arz ederiz. Bu kapsamda ayrıca, çalışmada emeği geçen ekip arkadaşlarımıza da teşekkür eder, hep birlikte, dijital dünyada daha güçlü ve bağımsız bir Türkiye olma yolunda nice önemli adımlar atılmasını dileriz.

Prof. Dr. Mustafa ALKAN

Bilgi Güvenliği Derneği Başkanı

İÇİNDEKİLER

ÖNSÖZ.....	1
İÇİNDEKİLER.....	2
TANIM VE KISALTMALAR.....	3
KATKIDA BULUNANLAR.....	11
YÖNETİCİ ÖZETİ.....	15
1. GİRİŞ.....	26
1.1. ÖNEMİ.....	26
1.2. AMAÇ VE KAPSAM.....	29
1.3. YÖNTEM VE RAPOR AKIŞI.....	30
1.4. STK’LARIN VE DİĞER PAYDAŞLARIN YAPTIĞI KATKILAR.....	31
2. DÜNYADAKİ GELİŞMELER, EĞİLİMLER VE BEKLENTİLER.....	35
2.1. GÜVENLİ DİJİTAL TEKNOLOJİLERİN GELİŞTİRİLMESİ VE SÜRDÜRÜLEBİLİRLİĞİ.....	37
2.2. KRİTİK DİJİTAL ALTYAPILARIN DAYANIKLILIĞI VE İŞ SÜREKLİLİĞİ.....	39
2.3. VERİ EGEMENLİĞİ POLİTİKALARI VE KRİPTOLOJİ.....	41
2.4. TOPLUMSAL DİJİTAL DAYANIKLILIĞIN SAĞLANMASI.....	42
2.5. SİBER OLAYLARIN VE SİBER OLAYLARA MÜDAHALENİN DÖNÜŞÜMÜ.....	46
2.6. ULUSAL SİBER GÜVENLİK YÖNETİŞİMİ.....	58
3. TÜRKİYE’DEKİ GELİŞMELER, EĞİLİMLER VE BEKLENTİLER.....	82
3.1. GÜVENLİ DİJİTAL TEKNOLOJİLERİN GELİŞTİRİLMESİ VE SÜRDÜRÜLEBİLİRLİĞİ.....	82
3.2. KRİTİK DİJİTAL ALTYAPILARIN DAYANIKLILIĞI VE İŞ SÜREKLİLİĞİ.....	86
3.3. VERİ EGEMENLİĞİ POLİTİKALARI VE KRİPTOLOJİ.....	95
3.4. TOPLUMSAL DİJİTAL DAYANIKLILIK.....	98
3.5. SİBER OLAYLARIN VE SİBER OLAYLARA MÜDAHALENİN DÖNÜŞÜMÜ.....	112
3.6. ULUSAL SİBER GÜVENLİK YÖNETİŞİMİ.....	120
4. TÜRKİYE’DE ATILMASI GEREKEN ORTA VE UZUN VADELİ ADIMLAR.....	142
4. 1. POST KUANTUM KRİPTOGRAFİ.....	149
4. 2. BİYO-İLHAMLI DİJİTAL BAĞIŞIKLIK.....	151
4. 3. YAPAY ZEKÂ (YZ) DESTEKLİ OTONOM SİBER MÜDAHALE.....	152
4. 4. SİBER SEFERBERLİK.....	153
4. 5. ULUSAL SİBER GÖREV GÜCÜ.....	154
4. 6. TEMEL BİLİŞİM SERVİSLERİNİN VATANDAŞA BEDELSİZ SUNULMASI.....	155
4. 7. MÜŞTEREK SİBER İSTİHBARAT VE TECRÜBE PAYLAŞIM PLATFORMU.....	157
4. 8. YERLİ SİBER GÜVENLİK ÜRÜNLERİNİN ÖNÜNDEKİ PSİKOLOJİK BARIYERİN KALDIRILMASI.....	158
4. 9. DEZENFORMASYONA KARŞI OTOMASYON.....	159

4. 10. ULUSAL SOSYAL MÜHENDİSLİK TATBİKATLARI.....	161
4. 11. ULUSAL SİBER GÜVENLİK MAKAMI.....	162
5. GENEL DEĞERLENDİRME.....	164
EKLER.....	168
KAYNAKÇA.....	169

TANIM VE KISALTMALAR

Tanımlar

TANIM	AÇIKLAMA
Bretton Woods	1944-1971 yılları arasında uygulanan finansal sistem
Allianz für Cyber-Sicherheit	Siber dayanıklılığı artırmak için bir araya gelmiş muhtelif Alman toplulukları
ARPANET	1968'de ABD'de kurulan ilk bilgisayar ağlarından biri
Bilgi Çağı	20. yy. ortalarından itibaren geleneksel sanayideki değişime işaret eden tanım
Boşluk Analizi (Gap Analysis)	Mevcut durum ile hedeflenen durum arasındaki farkları değerlendirme yöntemi
Computer Misuse Act	Siber Suçlar Kanunu
Computer Misuse Act	Veri Koruma Kanunu
Cyberagentur	Alman Siber Politikalar Kurumu
Endüstri 4.0	Üretimde otomasyon ve dijitalleşmeyi vurgulayan kavram
Esti	Estonya E-Devlet Platformu
Five-Eye	ABD, İngiltere, Avustralya, Yeni Zelanda ve Kanada arasındaki istihbarat paylaşım altyapısı
Gvahim	İsrail ilköğretim siber eğitim programı
Jus ad Bellum	Uluslararası Savaş Hukuku Kuralları
Kaitsepolitseiamet, KAPO	Estonya İstihbarat Servisi
Keidanren	Japon İş Dünyası Birliği
Knesset	İsrail Biyometrik Veri Tabanı Yasası
Lahav	İsrail Elit Polis Birimi
Ma'arach	İsrail Siber Güvenlik Direktörlüğü
Magna	İsrail Devlet Raporlama sistemi
Magshimim	İsrail ortaöğretim siber eğitim programı
McEliece Şifreleme	Kuantum dayanıklı bir tür kriptografi
Merkava	İsrail Devlet Kaynak Yönetim (ERP) Çözümü
NTRUEncrypt	Açık anahtarlı bir şifreleme algoritması
Rainbow	Bir tür kriptografik imza şeması
Réserve Citoyenne	Fransız ordusunun siber vatandaş rezervi
Cyberdélense	
Riigi Infosüsteemi Amet, RIA	Estonya Bilgi Sistemleri Otoritesi
Stuxnet	İran nükleer tesislerini hedef alan kötücül yazılım
Thalia	İsrail E-Devlet Platformu
The CyberCorps	ABD Devlet Siber Burs Programı
Toplum 5.0	İnsan merkezli 'süper akıllı toplum'
Tsifrovoy Suverenitet	Rusça. Dijital Egemenlik

Kısaltmalar

KISALTIMA	AÇIKLAMA
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri

KISALTMA	AÇIKLAMA
AfCS	Allianz für Cyber-Sicherheit (Siber Güvenlik Birliği)
AGİT	Avrupa Güvenlik ve İş Birliği Teşkilatı
AI	Artificial Intelligence (Yapay Zekâ)
ANSSI	Agence nationale de la sécurité des systèmes d'information (Ulusal Bilgi Sistemleri Güvenliği Kurumu)
ARPA	Advanced Research Projects Agency (İleri Araştırma Projeleri Kurumu)
AU	African Union (Afrika Birliği)
BCI	Brain Computer Interface (Beyin Bilgisayar Arayüzü)
BGD	Bilgi Güvenliği Derneği
BİT	Bilgi ve İletişim Teknolojileri
BKA	Bundeskriminalamt (Asayiş Büro Amirliği)
BM	Birleşmiş Milletler
BMI	Bundesministerium des Innern und für Heimat (İçişleri Bakanlığı)
BMVg	Bundesministerium der Verteidigung (Savunma Bakanlığı)
BOME	Bilgisayar Olayları Müdahale Ekibi
BSI	Bundesamt für Sicherheit in der Informationstechnik (Bilgi Güvenliği Dairesi)
BSIG	Bundesamt für Sicherheit in der Informationstechnik Gesetz (Bilgi Güvenliği Dairesi Kanunu)
BT	Bilgi Teknolojileri
BYOAI	Bring Your Own AI (Kendi Yapay Zekânı Getir)
BYOD	Bring Your Own Device (Kendi Cihazını Getir)
ÇG	Çalışma Grubu
CERT	Computer Emergency Response Team (Bilgisayar Olaylarına Müdahale Ekibi)
CIP	Critical Infrastructure Protection (Kritik Altyapı Koruma)
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act (Kritik Altyapı Yasası Kapsamında Siber Olay Raporlaması)
CISA	Cybersecurity and Infrastructure Security Agency (Siber Güvenlik ve Altyapı Güvenliği Ajansı)
CISP	Cyber Security Information Sharing Partnership (Siber Güvenlik Bilgi Paylaşımı Ortaklığı)
CRA	Cyber Resilience Act (Siber Dayanıklılık Kanunu)

KISALTMA	AÇIKLAMA
CRI	Counter Ransomware Initiative (Fidye Yazılımlarına Karşı Koyma Girişimi)
CSRB	Cyber Safety Review Board (Siber Güvenlik İnceleme Kurulu)
CTIIC	Cyber Threat Intelligence Integration Center (Cyber Threat Intelligence Integration Center)
CyOps	Cyber Operations (Siber Harekât)
DDO	Dijital Dönüşüm Ofisi
DDoS	Distributed Denial-of-Service (Dağıtık Servis Dışı Bırakma)
DHS	Department of Homeland Security (İç Güvenlik Bakanlığı)
DMA	Digital Markets Act (Dijital Piyasalar Yasası)
DoC	Department of Commerce (Ticaret Bakanlığı)
DoD	Department of Defence (Savunma Bakanlığı)
DoE	Department of Education (Eğitim Bakanlığı)
DoJ	Department of Justice (Adalet Bakanlığı)
DORA	The Digital Operational Resilience Act (Dijital İşletme Dayanıklılığı Kanunu)
DSA	Digital Services Act (Dijital Hizmetler Yasası)
EC	European Councel (Avrupa Konseyi)
ECC	Elliptic-Curve Cryptography (Eliptik Eğri Kriptografisi)
EDR	Endpoint Detection and Response (Uç Nokta Tespit ve Yanıtı)
EPCIP	European Programme for Critical Infrastructure Protection (Avrupa Kritik Altyapı Koruma Programı)
ERP	Enterprise Resource Planning (Enterprise Resource Planning)
FBI	Federal Bureu of Investigation (Federal Soruşturma Bürosu)
FIRST	Forum of Incident Response and Security Teams (Olay Müdahale ve Güvenlik Ekipleri Forumu)
FSB	Federal'naya sluzhba bezopasnosti (Federal Güvenlik Kurumu)
FSO	Federalnaya slujba ohranı (Federal Koruma Servisi)
GAMAM	Google, Apple, Amazon, Meta, Microsoft
GCHQ	Government Communications Headquarters

KISALTMA	AÇIKLAMA
	(Devlet Haberleşme Karargâhı)
GDPR	General Data Protection Regulation (Genel Veri Koruma Düzenlemesi)
GGE	Group of Government Experts (Hükûmet Uzmanları Grubu)
IASME	Information Assurance for Small and Medium Enterprises (Küçük ve Orta Ölçekli İşletmeler için Bilgi Güvencesi)
ICANN	The Internet Corporation for Assigned Names and Numbers (İnternet Tahsisli İsimler ve Sayılar Kurumu)
ICC	International Chamber of Commerce (International Chamber of Commerce)
ICT	Information and Communications Technology (Haberleşme ve Bilgi Teknolojisi)
IDF	Israel Defence Forces (İsrail Savunma Güçleri)
IETF	Internet Engineering Task Force (İnternet Mühendisliği Görev Gücü)
IGF	Internet Governance Forum (İnternet Yönetişim Forumu)
IMF	International Monetary Fund (Uluslararası Para Fonu)
INCB	Israel's National Cyber Bureau (İsrail Ulusal Siber Büro)
IoT	Internet of Things (Nesnelerin İnterneti)
ISACs	Information Sharing and Analysis Centers (Bilgi Paylaşım ve Analiz Merkezi)
ITU	International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
KP	Kalkınma Planı
KVKK	Kişisel Verilerin Korunması Kanunu
LKA	Landeskriminalamt (Eyalet Asayiş Şube Müdürlüğü)
LWE	Learning With Errors (Hatalardan Öğrenmek)
M	Moderatör
MFA	Multi-Factor Authentication (Çok Faktörlü Kimlik Doğrulama)
MISP	Malware Information Sharing Platform (Zararlı Yazılım Bilgi Paylaşım Platformu)
MUD	Manufacturer Usage Description (Üretici Kullanım Açıklaması)
NATO	The North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence (NATO Müşterek Siber Savunma Mükemmeliyet Merkezi)

KISALTMA	AÇIKLAMA
NATO CDMB	NATO Cyber Defence Management Board (NATO Siber Savunma Yönetim Kurulu)
NCIJTF	National Cyber Investigative Joint Task Force (Ulusal Siber Araştırma Ortak Görev Gücü)
NCSC	National Cyber Security Center (Ulusal Siber Güvenlik Merkezi)
NICE	National Initiative for Cybersecurity Education (Ulusal Siber Güvenlik Eğitimi Girişimi)
NIST	National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
NSA	National Security Agency (Ulusal Güvenlik Ajansı)
NSC	National Security Council (Millî Güvenlik Kurulu)
OECD	Organisation for Economic Co-operation and Development (Ekonomik İş Birliği ve Kalkınma Örgütü)
OIC	Organisation of Islamic Cooperation (İslam İşbirliği Teşkilatı)
ONCD	Office of the National Cyber Director (Ulusal Siber Direktör Ofisi)
OT	Operational Technology (Operasyonel Teknoloji)
PCCIP	The President's Commission on Critical Infrastructure Protection (Kritik Altyapı Koruma Başkanlık Komisyonu)
PDD	Presidential Decision Directives (Başkanlık Kararnamesi)
RAS	The Rapid Alert System (Hızlı Uyarı Sistemi)
RCC	Réserve Citoyenne Cyberdéfense (Vatandaş Siber Savunma Rezervi)
RSA	Rivest, Shamir, Adleman
SOC	Security Operations Center (Güvenlik Harekât Merkezi)
SRMA's	Sector Risk Management Agencies (Sektör Risk Yönetimi Ajansları)
SSB	Savunma Sanayii Başkanlığı
STK	Sivil Toplum Kuruluşu
TBD	Türkiye Bilişim Derneği
TBV	Türkiye Bilişim Vakfı
TESİD	Türk Elektronik Sanayicileri Derneği
TKG	Telekommunikationsgesetz (Telekomünikasyon Yasası)
TOBB	Türkiye Odalar ve Borsalar Birliği
TÜBİSAD	Türkiye Bilişim Sanayicileri Derneği

KISALTMA	AÇIKLAMA
UAB	Ulaştırma ve Altyapı Bakanlığı
UNDP	United Nations Development Programme (Birleşmiş Milletler Kalkınma Programı)
US-CERT	United States Computer Emergency Readiness Team (Birleşik Devletleri Bilgisayar Acil Durum Hazırlık Ekibi)
USOM	Ulusal Siber Olaylara Müdahale Merkezi
USSS	United States Secret Service (Birleşik Devletler Gizli Servisi)
VPN	Virtual Private Network (Sanal Özel Ağ)
WTO	World Trade Organization (Dünya Ticaret Örgütü)
XDR	Extended Detection and Response (Genişletilmiş Algılama ve Yanıt)
Y	Yazman

KATKIDA BULUNANLAR

BAŞKAN

Oğuz YILMAZ Bilgi Güvenliği Derneği – LABRİS NETWORKS

Raportörler

Oğuz BOZOKLU Bilgi Güvenliği Derneği – İternia Teknoloji

Aynur KOÇAK Bilgi Güvenliği Derneği - Gazi Üniversitesi

İçerik Komitesi

Prof. Dr. Ali AYDIN SELÇUK Bilgi Güvenliği Derneği - TOBB ETÜ

Salih TALAY Bilgi Güvenliği Derneği - HAVELSAN

Etkinlik Kurulu

Muhsin KILIÇ Bilgi Güvenliği Derneği - RTÜK

Zafer GÜNAL Bilgi Güvenliği Derneği - Türkiye Ulusal Ajansı

Ayşe MEDENİ Bilgi Güvenliği Derneği

ALT ÇALIŞMA GRUPLARI

Güvenli Dijital Teknolojilerin Geliştirilmesi ve Sürdürülebilirliği

Ali Aydın SELÇUK TOBB ETÜ (M)(Moderatör)

Bilgin METİN Boğaziçi Üniversitesi

Cumhur Doruk BOZAĞAÇ TÜBİTAK BİLGEM İLTAREN

Esra SÖĞÜT Gazi Üniversitesi (Y)(Yazman)

Murat HANÇEROĞLU Türk Telekom A.Ş.

Oğuzhan ALKAN Hazine ve Maliye Bakanlığı BTGM

Selahattin BAYGUT Sanayi ve Teknoloji Bakanlığı

Serkan ACAR Millî Savunma Bakanlığı

Süleyman ÖZARSLAN PICUS

Taha YÜCEL ASELSAN

Zeynep Deniz EYĞİ TÜBİTAK TEYDEB

Kritik Dijital Altyapıların Dayanıklılığı ve İş Sürekliliği

Atilla AŞÇIOĞLU EnerjiSA

Can DEMİREL	ICSFusion/Cyberwise Teknoloji A.Ş.
Ertan ALTUN	Vodafone
Fatih AYTEN	Nükleer Düzenleme Kurumu
Fırat UZUNHAN	Millî Savunma Bakanlığı
Halil Nadir TEBERCİ	Telkoder
İbrahim ÖZÇELİK	Sakarya Üniversitesi
Mehmet ÖZGEDİK	Ulaştırma ve Altyapı Bakanlığı
Mehmet Şevket ERGİN	Aselsan
Mehmet YILMAZER	EPDK
Mert Melih ÖZÇELİK	Millî Savunma Bakanlığı
Merve Başak UZUN	Gazi Üniversitesi (Y)
Muhammet Necmettin BOZKURT	EÜAŞ
Nuray DEDEOĞLU	EPDK
Ülkü KAHVE	Turkcell
Aynur KOÇAK	Gazi Üniversitesi (M)
<u><i>Veri Egemenliği Politikaları ve Kriptoloji</i></u>	
Ahmet Kemal AYGİN	Türk Telekom A.Ş.
Bülent TABAK	TBD
Durmuş Ali KESKİN	Millî Savunma Bakanlığı
Emre MERSİN	Ticaret Bakanlığı
Hasan KOSKA	Gazi Üniversitesi (Y)
Kazım DURAKLAR	Jandarma Genel Komutanlığı
Mahmut ALMAS	ASELSAN
Melike TERZİOĞLU	Cyberwise Teknoloji A.Ş.
Ömer CEYHAN	Adalet Bakanlığı
Remzi AKDAĞ	Millî Savunma Bakanlığı
Şeref SAĞIROĞLU	Gazi Üniversitesi / Gazi AI Center (M)
Sevil ŞEN	Hacettepe Üniversitesi
<u><i>Toplumsal Dijital Dayanıklılık</i></u>	
Abdullah Halis ŞAHİN	Kişisel Verileri Koruma Kurumu
Abdurrahman TABAR	Adalet Bakanlığı

Ahmet TUTAR	Erişim Sağlayıcıları Birliği (M)
Büşra KARAKAYA	EÜAŞ
Esra GÜNEŞ	Türkiye Ulusal Ajansı (Y)
Harun AKIN	Emniyet Genel Müdürlüğü
Muttalıp TULGAR	Turkcell
Şakir ŞİMŞEK	Siber Anadolu Toplulukları
Sinem TAN	Labris Networks

Siber Olayların ve Siber Olaylara Müdahalenin Dönüşümü

Cüneyt AKDENİZ	STM A.Ş.
Erdoğan YILMAZ	Barikat
Erhan YAZICI	Enerjisa
Hüseyin KURU	Jandarma Genel Komutanlığı
İren Berk ÖZALP	Türk Telekom A.Ş.
M. Tuncay GENÇOĞLU	Fırat Üniversitesi (M)
Mazlum BOZAN	BTK USOM
Murat DENER	Gazi Üniversitesi
Mustafa Çağrı FANUSCU	Adalet Bakanlığı BİGM
Nurcan MERT	TBD
Salih Efe KAHRAMANER	Dışişleri Bakanlığı
Sinem AYDOĞDU	Ulaştırma ve Altyapı Bakanlığı
Tuğçe PEHLİVANOĞLU	Enerjisa
Oğuz BOZOKLU	INTERNIA (Y)

Ulusal Siber Güvenlik Yönetişimi

Abdullah Sait ŞEKERCİOĞLU	Cumhurbaşkanlığı Savunma Sanayii Başkanlığı
Beytullah ŞİMŞEKOĞLU	TÜBİTAK SAGE
Duygu FİDANCIOĞLU	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
Emre ÖZKÖK	TÜBİTAK Bilgem Siber Güvenlik Enstitüsü
Hakan ÖZFİDAN	Siber Güvenlik Kümelenmesi / SSB
Haluk ÇATAL	TSK Siber Savunma Komutanlığı
Mahmut Esat YILDIRIM	BTK USOM
Metin DURMAZ	Millî Savunma Bakanlığı

Muhammed Raşit ÖZDAŞ Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı

Muhsin KILIÇ Radyo ve Televizyon Üst Kurulu (Y)

Ömer Faruk SORGUN Erişim Sağlayıcıları Birliği

Salih TALAY HAVELSAN (M)

Serhat YAPICI Ticaret Bakanlığı

Sinan AYDIN Enerjisa

Burak Furkan MERMER Ulaştırma ve Altyapı Bakanlığı

YÖNETİCİ ÖZETİ

İnternet ve Küreselleşme

Bir askerî araştırma projesi olarak ortaya çıkan, başlarda dar bir çerçevede denenen, bilahare akademide dosya paylaşımı için kullanılan ve sonraki dönemde bütün dünyaya mal olan İnternet, insanlığın yaşam biçimini temelden değiştirmiştir.

İşler, iş yapış şekilleri, iletişim ve ilişkiler başta olmak üzere tüm yaşam döngüsü, İnternet kaynaklı bir dönüşüme uğramıştır. İnternet sayesinde üretim ve lojistik maliyetleri düşmüş, daha ucuz hizmetler, daha hızlı ve kaliteli hâle gelmiştir. Nüfus artışına ayak uydurmakta zorlanan devlet ve şirketler için İnternet, bu süreçte âdeta bir can simidi olmuştur.

1980’ler ve sonrası canlanan kapitalizm, doğu blokunun çökmesiyle ivme kazanmış, İnternet yardımıyla küreselleşmiş ve birkaç on yıl içerisinde dünya, her türlü mal ve hizmetin çok daha hızlı dolaştığı, iletişimin artık günlerle değil saniyelerle ölçüldüğü, kitlesel haberleşmenin âdeta patladığı büyük bir ‘köy’ olarak anılır olmuştur.

Bu süreçte neo-liberal devlet yaklaşımının moda olması ve yaygınlaşması ile devlet-vatandaş ilişkileri değişime uğramış, kamu hizmetleri vatandaşa İnternet üzerinden verilir olmuş, devlet aygıtı dünya genelinde görece küçülmüş, etkinlik ve verimlilik artmıştır. Zaman zaman yaşanan savaşlar ve bölgesel çatışmalara rağmen küreselleşmenin büyümesi ve cazibesi devletleri ve devlet kavramını uzunca bir zaman esir almıştır.

Tereddüt ve Ulus Devletin Yükselişi

Küreselleşmenin, zaman içerisinde Çin gibi baş edilmesi zor bir ekonomik dev yaratması ve bu devin tedricen askerî ve finansal bir ‘tehdide’ dönüşmesi, küreselleşmenin fikir babası ve lokomotif ABD’nin alarma geçmesine ve bu kavramı sorgulamasına neden olmuştur.

ABD, yıpratıcı Vietnam Savaşı hezimetinin omuzlarına yüklediği ağır ekonomik yükün yorgunluğuyla 1971’de Bretton Woods uluslararası para idare sisteminden çekilmiştir. Sonraki dönemde, kendi parasını, herhangi bir karşılık göstermeden basabilmenin ve küresel para birimi olarak kullanılmanın konforunu yaşamıştır. Bilahare, Avrupa Birliğinin belirli bir olgunluğa gelmesiyle avronun da rekabete katılması ve Asya’daki ekonomik gelişmeler sonucunda bu baskın

durum sarsılmış, pervasızca basılan doların yarattığı enflasyon ve sanayi üretimini Çin'e kaptırmanın getirdiği ticaret açığı 2008 yılındaki büyük krize giden yolu açmıştır.

ABD'de başlayan ve hızla dünyaya yayılan bu finansal kriz, ülke ekonomilerini ve refahı da olumsuz etkilemiş, küreselleşme olgusuna dair soru işaretleri oluşmaya başlamıştır. Bu soru işaretleri, 2013'te sızdırılan ve CIA ajanı Edward Snowden tarafından ifşa edilen belgelerle İnternet'e olan güveni de derinden sarsmış, küreselleşme sevdası büyük bir tereddüde dönüşmüştür.

ABD İstihbarat Kurumu NSA'nın; PRISM, XKeyscore ve Tempora gibi İnternet izleme programları ile küresel İnternet erişimini izlediği, bilgileri yakın müttefikleriyle (Five-Eye) paylaştığı, bu yolla siyasi ve ticari birçok alanı manipüle ve istismar ederek çıkar sağladığı açıkça ortaya çıkınca bu defa gözler İnternet'e çevrilmiştir.

O güne dek, insan hayatını kolaylaştırdığı, yaşam koşullarını iyileştirdiği, daha adil ve demokratik bir dünya sunduğu varsayılan, koşulsuzca güvenilen ve biraz da hafife alınan bu sanal dünyanın, yaratıcısının elinde aslında bir silaha dönüştüğü, dünyanın geri kalanının güvenliğini ve mahremiyetini tehlikeye attığı fark edilmiştir.

2019 sonlarında başlayan ve 2020'de zirve yapan Kovid-19 salgını ise bu süreçte son önemli kilometre taşı olarak görülmelidir. Bu dönemde, uzunca sayılabilecek bir süre sınırlarını kapatan ülkeler ve evlerine kapanan insanlar, o güne kadar görmedikleri farklı bir tecrübe yaşamışlar, dünyanın başka bir yüzünü görmüşler, 'yeni normaller' tanımlama gereğini duymuşlardır.

Pandemi günleri, en temel gıda maddelerinde ihracat kısıtlamalarına gidildiğine ve acil sağlık malzeme ve ekipmanlarının dahi ülkeler tarafından birbirlerinin elinden çekip alındığına, âdeta çalındığına şahitlik etmiştir. Bu dönemdeki içe kapanma hâli, bir yandan İnternet'in hayatın idamesi için ne denli gerekli olduğunu ilk kez bu kadar açık bir biçimde insanlara gösterirken, diğer yandan, ABD'nin Çin'e karşı başlattığı ticaret kısıtlamaları ve Batı dünyasının Rusya ile yaşadığı siyasi ve askerî bir dizi gerilim ile birlikte küreselleşme hayallerine son büyük darbeyi vurmuştur.

Bölgesel ittifaklar, ikili veya çok taraflı menfaat birliktelikleri uluslararası ilişkilerin değişmez bir gereği ve gerçeği olmaya şüphesiz devam edecektir. Ancak geline nokta, ülkelerin

bilhassa kriz ve savaş durumlarında her anlamda kendi kendilerine yetebildiği güçlü bir ulus devlet modeli tekrar önem kazanmıştır. Bu kapsamda, Çin'in nispeten önde götürdüğü dijital egemenlik iddiası gün geçtikçe diğer ülkeler tarafından da belirli oranda kabul görmeye başlamıştır.¹ Dijital egemenlik, genellikle mahremiyet, ekonomik çıkar ve bireysel özgürlükleri önceleyen Avrupa Birliği ülkelerinde dahi karşılık bulan bir kavram olarak görülmeye başlamıştır².

Dijital Egemenlik ve Bağımsızlık

Modern çağda devlet kurumunun dijital izdüşümü olan elektronik devlet ve ülkede İnternet üzerinden bu yolla gerçekleşen her türlü iş ve işlem de devletlerin yukarıda tanımlı kendi kendine yetebilme hâli dâhilinde değerlendirilmektedir.

Fiziksel dünya ile dijital dünyanın iç içe geçtiği ve birindeki değişimin diğerini de yakından etkilediği ve ilgilendirdiği bu ortamda, aradaki sınırların yitirildiğini söylemek mümkündür. Gelenen noktada dijital bağımsızlık, tercih değil bir zorunluluk olarak görülmektedir. Tam bağımsızlık için, siyasi, idari ve ekonomik özgürlük kadar, dijital olarak da hür olmak gerektiği anlayışı her geçen gün daha fazla taraftar kazanmaktadır.

Büyük yol ve yön gösterici, askerî ve siyasi deha Gazi Mustafa Kemal Atatürk'ün 'Egemenlik kayıtsız şartsız milletindir' ve 'Bağımsızlık benim karakterimdir' sözlerini şiar edinmiş bir milletin mensubu olarak, bu gerekliliğin yerine getirilme koşullarını oluşturmak, bir tercih değil şüphesiz gönüllü bir mecburiyettir. Bu husus ülkemiz devlet erkânı tarafından da değişik vesilelerle muhtelif mecralarda vurgulanmaktadır³.

¹ Çin liderinden 'siber egemenliğe saygı' çağrısı 16 Aralık 2015, https://www.bbc.com/turkce/haberler/2015/12/151216_siber_egemenlik

² Macron'dan "Dijital Egemenlik" çağrısı, <https://www.ekonomim.com/kuresel-ekonomi/macron-dan-dijital-egemenlik-cagrisi-haberi-603013>

³ "Dijital egemenlik duvarları yükselmeye devam ediyor: Almanya'nın G10 yasa tasarısı", 16 May 2021, <https://www.freewebturkey.com/dijital-egemenlik-duvarlari-yukselmeye-devam-ediyor-almanyasin-g10-yasa-tasarisi>

⁴ T.C. Cumhurbaşkanı Recep Tayyip Erdoğan, 'Dijital Güvenliğiniz Yoksa Özgürlüğünüzü Sağlayamazsınız' https://www.ntv.com.tr/turkiye/dijital-guvenliginiz-yoksa-ozgurlugunuzu-saglayamazsiniz,0N_MIWFKw06hoRkFIh0-w

⁵ Fahrettin Altun, 'Dijital Evreni Siber Vatan olarak tanımlıyoruz', <https://www.trthaber.com/haber/gundem/fahrettin-altun-dijital-evreni-siber-vatan-olarak-tanimliyoruz-638909.html>

⁶ Ali Taha Koç, 'Nasıl ki sınırlarımızı, topraklarımızı koruyorsak Dijital egemenliğimizi de korumamız lazım', <https://www.aa.com.tr/tr/ekonomi/dijital-donusum-ofisi-baskani-koc-dijital-egemenlik-kurallarimize-uyan-her-turlu-firmaya-kapimiz-sonuna-kadar-acik/3003662#>

Dijital bağımsızlığın ön koşullarından biri dijital egemenlik, dijital egemenliğin gereği ise dijital dayanıklılık geliştirmedir. Ne var ki, dijital egemenliğin ilan edileceği bir Dijital Vatan'ın sınırlarını çizmek, o sınırlar dâhilindeki dijital varlıkları belirlemek, tanımlayabilmek ve kavramların içerisini hakkıyla doldurabilmek o derece kolay değildir.

Yazılı tarih kadar eski klasik devlet anlayışında egemenliğin en önde gelen koşulu, hâkim olduğu iddia ve ilan edilen fiziksel bir alanın varlığı ve o alanın geçtiği sınırlardır. Önceleri toprak ve kara sınırlarıyla tanımlanan egemenlik olgusuna, zaman içerisinde kıta sahanlığı, karasuları, münhasır ekonomik bölge, serbest kullanım alanı vb. yeni kavramlarla denizlere dair düzenlemeler ve bilahare hava sahası ve ilişkili külliyyat dâhil edilmiştir. Teknolojik gelişmeler ve araştırma imkânlarının artmasıyla, okyanus ve derin denizler, kutuplar ve uzayla ilişkili birçok konu da egemenlik başlığı kapsamında uluslararası hukukta yer bulmuştur⁴.

Ne var ki, egemenlik konusu, bilgi ve iletişim teknolojileri ve İnternet'in de dâhil olduğu dijital dünyaya geldiğinde, sınırların çizilmesi, egemen alanın belirlenmesi, varlıkların tanımlanması yönleriyle, içerisinde çok sayıda belirsizlik taşıyan bir problem yumağına dönüşmektedir. Konu, uluslararası egemenlik hukukunda yer bulmaması bir tarafa, siber yeteneklerin bir silah ve saldırı aracı olarak kullanılabilmesi nedeniyle de savaş, barış ve çatışma hukuku kapsamında ele alınması gereken çok boyutlu bir mesele olarak görülmektedir⁵.

Siber uzayda, aynı silahlar kullanılsa da siber suç ile siber saldırı kıyaslamasında en ayırt edici boyut, eylemin bir millî güvenlik kaygısıyla ve siyasi saikle gerçekleşip gerçekleşmediği meselesidir.³ Bir diğer önemli boyut, failin devlet olup olmadığıdır. Eğer eylemi gerçekleştiren, resmî bir devlet kurumu ve/veya doğrudan desteklediği bir aktörse, yaygın kanaat, bunun bir siber saldırı ve siber savaş ilanı olduğu yönündedir. Ne var ki devlet destekli bu tür saldırılarda gelişmiş gizleme yöntem ve teknolojileri kullanıldığından bugüne kadar bunun açıkça ispatı ve isnadı mümkün olmamıştır. Gürcistan ve Estonya'ya yönelik saldırılar ile İran'daki Stuxnet olayında dahi, saldırının aleniliğine rağmen gerçek kaynağa atıf ve devlet dahli delillendirilememiş, faaliyetler örtük bir şekilde yürütülmüştür.

⁴ Atilla Aydın, Dijital Çağda Egemenlik: Şapkayı Önümüze Koyma Vakti Geldi, 19 Mayıs 2018, <https://medium.com/@sibervatandas/dijital>

⁵ Şinasi Özgür Mumcu, Siber Saldırı ve Uluslararası Hukuk Hakkında Genel Bir Değerlendirme, 07 Mayıs 2019

Benzer teknik ve taktikler kullanılsa da siber saldırı kavramının, askerî terminoloji içerisinde kullanılıyor olması da konunun, siber suçlardan net bir şekilde ayrıldığına bir diğer göstergesidir. Hangi siber ürünün silah olarak kabul edileceği, silah kullanmanın hangi durumlarda hukuka uygun olduğu (*Jus ad Bellum*), içişlerine müdahale yasağını düzenleyen 36/103 sayılı BM Kararı, uluslararası haksız fiil, gereklilik, orantılılık, karşı tedbir, atıf kuralları, meşru müdafaa vb. çok sayıda kavram ve kararın siber uzaya uyarlanmasına ilişkin belirsizlikler bulunmaktadır³.

Ülkeler arası görüş farklılıkları ve uzlaşma noksanlığı nedeniyle bu belirsiz ve kararsız durumun uzunca bir süre daha devam etmesi beklenmektedir. Mevzunun hukuki boyutunun tartışılması kapsamında dikkat çekici son bir nokta olarak belki şu ifade edilebilir: İlan ve tanınmaya tabi olan egemenlik hakkı, bir yandan belirlediğiniz alanda size nüfuz yetkisi verirken, diğer yandan o alandan üçüncü taraflara yapılacak her türlü mütecaviz hareketin sorumluluğunu da size yüklemektedir.

Hukuki mülahazalar bir yana, dijital egemenlik sınırlarının belirlenmesi ve bu sınırlar dâhilinde özgürce hareket edilmesine dair teknik olarak da önemli zorluk ve açmazlar bulunmaktadır. İcat edildiği günden bu yana evrimleşerek büyük değişim ve dönüşüme uğramış olsa da İnternet, doğası gereği anonim ve dağıtık bir yapıda çalışmaktadır. Bu dağıtık yapı yeni gelişen blok zincir gibi teknolojilerle daha da ademi merkezi ve otonom olma eğilimindedir. Aynı teknolojiler ayrıca, suçu ve suçluyu gizleme ve finansman akışını kolaylaştırma yönleriyle de büyük imkânlar tanımaktadır.

Diğer yandan kriptografik uygulamalar, İnternet üzerinde iz takibini önemli ölçüde kısıtlamakta, izlenebilirliği ve şeffaflığı perdelemektedir. Yine aynı şifreleme imkânlarıyla iletişim kanalları üzerinde açılan uçtan uca sanal tüneller (VPN) vasıtasıyla yapılan ve suç unsuru içeren iletişimin engellenmesi veya zararlı içeriğin filtrelenmesi zorlaşmaktadır. Servis sağlayıcılar ve diğer yerel altyapı bileşenleriyle bu engeller belirli düzeyde aşılmaya çalışılsa da özellikle alçak yörünge haberleşme uydularıyla verilebilecek doğrudan İnternet erişimi ile bu olasılık da ortadan kalkabilecektir.

Egemenlik şartlarının belki de en öncelikli olanı, verinin yerelleşmesi ve ülkede üretilen verinin ülke menfaatleri doğrultusunda, katma değer ve refah üretecek şekilde kullanılmasıdır. Bu noktadaki sorumluluklarının yerine getirilmesi kapsamında atılacak öncü adımlar, veri merkezleri

ile yerel bulut bilişim hizmetlerinin oluşturulması ve büyük verinin işlenerek değere dönüştürülmesidir.

Nitelikli verinin işlenmesi, algoritmalar, analiz araçları, matematiksel ve istatistiksel metotlar yoluyla olmakla birlikte son zamanlarda makine öğrenmesi, derin öğrenme ve üretken yapay zekâ yöntemleriyle de daha büyük veriler işlenebilmektedir. Bunlar için artık daha yüksek işlemci gücüne ve dolayısıyla daha hızlı yarı iletken teknolojiler ile yongalara (çip) ihtiyaç duyulmaktadır. Dünyada çip endüstrisi büyük oranda tekel durumunda olup çip krizi yaşanmaktadır. Bu tekel durumunun kırılması ve ilgili ileri kritik teknolojinin ülkeye tedricen kazandırılması hususu hayati önemi haizdir.

Bilişim alanında temel servislerdeki ürün ve hizmet sağlayıcılar (donanım, işletim sistemi, uygulama yazılımı, depolama ve bulut çözümleri, e-posta, anlık mesajlaşma) ile sosyal medya uygulamaları da (ses, video, haber, iletişim vb.), istisnalar bir yana, ABD menşeli ‘Büyük Beşli’ (Google, Apple, Amazon, Meta, Microsoft) tarafından sağlanmaktadır. Bu alanda da bir tekelleşmeye gidildiğini söylemek yanlış olmayacaktır. İstisna olarak Çin ve belirli oranda Rusya’daki uygulamalar aksi yöndeki alternatif girişimlere örnek gösterilebilir.

Üzerinde egemenlik hakkı iddia edilen dijital dünyaya veya diğer adıyla siber uzaya daha yakından bakıldığında ise aslında üç katmandan oluştuğu görülmektedir.

En alt katman fiziki varlıklar olarak da tanımlayabileceğimiz, bilgisayarlar, sunucular, haberleşme ağ altyapıları, cep telefonları, baz istasyonları, kuleler, yönlendiriciler, anahtarlama cihazları vb. unsurlardır.

Bu katmanın bir üstünde veriyi işlemeye, depolamaya ve iletmeye yarayan araçlar ile verinin kendisinin de bulunduğu mantıksal katman yer alır. Mantıksal katman; e-devlet uygulamaları da dâhil olmak üzere türlü çeşit yazılımlar, DNS, IDN, alışveriş platformları, en basitinden en karmaşığına muhtelif yönetim bilişim sistemlerini barındırır.

En üstte ise bilişsel katman olarak da ifade edilen, algı katmanı bulunmaktadır. Önceki iki katmandaki kabiliyetler kullanılarak üretilen, iletilen, depolanan ve işlenerek bilgiye dönüşen veri, türlü iletişim uygulamalarıyla, videolar, görüntüler, sesler ve metinler hâlinde bilişsel katmanda

dolaşarak zihinlerdeki yankısıyla algıya dönüşür. Devletlerin stratejik iletişim faaliyetleri ve bilgi harekâtları (CyOps) hep bu katmandadır.

Dijital egemenlik iddiasında bulunabilmek için siber vatanın bu üç katmandaki yansımalarını da iyi tahlil ve nüfuz etmek gerekmektedir.

Dijital Dayanıklılık

Dijital dayanıklılık, en yalın hâliyle; çevrimiçi ortamda ne zaman riskin arttığını anlama, işler ters gittiğinde ne yapılması gerektiğini bilme, karşılaşılan zorluklardan en az hasarla sıyrılma ve olaydan ders çıkarma becerisidir.

Bu anlamda dijital dayanıklılık, sağlamlık kadar, çeviklik ve esneklik de gerektirmektedir. Kurumsal düzeyde, sadece siber güvenlik ürünlerine güvenmek ve bağımlı kalmaktan ziyade, etkili bir yönetim mekanizması oluşturmayı, güncel durumun dinamik şekilde takibini, proaktif davranış, hızlı reaksiyon ve karar alabilmeyi içeren, teknoloji kadar yol ve yöntemleri de kapsayan beceriler seti olarak tanımlanabilir.

Ulusal düzeyde de benzer boyutlar içeren dijital dayanıklılık; net tanımlanmış stratejik hedefler, güçlü bir bilgi teknolojileri altyapısı, teknolojik gelişim ve sıkı gözetim/denetimle zenginleşir, toplumsal farkındalık ve nitelikli insan gücü ile de desteklenir.

Dijital dayanıklılık konusunda küresel farkındalık gün geçtikçe artmaktadır. Son döneme dair yaşanan somut iki gelişmeye, Avrupa Birliği tarafından çıkarılan, Ocak 2023'te yürürlüğe giren ve finansal konulardaki bilişim düzenlemelerini içeren Dijital İşletme Dayanıklılık Yasası (The Digital Operational Resilience Act - DORA) ve yayım sürecinde olan Siber Dayanıklılık Yasası (Cyber Resilience Act - CRA) örnek olarak verilebilir.

Dijital dayanıklılık için gerekli ön şartlardan biri dijital bağımsızlık kazanılmasıdır. Günümüz siber güvenlik önlemleri, çoğunlukla ürüne dayalı ve statik bir görünüm arz etmekte, değişen ve gelişen saldırılarla baş etmekte zorlanmaktadır. Söz konusu sistemler herhangi bir vakayı atlamamak için çok fazla veri ve yanlış alarm üretebilmekte veya gerçek bir tehdit, bu yoğunluk içerisinde gözden kaçabilmektedir.

Doğadan ve insan vücudunun bağımsızlık sisteminden esinlenerek üretilen ve henüz emekleme aşamasında olan biyo-ilhamlı bilgi işlem kategorisinde tanımlanan dijital bağımsızlık

sistemi ise, evrimsel süreçlere dayalı genetik algoritmalar, yapay zekâ ve yapay sinir ağları, sensör ağları gibi bileşenleri içeren, yeni ve görünmeyen tehlikeleri sezmek için genellikle makine öğrenmesini kullanan adaptif bir yapıdır. Sistemik öğrenme, hafıza ve örüntü tanıma yeteneğine sahip bu yapı, olay dizilerini ilişkilendirerek sapkın⁶ modelin kötü niyetli olma olasılığını hesaplar. Tehlikelere yönelik olarak dağıtık veri tabanlarından toplanan verilere odaklı içgörülerden ve kitlelerin bilgeliğinden yararlanan dijital bağışıklık sistemleri *otonom hafifletme* ve *proaktif eylem* yoluyla sistem arızalarını azaltır⁷.

Her geçen gün daha da hızlanarak gelişen teknolojilerle değişen siber ortamda hayatta kalabilmek, etkin, caydırıcı ve saygın bir aktör olarak gelişmiş ülkeler arasında yer alabilmek için kazanılması gereken fazlaca kabiliyet ve üstesinden gelinmesi gereken sorun alanları bulunmaktadır. Gelişmiş dünyanın elinde tutmakta olduğu, yapay zekâ, kuantum, 5G başta olmak üzere ileri teknolojilerde aynı seviyeyi yakalamak, hatta üzerine çıkmak hedefiyle çalışmak gerekmektedir. Zira, kuantum hesaplama konusunda oluşabilecek teknolojik bir sıçrama ulusal güvenlikten ekonomiye, günlük yaşamdan uluslararası siyasete kadar her alanda ciddi sonuçlar doğuracaktır. Benzer şekilde yapay zekânın hayatımıza girmesiyle de insanlık öngörülemez bir döneme girmiş bulunmaktadır.

Uluslararası ortamın tanımlanmasında son dönemde sıklıkla; karmaşık, belirsiz, kaotik, çok kutuplu, gri vb. ifadeler kullanılmaktadır. Bu sıfatları, hibrit savaş, vesayet savaşları, siber savaş gibi hep savaştan bahseden bir dizi jargon takip etmektedir. Oysa bu, belki de uluslararası güvenlik ortamını açıklayamamanın başka ve dolaylı bir ifadesidir. Şüphesiz bu tespit ve tanımlamalarda haklılık payı vardır. Ancak geçmişten bugüne değişmeyen kadim mesele, güç ve nüfuz mücadelesidir⁸.

3'üncü Bilişim Şûrası ve Hazırlık Çalışmaları

⁶ *Sıfat*. Doğru yoldan ayrılmış olan. TDK Güncel Türkçe Sözlük.

⁷ STM ThinkTech, Bilim ve Teknoloji Blog, 07.06.2023, <https://thinktech.stm.com.tr/tr/dijital-bagisiklik-sistemleri#>

⁸ Cem Okyay, Bir Deniz Kuvveti Stratejisinin Temelleri, 03 Haziran 2023, <https://www.linkedin.com/pulse/bir-deniz-kuvveti-stratejisinin-temelleri-cem-okyay/?trackingId=up%2FXRw7fQqS47Hrg1g76xQ%3D%3D>

Türkiye 3. Bilişim Şûrası kapsamında ülkemizi bilişim alanında hak ettiği noktaya taşımak hedefiyle yürütülen faaliyetlerden “dijital egemenlik ve dayanıklılık” konusu Bilgi Güvenliği Derneği koordinesinde 2024 yılı Şubat ve Haziran aylarında iki çalıştayda tartışılmıştır.

Birinci Çalıştay’da Dijital Dayanıklılık ve Egemenlik konusunda mevcut durum, ihtiyaç duyulan çalışma alanları ile eğilim ve beklentilerin tespitinde bulunulmuş, İkinci Çalıştay’da ise ihtiyaçlar doğrultusunda öncelikli çalışma alanları belirlenerek somut çözüm önerileri geliştirilmesine gayret edilmiştir.

Mevcut duruma ilişkin olarak, ülkemizin siber güvenlik ve dolayısıyla dijital egemenlik ve dayanıklılık alanında ciddi çaba harcadığı ve çalışmalarda dünyadaki namzetleriyle nispeten eş zamanlı ilerlendiği ve bu kapsamda;

- Politika ve stratejilerin oluşturulduğu, hedeflerin belirlendiği, bir kısım mevzuatla da kapsanan bu hedeflere ulaşmak gayesiyle eyleme geçildiği,
- Eylemlerin hayata geçirilmesinde ve denetim boyutunda sınırlı kapasite geliştirildiği,
- Toplumsal farkındalığın belli bir düzeye taşındığı ve iş birliğini önceleyen bir ekosistemin öneminin bilindiği,
- Konunun, uluslararası iş birlikleri ile de belirli düzeyde desteklendiği tespitlerinde bulunulmuştur.

Ülkemiz, konu kapsamında görece olumlu bir noktada olmasına ve bu husus, uluslararası göstergelerle de destekleniyormuş izlenimine rağmen, öncü değerlendirmenin detaylarına inildiğinde, başta organizasyonel yapı ve teknoloji edinimi olmak üzere iyileştirme ve geliştirmeye açık yönlerin bulunduğu anlaşılmıştır.

Bu kapsamda öne çıkan tespit ve iyileştirme önerilerinden öne çıkan hususlar, önümüzdeki döneme rehberlik etmesi maksadıyla aşağıda sıralanmıştır.

- Başta yerli ve millî kavramları olmak üzere, tüm tanımlarda sadeleşme, netleşme, ortak anlayış ve eylem birliğine ihtiyaç bulunmaktadır.

- Yerli ve millî dijital güvenlik ürünlerinin sürdürülebilirliği ve istikrarı artırılmalı, kullanımlarına dair yasal tedbirler de dâhil olmak üzere konu yerli ürünler lehine nihayete kavuşturulmalıdır.
- Siber güvenlik konusunda yasal bir düzenleme ve bu hususta müstakilen sorumlu çatı bir teşkilat, etkin bir eşgüdüm makamına gerek duyulmaktadır.
- Alanda genel olarak nitelik eksikliği özellikle de seçkin insan kaynağı noksanlığının had safhada olduğu, yaşanan beyin göçü ile bu sorunun her geçen gün daha da derinleştiği görülmektedir.
- Topyekûn siber farkındalık için yaygın entelektüel gelişim ve toplumsal sosyo-kültürel dönüşüme ihtiyaç bulunmaktadır.
- Uygulamalara ilişkin sahada denetim ve takip, çerçevesi ve standartları oluşturulmuş tutarlı bir yapıda, güçlü bir merkezi otorite ve yetkin denetçiler tarafından yapılmalıdır.
- Gerginlik, kriz, savaş ve afet gibi olağanüstü hâllerde siber alandaki yönetim süreçlerinin netleştirilmesi gerekmektedir.
- Siber güvenliğin her alanına yönelik olarak detaylı bir envanter çalışması yapılmalı, bu çalışma canlı ve güncel tutulmalıdır.
- Siber güvenlik alanında kapasite geliştirmek için gerekli hususların, Siber Güvenlik Teknolojileri Yol Haritası ve TÜBİTAK Öncelikli Araştırma Alanlarında yer alması olumlu görülmekle birlikte, geliştirme aşamaları titizlikle takip edilmeli ve desteklenmelidir.
- Tek başına yüklenilmesi külfetli olan alanlarda, özellikle dost, kardeş, akraba ve oydaş⁹ ülke ve topluluklar yoluyla gerçekleştirilebilecek uluslararası ortaklıklar ve iş birlikleri imkânları geliştirilerek müşterek girişimlere ağırlık verilmelidir.

⁹ *İsim. Aynı düşüncede*, aynı inançta olan, aynı düşüncüyü savunanlardan her biri; düşünces, fikirdeş. TDK Güncel Türkçe Sözlük.

Müteakip safhada, yukarıda sıralı çıktılar, İkinci Çalıştay için bir girdi olarak kullanılmak suretiyle, yapılması gerekenler konusunda öncelikler ve somut hedefler tanımlanarak, önem ve öncelik atanması ve yöntem önerilerinde bulunulabilmesi maksadıyla katılımcıların dikkatine sunulmuştur.

Bu kapsamda yapılan değerlendirmeler sonucunda ise özet olarak;

- Dijital Egemenlik ve Dayanıklılığın kazanılması konusunun önemli olduğu ve gerekli yeteneklerin ağırlıklı olarak kısa ve orta vadede, en geç 2030 yılına kadar kazanılması gerektiği kanaati ön plana çıkmış,
- Ulusal siber güvenlik yönetiřimi, yeni nesil siber olayları ele alış biçimi ve kritik dijital altyapılara yönelik hususlara öncelikle eğilinmesi yönündeki görüşler ağırlık kazanmıştır.

Bu kapsamda, konuya ilişkin çözüm geliştirilmesi gerekli çok sayıda çalışma alanından görece önemli olarak aşağıda sıralı somut eylemlerin öncelikle ele alınmasında fayda görüldüğü sonucu ortaya çıkmış, bu alanlar şu şekilde sıralanmıştır.

- Beyin göçü, yetenek kaybı ve bilgi erozyonunun engellenmesi.
- Savaş ve seferberlik durumlarında, siber varlıkların korunmasına yönelik siber kriz yönetme becerisinin geliştirilmesi.
- Potansiyel siber saldırı ve afetlerin simülasyonu yoluyla müdahale planlarının ve prosedürlerinin etkinliğinin tatbikatlar yoluyla test edilmesi.
- Siber güvenlik alanında eğitim kalitesinin artırılması.
- Bilişim güvenliği ürünlerinde dışa bağımlılığın azaltılması.
- Ofansif güvenlik konseptine uygun olarak kazanılacak aktif ulusal siber savunma yetenekleri yoluyla caydırıcılık sağlanması.

Katkı ve katılımın iyi düzeyde görüldüğü ve yukarıda bir kısmından özet olarak bahsedilen süreç boyunca alınan bilgi, fikir ve görüşler, diğer çalışmalarla desteklenerek zenginleştirilmiş ve detayları çalışmamızın devam eden bölümlerinde sunulmuştur.

1. Giriş

1.1. Önemi

1.1.1. Büyük Dönüşüm

Daha önce benzeri görülmemiş çapta ve hızda bir dönüşümün tam ortasında yer alındığı konusunda yaygın bir kanaat ve mutabakat bulunmaktadır. Endüstri 4.0, Toplum 5.0, Bilgi Çağı vb. isimlerle anılan ve insanlık tarihi boyunca sadece birkaç kez şahit olunan bu büyük teknolojik dönüşüm, şüphesiz çok daha derin sosyal ve kültürel uzantıları bulunan köklü değişimleri içermekte ve aynı zamanda yeni değişimlerin de habercisi olarak görülmektedir.

Avcı-toplayıcılıktan tarım toplumuna, tarım toplumundan sanayi toplumuna geçen insanoğlunun yeni durağının bilgi toplumu olduğu anlaşılmaktadır. Bu dönüşümün öncekilerle kıyaslanamayacak ölçüde yüksek frekansa, büyük dalga boyuna ve devrimsel bir kapsama sahip olduğu görülmektedir. Makine insan yakınsamasının imkân tanıdığı teknolojiler sayesinde gerçeğinden zorlukla ayrılan bir dizi sanal deneyimin de bu süreçte yaşanacağı beklenmektedir.

Sadece bir ömür gibi kısa bir süreye sığabilen bu radikal dönüşüm, insan aklının ve kadim insanlık tecrübesinin alıştığı uyum sınırlarını zorlamaktadır. İnsanlar, mevcut bilgi, görgü ve tecrübeleriyle olayları ve kavramları anlamaktan daha çok seyretmekte, söz konusu konsept ve teknolojilerin sahibi olmayan taraflar süreci tercüme ederek yorumlamakta ama her halükârda anlaşılması zaman almaktadır. Benzetme yerindeyse adı geçen dönüşüm tüketilmekte ancak sindirilememekte, çoğu zaman sindirilemediği dahi fark edilememektedir.

Bu süreçte, hayatımıza giren bütün bu teknolojik yenilikler arasında şüphesiz en etkili olanı ve diğer bütün alanları kapsayanı İnternet'tir. İnternet, başlarda bir deneme alanı, askerî bir proje ve birkaç bilim insanının dar kapsamda ilgilendiği bir paylaşım platformuyken, modern hâline dönüştüğü ve sıradan insanların hayatına girdiği günden bugüne sadece 35 yıl geçmiş olmasına rağmen evrimleşerek geldiği nokta gerçekten etkileyicidir.

Oysa çok da uzak olmayan bir geçmişte İnternet, biraz da küçümseyici bir bakış açısıyla ele alınmış, âdeta çocuklar için bir oyun yeri, yalnızlar için bir arkadaş bulma platformu veya araştırmacılar için bir kütüphaneye erişimden öteye geçmeyeceği düşünülen “sanal” bir alan olarak görülmüştür.

Sanayi devriminden önce, yüzyıllardır işlettikleri at arabalarının yerini asla bu gürültülü ve kirletici hantal makinelerin alamayacağından emin olan arabacıların dönemin lokomotiflerine baktığı gibi, başlarda önemli bir çoğunluk da İnternet’i ve bağlantılı “sanal” teknolojik gelişmeleri hafife almış, günlük yaşantıya doğrudan etkilerine dair eksik ve yanlış öngörülerde bulunmuştur.

Ne zaman ki bankadaki parasını kaybetmiş, sosyal medya hesabı ele geçirilerek eski okul arkadaşları ve akrabaları dolandırılmış, sosyal medyadan edinilen bilgilerin doğruluğundan emin olunamamış, evden çalışarak para kazanılan işler ortaya çıkmış, salgınlarda hayat kurtarıcı, iş sürekliliği sağlayıcı vb. pek çok hususun merkezine oturmuş, işte o zaman insanlar, bu yeni mecranın sanal değil son derece gerçek olduğunun, içlerinde pek çok riski de barındırdığının ve kullanmaları ve kullanırken korunmaları gerektiğinin idrakine varmışlardır.

1.1.2. Dijital Egemenlik ve Dayanıklılık

İnsanlar, bu uyanış ve aydınlanma sonrası korunma ve kollanma ihtiyacını, pek doğaldır ki vatandaşları oldukları devletten beklemektedir. Doğası gereği, vatandaşların korunduğu, kollandığı ve adilce yönetildiği bir düzen için var olan devlet kurumu, sorumluluğunu yerine getirmek için egemenlik olgusundan türettiği yetkiyi kullanmaktadır.

Klasik devlet tanımının olmazsa olmaz üçlüsü olarak; toplum, toprak ve egemenlik kavramlarından ön plana çıkan egemenlik, ilk çağlardan bu yana toprak kavramıyla doğrudan ilişkilendirilen ve fiziki sınırları olan bir etki alanını içerdiğinden, tanımlanması nispeten kolay olmuştur.

Ne var ki dijital egemenlik konusunda durum bu kadar net değildir ve oldukça çok gri alan mevcuttur. Dijital sınırların nerede başlayıp nerede bittiği belli olmadığı gibi böylesi bir sınırın varlığı dahi tartışmalıdır. Bu tartışmalara bir de İnternet’in anonim ve dağıtık doğası ile türlü çeşit kriptografik kabiliyet eklendiğinde, bilinen anlamda sınırlardan ve sarıh bir egemenlik anlayışından bahsetmek kolay değildir. Bu kapsamda, dijital vatan ve dijital egemenlik tanımlarının belirginleşmesine de ihtiyaç vardır.

Mevcut duruma bakıldığında, dünyada dijital egemenlik konusunda farklı yaklaşımlar olsa da tartışmanın iki ana anlayış ekseninde yürütüldüğü ifade edilebilir. Bu eksenlerden birincisi ABD

ve yakın müttefiklerinin savunageldiği “özgürlükçü anlayış”, diğeri ise Çin ve Rusya’nın öncülük ettiği “dijital egemenliğin” mümkün olduğu ve olması gerektiridir.

ARPANET projesi ile bugünkü İnternet’in Ar-Ge’sini yapan ABD, dev bilgi teknolojisi firmalarıyla da (Apple, Meta, Amazon, Microsoft, Alphabet [Google]) İnternet’e hâlihazırda hükmedegeldiğinden, bu durumun keyfini sürme ve mevcut düzeni devam ettirme niyetindedir. Liderliğini Almanya ve Fransa’nın çektiği Avrupa Birliği ise zaman zaman bazı hukuksal girişimlerle adı geçen firmaları rahatsız edici eylemlerde bulunsa da mevcut durumla “temkinli uyumluluk” içerisinde.

Diğer yandan, bilgi teknolojileri alanına sonradan girmesine rağmen önemli mesafe kat eden Çin’in savunageldiği ve ‘Dijital Çin Seddi’¹⁰ başta olmak üzere muhtelif uygulamalar ve dev şirketleriyle büyük oranda ülkesinde hayata geçirdiği ‘dijital egemenliğin mümkün olduğu ve olması gerektiği’ görüşü, BM Uzmanlar Grubu başta olmak üzere farklı uluslararası platformlarda tartışılmaktadır. Bu görüşün önde gelen savunucularından bir diğeri Rusya Federasyonu’dur. Her iki ülke de muadil bilgi ve iletişim teknoloji uygulamaları ile ABD ve Batı hegemonyasını hafifletmek ve mümkünse ortadan kaldırmak niyetindedir.

Ülkemizin bu noktada duruşu ise Millî Teknoloji Hamlesi ve Siber Vatan şiarıyla Dijital Egemenliğini tesis etmek yönündedir. Ülkede üretilen verinin ülkede kalması ve kişisel verinin kullanıcı rızası dışında kullanılmaması esastır. Son dönemde yapılan düzenlemelerle, öncü teknoloji şirketlerinin, asgari olarak AB üyesi ülkelere sundukları sorumlulukları ülkemiz egemenlik haklarını gözeterek şekilde yerine getirmeleri sağlanmıştır.

Dijital Egemenliğin tesis edilmesinin ön şartlarından biri şüphesiz dijital dayanıklılıktır. Dijital dayanıklılık kabaca, dijital varlıklarınızın, gizliliğine, bütünlüğüne ve erişilebilirliğine zarar verebilecek her türlü eylemi engellemek veya defetmek, bunun yanında vatandaşı, bilgi kaynaklı istismardan korumak olarak tanımlanabilir. Bu noktada yeterli yerli ve millî güvenlik envanter ve altyapısının oluşturulması ve bu ürünler vasıtasıyla dijital bağımsızlık kazanılması hedefi öne çıkmaktadır.

¹⁰ Tarihi Çin Seddi’ne atıf yapılarak türetilen ve Çin Halk Cumhuriyeti’nin kapalı ve kontrollü İnternet’ine işaret eden benzetme.
<https://www.forbes.com/sites/timbajarin/2022/05/30/the-great-technology-wall-of-china/>

Bilgi ve iletişim teknolojileri alanında, tükettiğinden çok üreten ve ürettiği bilgiyi katma değere çeviren bir ülke olma hedefi makul ve gerçekçidir. Ülkemiz, dijital dönüşüm sürecinde, gerek devlet-vatandaş ilişkilerinde, gerekse devlet tüzel kişi münasebetlerinde bir hayli mesafe almıştır. Benzer nüfusa sahip ülkelerle kıyaslandığında, ortaya koyduğu e-devlet uygulamaları ile hatırı sayılır nicelik ve nitelikte hizmet sunulmaktadır.

Yoğun olarak kullanılan bu bilişim hizmetlerinin ve başta; enerji, sağlık ve finans olmak üzere hemen her sektörde kullanılan diğer uygulamaların yarattığı veri devasa boyuttadır. İsmiyle müsemma bu çağın, yakıtı da ham maddesi de bilgidir. Sanayi devriminden farklı olarak bu noktada bilgi devrimi, büyük ham madde kaynaklarını önceliklendirmemekte, bilinen anlamda sömürge ve kölelere ihtiyaç duymamaktadır.

Özellikle yapay zekâda yaşanan güncel gelişmeler, büyük verinin etkin bir şekilde değerlendirilmesine ve katma değer yaratan ürünler olarak hayata geçirilmesine her zamankinden daha çok imkân tanıyarak büyük bir teknolojik sıçrama yapılabilmenin kapısını aralamıştır.

1.2. Amaç ve Kapsam

Gelinen noktada; doğru hedefler belirleyen, bu hedeflere giden yol ve yöntemleri tanımlayan, düzgün planlar yapan ve planlarına sadık kalan ülke ve şirketlerin hayatta kalacağı, diğerlerinin siber dünyada yok olacağı açık olarak görülmektedir. BM’de resmen tanınıyor olmak ve vatandaşlarının, güvenli sınırlar dâhilinde görece huzur içerisinde yaşıyor olması bir devleti dijital ortamda var etmemektedir. Hâlihazırda gerçek hayatta var olan birçok devletin dijital dünyada esamisinin okunmadığı gerçeğinin altı, yakın gelecekte muhtemelen daha kalın çizgilerle çizilecektir. Bu anlamda teknolojik sıçrama için fırsat penceresi kapanmış değildir. Böylesi bir teknolojik sıçramayı, ekonomik olarak büyük bir atılımın takip etmesi mümkün ve muhtemeldir.

Devletin, bir yandan, dijital dünyada var olmak suretiyle vatandaşının hak ve hukukunu koruması, diğer yandan ülkesinde ortaya çıkan her türlü değer için küresel etki ve dirence sahip ulusal oluşumlara destek vermesi gerekir.

Devlete, bu alandaki ödevini yerine getirmesinde rehberlik etmek, konuya ilişkin üst düzey bir yol haritası sunmak ve vizyoner bir bakış geliştirmek maksadıyla geçmişten günümüze değişik

disiplinlerde çok sayıda faaliyet icra edilmiştir. Bilgi ve iletişim teknolojilerine ilişkin olarak bunlardan en bilineni ve hâlihazırda da 3'üncüsünün çalışmaları devam eden Bilişim Şûrası'dır.

Başlanan her işin bitirilemediği bilinen bir gerçektir. Ancak biten her işe mutlaka başlanmıştır. Bu kapsamda, doğru zamanda doğru işe karar vermek ve kaynak tahsis etmek son derece önemlidir. Doğru karara ise, önce doğru soruları sormak, sonrasında da o sorulara bulunan cevapların gösterdiği istikamette doğru işler yaparak ulaşılmaktadır.

Bu anlamda, konuya ilişkin olarak aklımızdaki sorulara yenilerini eklemek, başkaca doğru sorulara ve onların cevaplarına ulaşmak için, Şûra'ya hazırlık maksadıyla bir dizi çalıştay icra edilmiştir. Söz konusu çalıştaylar; tanışmak, karşılıklı danışmak, fikirleri çarpıştırmak suretiyle ilham alışverişinde bulunmak ve en faydalısına ulaşmak anlamında önemli fırsatlar sunmuştur.

İçinde bulunduğumuz yeni binyıl başlangıcında, 2002 ve 2004 yıllarında, “Bilgi Toplumuna Doğru” vizyonu, sırasıyla 1 ve 2'ncisi gerçekleştirilen Türkiye Bilişim Şûrası faaliyetlerinden 3'üncüsü 2024 yılında icra edilmektedir.

1.3. Yöntem ve Rapor Akışı

3'üncü Bilişim Şûrasına yönelik olarak yapılan çalışmalar kapsamında; süreç içerisinde konuya dair dile getirilen tüm görüşler, ilgililer tarafından paylaşılan bilgi, belge ve dokümanlar ile literatür taraması sonucunda konuya ilişkin elde edilen veriler titizlikle kayıt altına alınmış, tasnif edilmiş, değerlendirilmiş ve raporumuza ithal edilmiştir.

Bu çalışmada, ekseriyetle ittifak edilen görüşlerin öne çıkarılması, birbiriyle çelişen değerlendirmelerin ise bilim ve akıl çerçevesinde süzgeçten geçirilmesine gayret edilmiştir. Her türlü rafine çabasına rağmen, son tahlilde, konuya ilişkin sayıca çok ve nitelikçe ağır birtakım tespit, beklenti ve ihtiyaçların bulunduğu ortaya çıkmış, analiz sürecinin pek doğal bir neticesi olarak, ‘sorunlar, fırsatlar ve yapılması gerekenler’ gibi kavramlar arasındaki bulanıklık zaman zaman artmıştır.

Bu tespit, beklenti ve ihtiyaçların önem sırasına dizilmesi, önceliklendirilmesi ve teveccüh görmeyenlerin gündemden çıkarılması maksadıyla yapılan hazırlık; Ek-1’de örneği bulunan anket

formatında ilgililerin değerlendirmelerine sunulmuş, varsa ankette listelenmeyen hususların kendileri tarafından ilave edilebilmesine imkân tanınmıştır.

Raporda zikredilen ve anketimizde de listelenen bazı hususların, sadece yapılan çalıştaylardaki çıktılarla sınırlı olmadığını da bu noktada hatırlatmakta fayda görülmektedir. Geçmişten günümüze konuya dair, kamu kurumları, STK'lar, özel sektör ve bağımsız akademisyenlerce yapılan çalışmalar ile elde edilen sonuçlar, buna ek olarak konu odağında başkaca toplantı, görüşme vb. ortamlardan edinilen birikim de çalışmalarımıza yansıtılmıştır.

Dijital Egemenlik ve Dayanıklılık konusu, çalıştaylar kapsamında altı ana başlıkta irdelenmiş, katılımcıların katkı ve görüşleri Ek-2 ve Ek-3'teki formlar vasıtasıyla kendilerinden yazılı olarak da teslim alınmıştır. Tüm paydaşların çalışmanın tamamına hâkim olabilmesi ve resmin bütününe görebilmesi maksadıyla hazırlanmış olan ara rapor ve bu raporun özeti tüm ilgililerle paylaşılmıştır.

Şu ana kadarki çalışmalarımızın damıtılmış bir sürümü olarak görülebilecek elinizde bulunan bu nihai raporun akışında ise sırasıyla; sorumluluk alanımızda dünyada ve ülkemizdeki gelişmelere dair bilgi verilmekte, çalışma grubu konusunda atılması gereken orta ve uzun vadeli adımlar hakkında tespit ve önerilerde bulunulmakta, son olarak da elde edilen bilgiler ışığında genel bir değerlendirme ile raporumuz sonlandırılmaktadır.

1.4. STK'ların ve Diğer Paydaşların Yaptığı Katkılar

Yoğun bir emek, istişare ve ortak akıl ile üretilen önceki Şûra çıktıları, ülkemizin bilişim alanında gelişiminde yol gösterici ve belirleyici olmuş, bu süreçte temel altyapı büyük ölçüde tamamlanmış ve önemli başarılarla imza atılmıştır.

Gelinen noktada, içinde bulunduğumuz hızlı ve dramatik dijital dönüşüm sürecinin ülkemize sunduğu fırsatlar ve yarattığı olası tehditlere karşı hazırlıklı olmanın, tercihten ziyade bir zorunluluk olduğu açıkça görülmektedir. Hemen her gün yeni ihtiyaçlar tanımlanmakta veya doğmakta, tehditler artmakta ve bu ihtiyaçlara yönelik yeni teknolojiler ve ürünler ortaya çıkmakta, bilişim ekonomisi ve riskler artan bir tempoyla büyümektedir.

Bahse konu dijital dönüşüme yol açan teknolojik eğilimler doğrultusunda, 2030 ve ötesi Türkiye için üst seviye dijital dönüşüm yol haritamızın ortaya konulması amacıyla yaygın bir katılım ve katkıyla tüm paydaşların bu heyecana ortak olması arzu edilmiştir.

Anılan Şûra'nın hazırlıkları; Türkiye Bilişim Derneği eşgüdümünde, aşağıda yer alan çalışma grubu (ÇG) başlıklarında ve ilgili STK'nın sorumluluğunda aşağıda verilen çalışma grupları ve konu başlıklarında yürütülmüştür.

- ÇG1: Dijital Beceriler ve Çevik İşgücü Uyumu (*TOBB Yazılım Meclisi*)
- ÇG2: Küresel Veri Ekonomisinde Daha Güçlü Yer Alma (*Türkiye Bilişim Sanayicileri Derneği*)
- ÇG3: Sürdürülebilir Kalkınma için Yeni Nesil Dijital Teknolojiler (*Türkiye Bilişim Derneği*)
- **ÇG4: Dijital Egemenlik ve Dayanıklılık (*Bilgi Güvenliği Derneği*)**
- ÇG5: Bilişim Hukuku ve Etik (*Türkiye Bilişim Vakfı*)
- ÇG6: Dijital Yaşam (*Yazılım Sanayicileri Derneği*)

Bilgi Güvenliği Derneği eşgüdümünde faaliyetlerini yürüten **Dijital Egemenlik ve Dayanıklılık** Çalışma Grubunda, ülkemizin dijital egemenliğinin ve dayanıklılığının sağlanmasına yönelik ilgili teknolojilerin etkisi değerlendirilmiş, ihtiyaçlar belirlenmiş ve öneriler sunulmuştur. Bu çalışmalar sırasında dijital dayanıklılık hedefine temel oluşturabilecek konular, kamu düzeni, veri, altyapılar, vatandaş, siber güvenlik ve teknoloji gibi yönlerden incelenmiştir.

Bilişim ile ilgili böylesi bir Şûrada konunun güvenlikle ilişkili kısımları, siber güvenlik gibi taktik-operasyonel (kısa-orta vade) bir çerçeveden daha çok stratejik bir bakışla dijital egemenlik ve dayanıklılık başlığı altında ele alınmıştır.

Çalışmalar, aşağıda sunulan alt konu başlıkları çerçevesinde yürütülmüştür.

● Dijital vatan ve dijital egemenlik tanımı ve kapsamı nedir? Kamu düzeninin sağlanması açısından ilgili tartışmalar genel çerçevede nereye gitmektedir?

● Güvenli dijital teknolojilerin geliştirilmesi ve sürdürülebilirliği (*beceri, teknoloji, iş modeli, teknoloji, hizmet, malzeme ve materyal bağımlılığı vb. açılardan*).

● Kritik Dijital Altyapıların afetlerde ve salgınlarda dayanıklılığı ve iş sürekliliği.

● Veri egemenliği politikaları ve kriptoloji (*yerelleştirme, şifreleme, veri akışları, anonimleştirme ve mahremiyet*).

● Toplumsal dijital dayanıklılığının sağlanması (*farkındalık, siber sivil savunma, dezenformasyona karşı dayanıklılık*).

● Yeni nesil dijital teknolojiler ışığında organize siber olayların ve siber olaylara müdahalenin dönüşümü.

Yukarıda sıralı her bir alt konu başlığı, çalıştaylarda bir alt çalışma grubu / masa tarafından müstakil olarak ele alınmış, “Dijital Egemenlik, Dijital Dayanıklılık ve Dijital Vatan” gibi yeni kavramların tanımı ve içeriği ise tüm alt çalışma gruplarında tartışılmıştır.

Bununla beraber ulusal siber güvenlik yönetişimi ile ilgili bir çalışma ortamı oluşturularak yönetişimin getireceği başarı ayrı bir başlık altında çalışılmıştır.

1.4.1. İcra Edilen Çalıştaylar

Çalışmalar süresince, her iki çalıştay da kapsayacak şekilde aşağıda tanımlı mantıksal akış dâhilinde hareket edilmesi sağlanmıştır.

I. Durum: Anılan başlıklarda, sorun alanlarında ülkede mevcut durum nedir? Konuya ilişkin elde neler vardır? Envanter nedir? Ülkemizin konuya/alt konuya dair güçlü ve zayıf yanları ile fırsat ve tehditler (GZFT analizi) nelerdir?

II. Ulaşılabilecek Hedef: Kısa (5 yıl, 2024-2028, 12. KP), orta (10 yıl, (2029-2033) 13. KP) ve uzun (15 yıl, 2034-2038, 14.KP) vadeyi içerecek perspektifte değerlendirmeler yapılmıştır. Bu

zaman zarfında ve sonrasında, ülke olarak nerede olunacağını veya olunması gerektiğinin hayal edilmesi ve tespiti hedeflenmiştir. Bu bölüm, çalışmanın; kestirim, tahmin ve öngörü ağırlıklı, görece zorluklar ve meydan okumalar içeren bölümüdür.

III. Yapılacaklar: Hedeflenen noktaya ulaşmak için ihtiyaçlar ve yapılması gerekenler nelerdir? Boşluk Analizi sonucunda ülkemizin bu alanda, geliştirilmesi ve ön plana çıkarılması gereken yönleri hangileridir? Bu hususlarda ne yapmak, hangi teknolojilere yönelmek gerekmektedir? Aksiyon alanları neler olmalıdır?

Şûra hazırlık sürecindeki ilk Çalıştay olan 27 Şubat 2024 Çalıştayı ile I ve II'nci aşamalara ulaşmak hedeflenirken, 2. Çalıştay'da ise III, yani yol haritası araştırılmıştır.

1.4.2. İlke, Beklenti, Varsayım ve Kısıtlar

Yakın zamanda yayınlanan On İkinci Kalkınma Planı (12. KP) (2024-2028), önemli makroekonomik analizlere dayanmaktadır. Çalışmamızda aynı öneriler tekrarlanmayıp, söz konusu hedeflere ulaşılabilecek varsayımı üzerine gidilmiş ve planda zikredilen hedeflerin gerçekleşmesi için kritik olarak nelerin yapılması gerektiğine dair somut öneriler aranmıştır.

Çalışmamızda amaç, sadece “yeni bir rapor” üretmek değil, 2000’li yılların başında “e-Türkiye” ve “e-Dönüşüm Türkiye” makro politikalarında olduğu gibi bu süreçte de karar vericilerin gündemine çarpıcı ve ufuk açıcı bir ihtiyaç değerlendirmesi ortaya koymak ve ülkede, koordineli yeni bir bakış açısı ve gündem yaratmak olmuştur.

Çalıştayların, gündelik operasyonel sorunların dile getirildiği bir dertleşme ortamı, bilgi ve kemikleşmiş kanaatlerin yarıştırıldığı ve/veya dikte edildiği bir mecra olmamasına gayret edilmiştir. Çalıştaylardan edinilen sonuçların, bilinenin tekrarı olmaktan çok, yeni sözler söylemesi, taze bakış açıları ve öneriler sunması, vizyoner bir perspektifte pusula ve rehber niteliğinde olması hedeflenmiştir.

Şûra sonuç raporu ve çalışma grubu raporlarında tüm ihtiyaç alanlarına temas etmek ve çözüm önermek yönünde bir beklenti içerisine girilmemiştir. Bu kapsamda çalıştaylarda dijital teknolojilerin farklı sektörlere etkisine yönelik değerlendirmeler ortaya konulmuş ise de sektör özelinde detaya girilmemiştir.

Çalışmalar sürecinde, gelişmekte olan ulusal ve uluslararası ihtiyaçlar ile küresel teknolojik eğilimler doğrultusunda 2030 ve sonrası Türkiye için üst seviye bir yol haritamızın ortaya konulması beklenmiştir.

1.4.3. Katkı ve Katılım

Yukarıda sıralı ilke ve prensipler ışığında yürütülen çalışmalara; kamu, akademi, özel sektör ve sivil toplum kuruluşlarından yaklaşık 100 uzmanın gönüllülük esasına dayalı önemli ve nitelikli katkı ve katılımı sağlanmıştır.

2. Dünyadaki Gelişmeler, Eğilimler ve Beklentiler

Dijital egemenlik, devletlerin ve bireylerin dijital dünyadaki verilerini, sistemlerini ve altyapılarını kontrol etme yeteneğini ifade etmektedir. Günümüzde dijitalleşmenin hızla artması, dijital egemenlik konusunu daha da önemli hâle getirmiştir. Özellikle büyük teknoloji şirketlerinin ve yabancı devletlerin etkisi altındaki dijital alanlarda egemenlik sağlama çabaları, küresel politika ve güvenlik gündeminin merkezine oturmuştur.

Ülkeler bazında bu alanda ele alınan konular ve yapılan çalışmalar, aşağıda, Siber Güvenlik Yönetişimi alt başlığı altında detaylıca verilmiştir. Ancak konuya ilişkin küresel eğilimlere ve gelişmelere genel olarak bakıldığında durum şu şekilde görülmektedir.

Dünya genelinde, ülkeler kişisel ve ticari verilerin kendi sınırları içinde tutulmasını ve işlenmesini sağlamaya yönelik veri egemenliği ve yerelleştirme konusunda politikalar geliştirmektedir. Bu eğilim, veri güvenliği ve gizliliği konusundaki endişelerle birlikte, ekonomik bağımsızlık ve ulusal güvenlik nedenleriyle de desteklenmektedir. Özellikle Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği (GDPR) bu alandaki en belirgin örneklerden biridir.¹¹

Siber saldırıların artması, devletleri ve uluslararası kuruluşları bir diğer ana konu başlığı olarak siber güvenlik politikaları ve stratejileri geliştirmeye yönlendirmiştir. Uluslararası Telekomünikasyon Birliği (ITU) gibi kuruluşlar, siber güvenlik standartları ve iş birliği mekanizmaları oluşturarak, küresel düzeyde siber güvenliğin artırılmasını amaçlamaktadır.¹²

İnternet'in yönetişimi ve dijital teknolojilerin düzenlenmesi, küresel dijital egemenlik çabalarının bir diğer önemli parçası olarak görülebilir. İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN) gibi uluslararası kuruluşlar, İnternet'in teknik altyapısının ve kaynaklarının yönetişiminde merkezi bir rol oynamaktadır. Ayrıca, Birleşmiş Milletler (BM) bünyesindeki İnternet Yönetişimi Forumu (IGF), İnternet'in küresel yönetimi konusundaki tartışmalara ev sahipliği yapmaktadır. Bu noktada ülkeler İnternet'in yönetişimine daha fazla müdahil olabilmek ve etki alanlarını genişletebilmeye yönelik girişimlerini sürdürmektedir.

¹¹ General Data Protection Regulation, GDPR. <https://gdpr-info.eu/>

¹² International Telecommunication Union. (2021). Global Cybersecurity Index. <https://www.itu.int>

Bu noktada BM, dijital egemenlik konusundaki çalışmalarıyla öne çıkmaktadır. BM Genel Kurulu ve ilgili organları, dijital haklar, veri koruma ve siber güvenlik konularında çeşitli kararlar ve bildiriler yayınlamaktadır. BM, ayrıca dijital eşitsizliklerin giderilmesi ve dijital ekonominin sürdürülebilir kalkınmaya katkıda bulunması amacıyla çeşitli projeler yürütmektedir¹³.

Avrupa Birliği, dijital egemenlik ve dijital pazar konularında kapsamlı yasal düzenlemeler ve stratejiler geliştirmektedir. Dijital Pazar Yasası (DMA)¹⁴ ve Dijital Hizmetler Yasası (DSA)¹⁵ gibi düzenlemeler, AB'nin dijital pazarda bağımsızlığını ve rekabet gücünü artırma çabalarının bir parçasıdır. Ayrıca, AB, siber güvenlik stratejileri ve veri koruma yönetmelikleri ile de dijital egemenliğini pekiştirmektedir.

Ekonomik İş Birliği ve Kalkınma Örgütü (OECD), dijital ekonomi politikaları, veri yönetimi ve siber güvenlik konularında üye ülkeler arasında iş birliğini teşvik etmektedir. OECD, dijitalleşmenin getirdiği fırsat ve zorluklar konusunda araştırmalar yaparak, politika önerileri sunmaktadır.

Dünya Ekonomik Forumu (WEF), dijital egemenlik ve teknoloji yönetimi konularında küresel düzeyde farkındalık yaratmayı amaçlayan bir dizi çalıştay ve rapor düzenlemektedir. WEF, dijital dönüşümün ekonomik ve toplumsal etkilerini ele alan çeşitli inisiyatifler yürütmektedir.

Dijital egemenlik ve bağımsızlık konusunda öne çıkan temel yaklaşımlar olarak aşağıdaki hususlar göze çarpmaktadır.

Dijital egemenlik konusundaki küresel eğilimlerin önemli bir boyutu, dijitalleşmenin kapsayıcı ve sürdürülebilir olmasını sağlamaktır. Bu kapsamda, dijital teknolojilere erişimde adaletin sağlanması, dijital okuryazarlığın artırılması ve dijital uçurumun kapatılması hedeflenmektedir. Birleşmiş Milletler'in Sürdürülebilir Kalkınma Hedefleri arasında yer alan dijital kapsayıcılık, bu alandaki uluslararası iş birliğinin önemli bir parçasıdır.

Dijital egemenlik çabalarının başarılı olabilmesi için uluslararası iş birliği ve standartların belirlenmesi gerekmektedir. Uluslararası Telekomünikasyon Birliği (ITU), Dünya Ticaret Örgütü

¹³ United Nations. (2021). General Assembly Resolutions on Cybersecurity. <https://www.un.org>

¹⁴ European Commission. (2021). Digital Markets Act (DMA). <https://ec.europa.eu>

¹⁵ European Commission. (2021). Digital Services Act (DSA). <https://ec.europa.eu>

(WTO) ve diğer uluslararası kuruluşlar, dijital ekonomi ve siber güvenlik konularında küresel standartlar ve düzenlemeler geliştirmektedir. Bu iş birliği, dijital tehditlere karşı daha güçlü ve koordineli bir yanıt verilmesini sağlamaktadır.

Bu konudaki tartışmaların diğer bir boyutu da teknoloji ve insan hakları arasındaki ilişkiyi düzenlemek konusundadır. Dijital haklar, bireylerin dijital dünyada özgür ve güvenli bir şekilde var olabilmelerini garanti altına almayı amaçlamaktadır. Bu kapsamda, ifade özgürlüğü, veri gizliliği ve İnternet erişimi gibi konular ön plana çıkmaktadır. Uluslararası kuruluşlar, dijital hakların korunması ve güçlendirilmesi için çeşitli inisiyatifler yürütmektedir.

Sonuç itibarıyla, günümüzde dijital egemenlik, ulusal güvenlik, ekonomi ve toplumsal düzen açısından kritik bir öneme sahiptir. Küresel eğilimler ve uluslararası kuruluşların çalışmaları, dijital egemenlik konusundaki farkındalığı artırmakta ve ülkeler arası iş birliğini teşvik etmektedir. Dijital dünyanın geleceğini şekillendirecek olan bu çabalar, devletlerin ve bireylerin dijital alanlarda daha bağımsız ve güvenli bir şekilde var olmalarını sağlayacaktır. Dijital egemenlik konusundaki gelişmelerin yakından takip edilmesi, dijital çağda bağımsızlık ve güvenlik için hayati öneme sahiptir. Dijital egemenlik kapsamında, dünyadaki duruma dair alt çalışma alanlarına/konu başlıklarına özel detaylı bilgiler ise aşağıda sunulmuştur.

2.1. Güvenli Dijital Teknolojilerin Geliştirilmesi ve Sürdürülebilirliği

Uluslararası küresel düzen dinamiktir ve jeopolitik, teknolojik ve ekonomik gelişmeler ile sosyokültürel dinamiklerdeki değişikliklere yanıt olarak zaman içinde dönüşmektedir. Uluslararası hukuk kavramı devletlerin ve uluslararası kuruluşların davranışlarını düzenleyen kurallar ve ilkeler sistemidir. Uluslararası hukuk, diplomasi, ticaret, insan hakları, silahlı çatışma ve çevre gibi konuları düzenleyen anlaşmaları, sözleşmeleri, geleneksel uygulamaları ve yargı kararlarını kapsamaktadır.

Uluslararası kurumlar, devletler arasında iş birliğini, koordinasyonu ve karar almayı kolaylaştıran çok taraflı kuruluşlar ve forumlardır. Örnekler arasında Birleşmiş Milletler (BM), Dünya Bankası, Uluslararası Para Fonu (IMF), Dünya Ticaret Örgütü (WTO) ve Avrupa Birliği (AB), Afrika Birliği (AU) ve Güneydoğu Asya Ülkeleri Birliği (ASEAN) gibi bölgesel kuruluşlar yer almaktadır. İttifaklar ve antlaşmalar karşılıklı savunmayı, güvenliğini, ekonomik iş birliğini veya

siyasi uyumu teşvik etmeyi amaçlayan devletler arasındaki resmî anlaşmalar ve ortaklıklar sağlamaktadır.

NATO (Kuzey Atlantik Antlaşması Örgütü) gibi ittifaklar ve iklim değişikliğine ilişkin Paris Anlaşması gibi anlaşmalar uluslararası küresel düzenin temel unsurlarıdır. Uluslararası alanda devlet davranışını ve etkileşimlerini yönlendiren ortak değerler, normlar ve ilkelerdir. Bunlar egemenlik, insan hakları, demokrasi, müdahale etmeme, çok taraflılık ve çatışmaların barışçıl çözümü ilkelerini içerebilir.

Son zamanlarda küresel entegrasyonun yerini çok kutuplu ve az bağlantılı bir dünya almıştır. Jeopolitik konum ve gelişmeler bu durumun arkasındaki ana sebeplerdir. Ülkelerin jeopolitik konumlarını koruması ve güçlendirmesi için önlem alması gerekmektedir.

Tek süper güç olarak ortaya çıkan ve teknolojik üstünlüğü ile devamlılığını sürdüren ABD, dönem içerisinde Çin'in teknolojik gelişimini bir risk olarak görmeye başlamıştır. Çin bu bağlamda daha etkili bir oyuncu olarak konumlanmaya çalışmakta ve ABD ile arasındaki gerilimi artırmaktadır. Bu durum uluslararası ticareti olumsuz etkilemekte ve sonuçta askerî çatışmalara ve çok uluslu şirketlerin performansına ciddi ölçüde zarar vermektedir.

Uluslararası küresel düzen, iş birliği ve rekabetin, fikir birliği ve çatışmanın, istikrar ve değişimin karmaşık bir etkileşimi ile karakterize edilir. Devletlerin ve aktörlerin, küresel meseleleri yönetmek ve birbirine bağlı bir dünyada barışı, güvenliği, refahı ve sürdürülebilirliği teşvik etmek için normlar, kurumlar ve mekanizmalar oluşturmaya yönelik kolektif çabalarını yansıtır.

Dijital rekabetçilik ve gelişim endekslerine göre dünyadaki ilk beş ülke ABD, Singapur, Güney Kore, Almanya, Finlandiya olarak sıralanmaktadır.¹⁶ Dijital rekabetçilik ve gelişim endekslerine göre sıralanan ülkeler, siber saldırılara karşı dayanıklılığı artıran teknoloji uygulamalarını ne kadar benimsediklerine ve hükümetlerin güvenli dijital işlemleri destekleyen politika çerçevelerine dayalı olarak değerlendirilmektedir. Bu sıralama, ülkelerin performansını kritik altyapı, siber güvenlik kaynakları, kurumsal kapasite ve politika taahhüdü gibi dört ana kriterdeki puanlarına göre belirlemektedir.

¹⁶ Global Innovation Index 2023, World Economic Forum.

2.2. Kritik Dijital Altyapıların Dayanıklılığı ve İş Sürekliliği

Kritik altyapı kavramı, 1997 yılında (ABD) Başkanlık Kritik Altyapı Koruma Komisyonu (PCCIP) raporunun yayınlanmasıyla ön plana çıkmıştır¹⁷. Bu rapor, enerji, ulaşım, telekomünikasyon, su gibi toplumun ve ekonominin işleyişi için gerekli olan sektörleri ve sistemleri belirlemiştir.

1998 Başkanlık Karar Direktifi 63 (PDD-63)

Mayıs 1998'de ABD Başkanı Bill Clinton, ulusal güvenliği ve ekonomik refahı sağlamak için kritik altyapının korunmasının önemini vurgulayan PDD-63'ü yayınlamıştır¹⁸. Direktif, devlet kurumları, özel sektör kuruluşları ve diğer paydaşlar arasındaki iş birliği yoluyla kritik varlıkların güvenliğini ve dayanıklılığını artırmaya yönelik bir çerçevenin ana hatlarını çizmiştir.

O tarihten bu yana, kritik altyapının korunması ABD'deki ardışık yönetimler için en önemli öncelik olmaya devam etmiştir. Çabalar, kilit sektörlerde risk yönetimi, bilgi paylaşımı, siber güvenlik, fiziksel güvenlik ve dayanıklılık önlemlerinin iyileştirilmesine odaklanmıştır. İç Güvenlik Bakanlığı (DHS), CIP (Critical Infrastructure Protection) çabalarını koordine etmede ve ortaya çıkan tehditleri ve güvenlik açıklarını ele almak için paydaşlarla birlikte çalışma konusunda merkezi bir rol oynamaktadır.

Genel olarak, kritik altyapının ulusal güvenlik ve toplumsal refah açısından hayati öneme sahip olduğunun kabul edilmesi, bu altyapının çeşitli tehdit ve tehlikelere karşı korunmasını ve dayanıklılığını artırmaya yönelik çabaların devam etmesine yol açmıştır.

AB, kritik varlıkları terörizm de dâhil olmak üzere çeşitli tehditlere karşı korumanın önemini kabul etmiş ve bu varlıkların güvenliğini ve dayanıklılığını artıracak önlemleri uygulamaya koymuştur. Atılan önemli adımların bir özeti şu şekildedir:

2004 Terörle Mücadelede Kritik Altyapıların Korunması Raporu

Avrupa Komisyonu bu raporu 20 Ekim 2004'te yayınladı. Raporda kritik altyapılar tanımlandı, tehditler tespit edildi ve güvenliklerinin artırılmasına yönelik önlemlere ilişkin öneriler

¹⁷ Başkanlık Kritik Altyapı Koruma Komisyonu Raporu (PCCIP), 1997.

¹⁸ Critical Infrastructure Protection (PDD-63), 1998.

sunuldu. Bu rapor, AB içindeki kritik altyapının korunmasına yönelik sonraki eylemlerin temelini oluşturdu.

Avrupa Kritik Altyapıların Korunması Programı (EPCIP)¹⁹: 2004 raporuna yanıt olarak Avrupa Komisyonu, 2004 yılında EPCIP'yi başlattı. Bu program, AB üye ülkeleri genelinde kritik altyapıların güvenliğini güçlendirmeyi amaçlamaktaydı.

17 Kasım 2005'te Avrupa Komisyonu, EPCIP'in kurulmasına ilişkin politika ilkelerini özetleyen bir belge yayınladı. Bu ilkeler, kritik altyapıların AB düzeyinde korunmasına yönelik çabaları koordine etmek için bir çerçeve sağladı. EPCIP, Avrupa Konseyi tarafından duyurulduğu üzere Nisan 2007'de tamamlanmıştır. Üye ülkelere kendi sınırları içindeki kritik altyapıları koruma sorumluluğu verildi. EPCIP'in tamamlanmasının ardından Avrupa Komisyonu, Avrupa'daki kritik altyapıların belirlenmesi ve bunların tehdit ve saldırılara karşı korunmasına yönelik prosedürler geliştirerek çalışmalarına devam etti. Devam eden bu çaba, AB'nin kritik varlıkların güvenliğini ve dayanıklılığını artırma konusundaki kararlılığını yansıtmaktadır.

Genel olarak AB'nin kritik altyapıları koruma yaklaşımı, üye devletler arasında iş birliğini, AB düzeyinde koordinasyonu ve çeşitli sektörlerde tehditleri azaltmaya ve güvenliği artırmaya yönelik politika ve prosedürlerin geliştirilmesini içerir.

Avrupa Konseyi'nin 2008/114/EC sayılı Direktifi

Avrupa Komisyonu'nun 2009 raporuyla birlikte, AB içindeki kritik varlıkların güvenliğinin ve dayanıklılığının artırılmasına yönelik süregelen kararlılığın altını çizmektedir. Bu gelişmeleri kısaca özetleyecek olursak:

Konsey Direktifi 2008/114/EC²⁰, Avrupa Birliği Konseyi tarafından yayınlanan bu direktif, özellikle enerji ve ulaştırma sektörlerinde kritik altyapıların güvenliğinin artırılmasına odaklanmaktadır. Ancak aynı zamanda bilgi ve iletişim teknolojilerine ilişkin hükümleri de içermektedir. Bu direktif, temel sistemleri terörizm de dâhil olmak üzere çeşitli tehditlere karşı korumanın önemini vurgulamaktadır.

¹⁹ European Programme for Critical Infrastructure Protection (EPCIP), 2004.

²⁰ The Council of The European Union, 2018

Avrupa Komisyonu tarafından 30 Mart 2009'da yayınlanan Avrupa'nın Büyük Ölçekli Siber Saldırlara ve Kesintilere Karşı Korunmasına İlişkin Rapor²¹, siber saldırıların kritik altyapılara yönelik oluşturduğu artan tehdidi ele almaktadır. Büyük ölçekli siber olayların etkisini azaltmak için hazırlığı, güvenliği ve dayanıklılığı artırma ihtiyacını vurgulamaktadır. Bu, kritik altyapının karşılaştığı tehditlerin gelişen doğasını ve güvenlik önlemlerinin buna göre uyarlanmasının önemini yansıtmaktadır.

Genel olarak bu belgeler, Avrupa Birliği'nin kritik altyapıya yönelik tehditlerin yol açtığı güvenlik sorunlarını ele alma konusundaki kararlılığının altını çizmektedir. Siber güvenlik hususlarının dâhil edilmesi, modern altyapı sistemlerinin birbirine bağlı doğasının ve kapsamlı koruma önlemlerine duyulan ihtiyacın kabul edildiğini göstermektedir. AB, güvenliğe ve dayanıklılığa öncelik vererek kesinti riskini en aza indirmeyi ve vatandaşları için temel hizmetlerin sürekliliğini sağlamayı amaçlamaktadır.

2.3. Veri Egemenliği Politikaları ve Kriptoloji

Birçok ülke ve bölge, veri merkezi endüstrisinin öneminin farkındadır ve rekabetçi vergi indirimleri de dâhil olmak üzere çeşitli yollarla veri merkezi sektörünün büyümesini aktif olarak teşvik etmektedir. Bu vergi teşvikleri, veri merkezi sektöründe yatırımı çekmek, ekonomik aktiviteyi teşvik etmek ve sürdürülebilirliği teşvik etmek için tasarlanmıştır. Veri merkezi endüstrisini desteklemek için ülkeler ve bölgeler tarafından sunulan bazı yaygın vergi indirimi türleri vardır.

- *Vergi muafiyetleri:* Hükümetler, yeni veri merkezi projelerine veya genişletmelerine belirli bir süre için kurumsal gelir vergisinden veya diğer vergilerden geçici muafiyetler sunabilir. Bu, şirketleri yetki alanı dâhilinde veri merkezi tesisleri inşa etmeye veya genişletmeye yatırım yapmaya teşvik eder.

²¹ Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, 2009.

- *Sermaye yatırımı teşvikleri:* Veri merkezi altyapısını kurmak veya geliştirmek için gerekli olan inşaat, yenileme veya ekipman alımlarıyla ilgili sermaye harcamaları için veri merkezi operatörlerine vergi kredileri veya kesintileri sağlanabilir.
- *Satış vergisi muafiyetleri:* Hükümetler, veri merkezlerinin inşaatı, işletimi veya bakımında kullanılan belirli ekipman, malzeme veya hizmetlere ilişkin satış vergilerinden feragat edebilir veya azaltabilir. Bu, veri merkezi projeleri için ön maliyetlerin azaltılmasına yardımcı olur ve altyapı geliştirme yatırımlarını teşvik eder.
- *Emlak vergisi teşvikleri:* Yerel makamlar, veri merkezi tesisleri, arazi veya ekipmanı için emlak vergisi indirimleri veya indirimleri sunabilir. Bu teşvikler, veri merkezi operatörlerinin işletme maliyetlerini düşürür ve bölgeyi yatırım için daha cazip hâle getirir.
- *Enerji verimliliği teşvikleri:* Hükümetler, yenilenebilir enerji üretimi, soğutma sistemi optimizasyonu veya atık ısı geri kazanımı gibi enerji açısından verimli teknolojiler veya uygulamalar uygulayan veri merkezleri için teşvikler veya hibeler sağlayabilir. Bu, sürdürülebilirliği teşvik eder ve veri merkezi operasyonlarının çevresel etkisinin azaltılmasına yardımcı olur.

Genel olarak, bu vergi indirimleri ve teşvikler, veri merkezi endüstrisinde yenilikçiliği teşvik etmeye, yatırımı çekmeye, iş yaratmaya ve çevresel sürdürülebilirliği teşvik etmeye yönelik daha geniş hükümet stratejilerinin bir parçasıdır. Ülkeler ve bölgeler, rekabetçi vergi teşvikleri sunarak kendilerini veri merkezi yatırımı için uygun yerler olarak konumlandırmayı ve dijital ekonomilerinin büyümesine ve gelişmesine katkıda bulunmayı amaçlamaktadır.

2.4. Toplumsal Dijital Dayanıklılığın Sağlanması

Dijital vatandaş, siber vatandaş, siber güvenilir vatandaş, dijital dayanıklılık, dijital dayanıklı toplum gibi görece yeni kavramlar bir süredir dünya kamuoyunun gündemine girmiştir.

Bu kavramlar içerisinde dijital dayanıklı vatandaş, modern toplumun sosyal direnç kapasitesinde hayati bir rolü ifade etmektedir.

Dirençli bir toplumun yeni teknolojilerin doğasına ve etkisinin yarattığı değişime hazır, uyum becerisi yüksek ve zorlu zamanlarda kendisini destekleyebilen bir yapı olduğu görüşü yaygınlaşmaktadır. Dijital eğitimin sosyal ve ekonomik büyüme üzerindeki yadsınamaz faydaları yanında hızlı öğrenme ve kavrayışla teknoloji anlayışını artırabileceği görülmektedir. Dolayısıyla belirsiz ve zor zamanlara hazırlanmanın anahtarı, değişime uyum sağlayabilen, yaratıcı ve kapsamlı dijital yeterlilik becerilerine sahip vatandaşları geliştirmektir.

Bu kapsamda, toplumsal dijital dayanıklılığı artırmak hedefiyle Avrupa Birliği Komisyonu, dezenformasyonla mücadeleyle ilişkin 2018’de bir eylem planı yayımlamıştır. Eylem planının önemli maddelerinden biri, üye devletler arasında irtibat, koordinasyon ve iş birliğini artırmak suretiyle birlikte hareket edebilmeyi sağlamaya yönelik web tabanlı Hızlı Alarm Sistemi’nin (*The Rapid Alert System - RAS*) hayata geçirilmesi olarak açıklanmıştır²². 2019 Mart ayında hizmete alındığı belirtilen söz konusu sistemin çalışırılığına dair açık kaynakta herhangi bir bilgiye rastlanmamıştır. AB faaliyetleri kapsamında ayrıca, Rusya’nın ‘dezenformasyon’ kampanyalarına karşı 2015’ten bu yana stratejik iletişim faaliyetleri yürüten Doğu Stratejik İletişim Görev Gücü bulunmakta ve bu kapsamda *EUvsDisinfo* isimli bir web portal işletilmektedir²³.

Bahsi geçen gayretlere ek olarak, haber değeri taşıyan dosyaların ve sosyal medya aracılığıyla yayılan içeriğin tespit edilmesi ile güvenilirliğinin ve doğruluğunun kontrol ve teyidi için hizmet sağlayan *InVid* isiminde bir platform bulunmaktadır.²⁴

Diğer yandan, Haziran 2024’te yapılan Avrupa Parlamentosu seçimleri öncesinde kullanıcıları dezenformasyondan korumak maksadıyla Facebook ve Instagram’ın sahibi Meta, çalışmalarını hızlandırmıştır. Şirket, 24 Şubat 2024’te yaptığı açıklamada, Avrupa’da; istihbarat uzmanları, veri bilimcileri, mühendisler ve araştırmacılardan oluşan bir ekip kurmayı planladığını ve bu ekibin, seçimle ilgili tehditleri gerçek zamanlı olarak tespit etmek ve azaltmakla görevlendirileceğini duyurmuştur. Buna ek olarak Meta, Bulgaristan, Fransa ve Slovakya’da üç

²² EU Commision, Action Plan Against Disinformation, 2018

²³ AB Dezenformasyonla Mücadele Platformu, <https://euvsdisinfo.eu/about/>

²⁴ AB Video Teyit Platformu, <https://www.invid-project.eu/>

yeni ortakla ‘Doğruluk Kontrol Ağını’ genişleteceğini ve platformlarındaki içeriği inceleyen ve derecelendiren bağımsız doğruluk kontrolörlerinin toplam sayısını AB genelinde yaklaşık 30’a çıkartacağını belirtmiştir.²⁵

Kanada Vatandaşlık Enstitüsü, Dayanıklı Vatandaş²⁶ ‘*Citizen Resilience Project*’ isminde bir proje yürütmektedir. Proje, Kanadalıları yanlış bilgi tehditlerini tanımaya, mücadeleye ve iş birliğine teşvik etmeyi amaçlamaktadır. Vatandaşların çevrimiçi içerik türleri arasında ayrım yapabilmesinin önemine odaklanan proje, haber, haber benzeri içerik, reklam ve uydurulmuş içerik gibi çeşitli bilgi türlerini tanımlama konusunda rehberlik etmektedir. Kullanıcıların, okudukları şeylerin arkasındaki etkileri ve ön yargıları sorgulayarak eleştirel düşünme becerilerini geliştirmeleri ve daha üretken bir kamu iletişimi oluşturabilmeleri için kendilerine sorabilecekleri bir dizi soru sunmaktadır.

Projede ayrıca, İnternet üzerindeki ayrıştırıcı dilin tehlikelerine dikkat çekilerek son dönemde birçok konuda kutuplaşmanın arttığı ve İnternetin de nefret dolu içeriklerin yayılmasına ortam sağlayarak ayrışmayı derinleştirdiği tespitinden yola çıkılarak, bu durumun kamu kurumlarına ve vatandaşların birbirlerine olan güvensizliği artırdığı belirtilmektedir. Doğru bilgiyi tanıma ve sağlıklı bir bilgi alışkanlığı için kullanılabilecek çeşitli araçlar hakkında vatandaşlara ipuçları da sunulan çalışmada, çeşitli topluluk etkinlikleri, eğitim kaynakları ve çevrimiçi kampanyalar da önerilmektedir.

OECD tarafından yayımlanan “21. Yüzyıl Okurları: Dijital Dünyada Okuryazarlık Becerilerinin Geliştirilmesi” başlıklı, Türkiye’nin de dâhil olduğu rapora göre, OECD ülkelerinde 15 yaşındaki gençlerin %88’i İnternete ve dijital cihazlara erişim imkânına sahip olmasına rağmen, bu kişilerin yalnızca %54’ü, ulaştığı bilginin doğru olup olmadığını nasıl anlayacağını okulda öğrenmektedir. İlgili bir diğer OECD verisine göre ise adı geçen gençlerin yalnızca %9’u gelişmiş okuma becerilerine sahip bulunmakta ve okuduğu metindeki gerçekleri fikirlerden ayırt edebilmektedir.

Pandemiyle birlikte daha da önem kazanan bu beceri, kişilerin dijital kaynaklardaki ön yargılı bilgileri, sahte haberleri ve kötü niyetli içerikleri tespit edebilmesini sağlamaktadır.

²⁵ Halil ÖZTÜRKÇİ, X (Twitter), <https://x.com/halilozturkci/status/1762786304431968661>

²⁶ Dayanıklı Vatandaş Programı, Kanada, <https://inclusion.ca/research-and-ideas/citizen-resilience-project-2/>

OECD'nin bu raporu ayrıca, dijital ortamda ön yargılı bilgilerin nasıl tespit edileceği konusunda eğitim alma imkânının ülkeden ülkeye farklılık gösterdiğini ortaya koymaktadır.

Bu konuda Avustralya, Kanada, Danimarka ve Amerika Birleşik Devletleri'ndeki öğrenciler, İsrail, Letonya, Slovak Cumhuriyeti, Slovenya ve İsviçre'deki akranlarına göre neredeyse 2 kat daha fazla imkâna sahip bulunmaktadır. Rapora göre, dijital okuryazarlık becerilerinin geliştirilmesi için bilgiyi eleştirel bir şekilde anlamak, hatırlamak, özetlemek ve değerlendirmek gerekmektedir. Ayrıca, dijital cihazların ve İnternetin nasıl ve hangi amaçla kullanıldığı da dijital okuryazarlık becerilerinin artmasında belirleyici olmaktadır²⁷.

Dijital okuryazarlık düzeyini etkileyen bazı temel unsurlar aşağıda sıralanmıştır.

- *Teknolojiye erişim:* Dijital okuryazarlık, bilgisayarlar, akıllı telefonlar ve İnternet gibi teknolojiler gerektirir. Teknolojiye erişim düzeyi yüksek olan ülkelerin dijital okuryazarlık düzeylerinin daha yüksek olması gerektiği yargısı aklın gereğidir.
- *Eğitim ve öğretim:* Dijital okuryazarlık becerileri genellikle eğitim ve öğretim programları aracılığıyla geliştirilir. İnsanlara teknolojiyi öğrenmeleri ve kullanmaları için fırsatlar sağlayan güçlü eğitim sistemlerine sahip ülkelerin dijital okuryazarlık düzeylerinin daha yüksek olması beklenir.
- *Sosyoekonomik faktörler:* Gelir, eğitim ve meslek gibi sosyoekonomik faktörler, bir kişinin teknolojiye erişimini ve dijital okuryazarlık becerilerini geliştirme fırsatlarını etkileyebilir. Daha düşük sosyoekonomik geçmişe sahip insanlar, teknolojiye daha az erişebilir ve dijital okuryazarlıklarını geliştirmek için daha az fırsata sahip olabilir, bu da genel olarak daha düşük dijital okuryazarlık seviyelerine neden olabilir.
- *Yaş:* Yaş, dijital okuryazarlıkta önemli bir faktördür. Genç nesillerin dijital okuryazar olmak için gerekli cihazlara ve İnternet bağlantılarına ve gerekli eğitime erişme olasılığı daha yüksektir.
- *Kültürel ve dille ilgili engeller:* Dijital okuryazarlık, teknolojiyi kullanma konusunda kültürel veya dille ilgili engeller bulunan ülkelerde daha düşük olabilir. Ana dilinde İnternet kullanmayan kişiler bu teknolojilere erişim ve yararlanmada zorluk yaşayabilir.

²⁷ Türkiye'de Dijital Dönüşüm ve Dijital Okuryazarlık, BTK, Aralık 2022

- *Devlet politikaları ve girişimleri:* Hükümetler, teknolojiye erişimi, eğitim ve öğretim programlarını ve dijital uçurumu kapatma çabalarını destekleyen politikalar ve girişimler yoluyla dijital okuryazarlığı teşvik edebilir. Dijital okuryazarlık için güçlü devlet desteğine sahip olan ülkelerin, nüfusa oranla daha yüksek dijital okuryazarlık seviyelerine sahip olması muhtemeldir.

Dijital dayanıklılık konusunda dünyadaki genel duruma birey ve toplum perspektifinden bakıldığında özetle, bilgi ve iletişim teknolojilerinin yaygınlaşmasıyla artık her bir bireyin güvenlik, direnç ve dayanıklılık gibi konularda önem kazandığı ve siber saldırılar ile dezenformasyonun hedefi olduğu görülmektedir. Bilinçli bireylerin, saldırılara karşı daha uyanık olmaları hem onları hem de toplumu daha bağışık ve müreffeh kılacaktır.

2.5. Siber Olayların ve Siber Olaylara Müdahalenin Dönüşümü

Yeni nesil dijital teknolojilerin benimsenmesi, organize siber olayların ve siber olaylara müdahalenin dönüşümünde dünya genelinde önemli bir etkiye sahiptir. Bu teknolojik gelişmeler, siber alanın dinamik yapısını değiştirerek hem saldırganlar hem de savunma mekanizmaları için yeni fırsatlar ve zorluklar yaratmaktadır.

Organize siber olaylar, geleneksel suç faaliyetlerinin dijital ortama taşınmasıyla giderek karmaşık hâle gelmektedir. Siber suçlular, gelişmiş kötü amaçlı yazılımlar, fidye yazılımları ve diğer zararlı araçlar kullanarak hükümetler, işletmeler ve bireyler üzerinde ciddi ekonomik ve güvenlik tehditleri ile baskı oluşturmaktadır.

Siber olaylara müdahalede, yapay zekâ, makine öğrenimi ve büyük veri analitiği gibi yeni teknolojilerin kullanımı önemli bir dönüşüm sağlamaktadır. Bu teknolojiler, siber saldırıları tespit, analiz ve önleme yeteneklerini artırarak, müdahale süreçlerini daha hızlı ve etkili hâle getirebilmektedir.

Ayrıca, uluslararası iş birliği ve ortak stratejiler de siber olaylara müdahalede önemli bir rol oynamaktadır. Uluslararası platformlarda bilgi paylaşımı, ortak tatbikatlar ve standartların belirlenmesi gibi girişimler, siber tehditlere karşı daha etkili bir savunma sağlamak için gereklidir.

Bu kapsamdaki genel eğilimler, hızla evrensel bir tehdit hâline gelen siber suçların ve organize siber olayların artışıyla şekillenmektedir. Yeni nesil dijital teknolojilerin benimsenmesiyle birlikte, siber saldırganlar daha sofistike ve karmaşık saldırı yöntemleri geliştirmekte, hedeflerini genişletmekte ve güvenlik önlemlerini aşmak için çeşitli yeni taktik ve teknikler kullanmaktadır.

Bu eğilimlere yanıt olarak, devletler ulusal ve uluslararası düzeyde siber güvenlik politikaları oluşturmakta, savunma kapasitelerini artırmakta ve siber suçlarla mücadele için iş birliği ve ortaklıklar yapmaktadır. Özel sektördeki kuruluşlar da siber güvenlik önlemlerini güçlendirmekte, uzmanlaşmış firmalara yatırım yapmakta ve kamu-özel iş birlikleri aracılığıyla daha etkin bir koruma sağlamaya çalışmaktadır.

Ayrıca, yapay zekâ ve makine öğrenimi gibi teknolojilerin kullanımıyla birlikte, siber güvenlik alanında otomatik tespit ve yanıt sistemleri geliştirilmekte ve siber saldırıları önlemek için daha proaktif yaklaşımlar benimsenmektedir.

Küresel düzeyde, uluslararası toplum siber güvenlik standartlarını ve regülasyonları güçlendirmekte, uluslararası iş birliğini teşvik etmekte ve siber suçlarla mücadele için koordinasyon sağlamaktadır.

Bu bağlamda, siber güvenlik alanındaki genel eğilimler, teknolojik yeniliklerin yanı sıra uluslararası iş birliği ve etkili politika oluşturma önemini de bir kez daha hatırlatmaktadır. Yeni nesil dijital teknolojilerin organize siber olaylar ve siber olaylara müdahale üzerindeki etkisi, sürekli olarak evrilen bir alan olup, teknolojik yeniliklerin yanı sıra uluslararası iş birliği ve koordinasyonun önemini de artırmaktadır.

Bilgi ve iletişim teknolojilerinde yaşanan gelişmeler ışığında siber tehditler, gün geçtikçe daha karmaşık, zor tespit edilebilir, daha yaygın ve sayıca çok bir görünüm arz etmektedir. Bu durum hem fırsat hem de tehditleri beraberinde getirmektedir. Bu tehditlerle mücadelede yeni nesil teknolojilerden istifade edilmesi önem arz etmektedir. Yapay zekâ, kuantum hesaplama gibi gelişmeler özellikle bu alanda dikkat çekmektedir.

Gelişen teknoloji, İnternete kolay erişim ve dijitalleşmenin hızlı yükselişi sonucu, erişilebilirlik, bütünlük ve gizlilik/güvenlik dengesinde bilince bağlı olarak değişen bir düzlemde saldırıların faaliyet alanı da genişlemiş, çok vektörlü bir saldırı ortamı doğmuştur.

Yeni nesil dijital teknolojiler, siber olayların doğasını ve müdahale yöntemlerini önemli ölçüde değiştirmektedir. Yapay Zekâ, Bulut Bilişim, Nesnelerin İnterneti ve 5G Teknolojileri bir yandan siber kabiliyetlere imkân tanırken bazı sınamaları da beraberinde getirmektedir. Geline nokta, siber güvenliği sağlamak için bu yeni teknolojilerin sunduğu fırsatlardan yararlanmak ve siber saldırılara karşı proaktif bir yaklaşım benimsemek önem kazanmıştır.

Riskleri en aza indirmek ve oluşabilecek tehlikeleri bertaraf etmek maksadıyla gelişmiş ülkeler ve güçlü uluslararası kuruluşlar, eksiksiz bir mevzuat, işleyen bir organizasyon ve uygulanabilir kurallar oluşturmanın yanı sıra, tatbikatlarla siber güvenlik direnç ve kondisyonlarını yukarıda tutmaya, büyük araştırma projeleri ve önceliklendirmelerle de alandaki teknolojiye liderlik etmeyi hedeflemektedirler.

2.5.1. Siber Saldırı Trendleri ve Yeni Nesil Tehditler

Avrupa Birliği Siber Güvenlik Kurumu (ENISA) tarafından 2023 yılı siber olayları incelenerek başlıca tehdit alanları olarak; Fidyeye Yazılımı, Kötücül Yazılımlar, Sosyal Mühendislik, Veri Sızıntısı, DDoS, İnternet Kesintileri, Bilgi Manipülasyonu, Tedarik Zinciri Saldırıları olarak sıralanmıştır.²⁸ Yine aynı raporda, yapay zekâ destekli sosyal mühendislik saldırılarında dikkat çekici artış görüldüğü, yeni saldırı türü ve taktiklerin gelişmesi ile birlikte ortalama saldırılarının hâlâ başı çektiği belirtilmiştir.

Yapay Zekâ

Artık yapay zekâ ile insan veya şirket davranışını taklit edebilen çok daha gerçekçi e-postalar gönderilebilmekte, insan ses ve görüntüsünü klonlamak suretiyle sahtecilik yapılabilmekte ve veri madenciliği gerçekleştirilebilmektedir. Bu kapsamda 2023 yılı Ocak ile Şubat arasında sosyal mühendislik saldırılarında %135’lik bir artış görüldüğü rapor edilmiştir²⁹. Yapay zekâ ile veri madenciliğinde (AI-driven data mining) ise saldırının başarı ihtimalini artırmak maksadıyla

²⁸ ENISA Threat Landscape 2023 July 2022 to June 2023, Ekim 2023

²⁹ DARKTRACE, <https://ir.darktrace.com/pressreleases/2023/4/3/>

kurbana dair yapay zekâ marifetiyle toplanan verilerle ona en zayıf olduğu zamanda en doğru noktadan yaklaşmak hedeflenmektedir.

Raporda ayrıca; yapay zekâ sohbet robotları kullanımında yaşanan patlamanın, siber güvenlik tehditlerine ilişkin manzarayı etkilediği, OpenAI ChatGPT, Microsoft Bing ve Google Bard gibi üretken yapay zekâ sohbet botlarının benimsenmesinin, iş, yaşam ve eğlence alanlarında köklü değişikliklere yol açtığı ve bu değişimin, veri paylaşımı ve analizi etrafında şekillenmekte olduğu belirtilmektedir.

Kendi Yapay Zekâ Aracını İşe Getir! (Bring Your Own AI, BYOAI)

Çalışanların kendi bilgi sistem cihazlarını iş yerlerine getirmeleri ve bunları çalışmalarında kullanmaları Kendi Cihazını Getir (Bring Your Own Device - BYOD) sloganıyla bir süredir çalışma hayatında yer bulmaktadır. Bu sayede şirketlerin işletme maliyetleri azalırken, iş ve özel hayat arasındaki çizgi belirsizleşmekte ve işletme lehine finansal anlamda bazı somut sonuçlar ortaya çıkmaktadır.

Kendi yapay zekâ aracını işe getir kavramı da bu noktadan esinlenmekle birlikte başka bir güvenlik riskine işaret etmektedir. Beyaz yakalı çalışanlar bir süredir görevlerini yerine getirmede yapay zekâ araçlarından yararlanmakta, bu sayede zaman tasarrufunda bulunarak iş ve yaşam kalitelerini artırmaktadırlar. Oysa, "Kendi Yapay Zekâ Aracını İşe Getir" (BYOAI) eğilimi, istem dışı ve farkında olmadan veri ihlallerine yol açabilir. Kişisel AI araçları genellikle kurumsal düzeyde güvenlik özellikleriyle tasarlanmadığından, hassas bilgileri açığa çıkarabilir. Bu eğilim, veri güvenliği protokollerinin yeniden değerlendirilmesini ve yapay zekânın profesyonel ortamlarda güvenli kullanımına ilişkin çalışanların eğitimini gerektirmektedir.

Kuantum Hesaplama

Kuantum hesaplama, verileri işlemek için kuantum mekaniğini kullanan bir teknolojidir. Karmaşık sorunları geleneksel bilgisayarlardan çok daha hızlı çözme potansiyeline sahiptir. Bu teknoloji henüz emekleme aşamasında olmasına rağmen, daha güvenli şifrelemeye olanak sağlayarak siber güvenlik alanında devrim yaratma potansiyeline sahiptir³⁰. Diğer taraftan kuantum teknolojisi, günümüzde yaygın kullanılan ve mevcut işlemci gücüyle kırılması çok uzun zaman

³⁰ EC-Council University, <https://www.eccu.edu/blog/technology/the-latest-cybersecurity-technologies-and-trends/>

gerektiren RSA, ECC gibi kriptografik algoritma çözümlerini bir anda geçersiz kılacak ve bu kuantum yeteneği olmayan taraflar çaresiz kalacaktır. Bu nedenle konuya stratejik seviyede önem atfedilmekte ve ABD başta olmak üzere gelişmiş ülkelerin strateji belgelerinde kuantum sonrası döneme yönelik çalışmalar yer bulmaktadır.

Kuantum Sonrası Şifreleme (Post Quantum Cryptography)

Post-Kuantum Kriptografi, kuantum bilgisayarlarının gücünden etkilenmeyecek şekilde tasarlanmış kriptografik algoritmaları tanımlamaktadır. Bu algoritmalar, klasik ve kuantum bilgisayarlar tarafından güvenli bir şekilde kullanılabilir olmalıdır. Post-Kuantum Kriptografide kullanılan teknikler arasında kriptografik kafesler, kod tabanlı kriptografi ve çok taraflı hesaplama gibi çeşitli yaklaşımlar bulunur. Bazı önemli post-kuantum algoritmalar ve kısa açıklamaları şu şekildedir³¹.

- Izgara Tabanlı Kriptografi (Lattice-based Cryptography):
 - *NTRUEncrypt*: Açık anahtarlı bir şifreleme algoritmasıdır. Çalışma prensibi, çok büyük boyutlu matrisler ve çok terimli çarpımlar üzerine kuruludur.
 - *Learning With Errors (LWE)* ve *Ring-LWE*: Şifreleme ve imza şemalarında kullanılan matematiksel problemler üzerinedir. Matematiksel yapıları kuantum bilgisayarların çözmesini zorlaştırır.
- Kod Tabanlı Kriptografi: (Code-based Cryptography)
 - *McEliece Şifreleme Sistemi*: Büyük hata düzeltme kodlarına dayanır ve kuantum bilgisayarlar karşı dayanıklıdır.
 - *Niederreiter Şifreleme Sistemi*: McEliece sisteminin bir varyantıdır ve benzer dayanıklılığa sahiptir.
- Çok Taraflı Kuadratik Denklem Tabanlı Kriptografi (Multivariate Quadratic Equations)
 - *HFE (Hidden Field Equations)*: Kuadratik polinomlar üzerinden çalışan bir imza algoritmasıdır.

³¹ Post-Quantum Cryptography, NIST, <https://csrc.nist.gov/projects/post-quantum-cryptography>

- *Rainbow*: Çok değişkenli kuadratik denklemler kullanan bir imza şemasıdır. Birden fazla katman kullanarak güvenliği artırır.

5G

Beşinci nesil kablosuz iletişim teknolojisini ifade eder. Mobil iletişimde bir sonraki aşama olarak kabul edilen 5G, önceki nesil kablosuz teknolojilere göre çok daha hızlı veri aktarım hızları ve düşük gecikme süreleri sunar. Bu teknoloji, geniş bant bağlantısı, daha yüksek kapasite ve daha fazla cihazın aynı anda bağlanabilmesi gibi özellikleriyle dikkat çeker.

Dolayısıyla 5G, yüksek hızlı veri indirme ve yükleme, daha düşük gecikme süreleri ve bağlantı istikrarı gibi avantajlarıyla daha iyi mobil İnternet deneyimi, daha kaliteli video akışı, sanal ve artırılmış gerçeklik uygulamalarının daha etkin kullanımı gibi birçok fayda sağlar. Ayrıca, Nesnelerin İnterneti (IoT) cihazlarının daha verimli bir şekilde bağlanmasına ve iletişim kurmasına yardımcı olur.

5G teknolojisi, mobil iletişim altyapısının yeniden şekillendirilmesine ve gelecekteki dijital dönüşümün temelini oluşturmaya yönelik büyük bir adımdır. Bu teknoloji, daha akıllı ve bağlantılı bir dünya için gerekli altyapıyı sağlayarak birçok endüstride devrim yaratma potansiyeline sahiptir.

Sunduğu bu imkânların yanında 5G kullanımıyla artan bant genişliği ve bağlantı sayısı nedeniyle saldırı yüzeyi genişleyecek, saldırının şiddeti artacaktır. Bu olumsuzluğu en aza indirmek, yetkisiz erişimi ve veri ihlallerini önlemek amacıyla ilave katmanlandırma (*segmentation*) ve yalıtım (*isolation*) tedbirlerine gereksinim duyulacaktır³².

IoT Cihazları

IoT cihazlar ise, yaygınlıkları, görece zayıf donanımları, çoğunlukla konfigüre edilmeden hatta varsayılan parolaları dahi değiştirilmeden kullanılmaları, mobil cihazlar başta olmak üzere kullanıcılarının teknik bilgilerinin oldukça sınırlı olması gibi nedenlerle siber saldırıların hedefi olmakta, özellikle dağıtık servis dışı bırakma (DDoS) saldırılarının hem hedefi hem de bir ‘askeri’ olarak rol alabilmektedir.

³² MetaCompliance, MetaBlog, <https://www.metacompliance.com/blog/cyber-security-awareness/emerging-technologies-and-their-impact>

Blokzincir Teknolojisi

Blokzincir teknolojilerinin dağıtık ve otonom yapısı gereği veri güvenliği uygulamalarında kullanılması hususu değerlendirilmektedir. Diğer yandan özellikle fidye saldırılarında kurbandan tahsilat kripto paralar vasıtasıyla bu teknoloji üzerinden yapılmakta, yine blok zincirdeki güvenlik zafiyetleri kullanılarak insanlar dolandırılmaktadır.

Uzaktan Çalışma

Özellikle pandemi sırasında ve sonrasında, merkezi gözetim ve denetimden uzak bir şekilde yaygınlaşan uzaktan çalışma uygulaması birtakım siber güvenlik risklerini de beraberinde getirmekte, bu kapsamda; işle ilgili konularda kişisel bilgisayar kullanımı kurum güvenlik standartları ve sıkılaştırmalarının dışına çıkılmasına neden olmakta, çalışanlar güvensiz olarak kamuya açık İnternet ağlarından (Wifi) bağlanabilmekte, bulut bilişim kullanma zorunluluğu nedeniyle olası zafiyet alanları oluşmakta, kullanıcılar sosyal mühendislik ve oltalama saldırılarına karşı daha açık bir hâlde bulunmakta, kullanılan VPN'deki bir zafiyet bütün operasyonu riske sokmakta, yama yönetimi ve uç kullanıcı güvenlik yönetimi son derece zorlaşmakta, yakın gözetim olamadığından iç tehditlerin artması ihtimali çoğalmaktadır.

Devlet Destekli Siber Tehditler

Siber saldırıların ulus devletler tarafından siyasi hedeflere ulaşmak için stratejik bir araç olarak kullanılması, kuruluşların siber güvenlik stratejilerinde jeopolitik dinamikleri dikkate almaları ihtiyacını doğurmuştur. Devlet tarafından yaratılan bu tür siber tehditler, genellikle son derece karmaşık teknikler, sıfır gün açıklıkları ve önemli kaynaklar içermesi bakımından gerek özel sektör gerekse hedef ülkenin ilgili kamu kurum ve kuruluşları için karşı tedbir alma konusunda önemli zorluklar barındırır.

2.5.2. Yeni Nesil Siber Güvenlik Teknoloji ve Konseptleri

Yeni nesil siber tehditlere karşı geliştirilen ve yaygınlaşmakta olan bazı teknoloji ve konseptler kısa açıklamalarıyla birlikte aşağıda sunulmuştur³³.

Davranışsal Analiz (Behavioral Analytics)

³³ Cyber Degrees, 21.03.2023, <https://www.cyberdegrees.org/resources/hot-technologies-cyber-security/>

Davranışsal analiz, insanların web sitelerinde, mobil uygulamalarda, sistemlerde ve ağlarda nasıl davrandıklarını anlamak için verilere bakar. Siber güvenlik uzmanları, davranışsal analiz platformlarını potansiyel tehditleri ve zayıflıkları bulmak için kullanabilirler. Davranış kalıplarını analiz etmek, siber güvenlik tehditlerini işaret edebilecek olağandışı olayları ve eylemleri belirlemenin bir yolunu sağlayabilir.

Örneğin, davranışsal analiz, olağandışı derecede büyük veri miktarlarının bir cihazdan geldiğini bulabilir. Bu, bir siber saldırının yaklaşmakta veya aktif olarak gerçekleşmekte olduğu anlamına gelebilir. Kötü niyetli faaliyetlerin diğer belirtileri arasında olayların garip zamanlaması ve olağandışı bir sıra içinde gerçekleşen eylemler de bulunur.

Davranışsal analiz kullanmanın faydaları arasında potansiyel saldırıların erken tespiti ve gelecekteki saldırıları tahmin etme yeteneği bulunur. Kuruluşlar, davranışsal analiz kullanarak tespit ve yanıtı otomatikleştirebilirler.

Blokzincir (Blockchain)

Blokzincir, verileri bloklar hâlinde güvenli bir şekilde depolayan bir veri tabanı türüdür. Blokları kriptografi aracılığıyla birbirine bağlar.

Blokzincir, bilgilerin toplanmasına izin verirken düzenlenmesini veya silinmesini engeller. Siber güvenlik uzmanları, blokzinciri, sistemleri veya cihazları güvence altına almak, standart güvenlik protokolleri oluşturmak ve saldırganların (hacker) veri tabanlarına sızmasını neredeyse imkânsız hâle getirmek için kullanabilirler. Blokzincirin faydaları arasında daha iyi kullanıcı gizliliği, insan hatası azaltma, daha büyük şeffaflık ve üçüncü taraf doğrulamasına gerek olmaksızın maliyet tasarrufu sağlamak bulunur.

Blokzincir ayrıca verilerin bir yerde depolanma güvenlik sorununu ortadan kaldırır. Bunun yerine, veriler ağda dağıtık olarak depolanır, bu da saldırganların daha çaresiz olduğu merkezi olmayan bir sistem oluşturur. Diğer yandan blokzincir kullanmanın dezavantajları ve zorlukları maliyet ve verimsizlik olarak ifade edilebilir.

Bulut Şifreleme (Cloud Encryption)

Bulut hizmetleri verimliliği artırır, kuruluşların gelişmiş uzaktan hizmetler sunmasına ve tasarruf etmesine yardımcı olur. Ancak verilerin uzakta depolanması güvenlik açıklarını artırabilir.

Bulut şifreleme teknolojisi, verileri buluta girmeden önce anlaşılabilir bilgilerden okunamayan bir koda dönüştürür.

Siber güvenlik uzmanları bulut şifrelemeyi tamamlamak için matematiksel bir algoritma kullanır. Yalnızca şifreleme anahtarına sahip yetkili kullanıcılar kodun kilidini açarak verileri yeniden okunabilir hâle getirebilir. Bu kısıtlı erişim, yetkisiz saldırganların veri ihlali olasılığını en aza indirir.

Bağlama Duyarlı Güvenlik (Context-Aware Security)

Bağlama duyarlı güvenlik, işletmelerin gerçek zamanlı olarak daha iyi güvenlik kararları almasına yardımcı olan bir tür siber güvenlik teknolojisidir.

Geleneksel siber güvenlik teknolojileri, evet/hayır soruları sorarak birinin bir sisteme veya verilere erişmesine izin verilip verilmeyeceğini değerlendirir. Bu basit süreç, bazı meşru kullanıcıların reddedilmesine neden olarak verimliliğin düşmesine neden olabilir.

Bağlama duyarlı güvenlik, yetkili bir kullanıcının girişinin reddedilme olasılığını azaltır. Statik evet/hayır sorularına verilen yanıtlara güvenmek yerine, bir kullanıcının yasal olup olmadığını değerlendirmek için zaman, konum ve URL itibarı gibi çeşitli destekleyici bilgileri kullanır.

Bağlama duyarlı güvenlik, verilere erişim süreçlerini ve meşru kullanıcıların işlerini yapmasını kolaylaştırır. Ancak son kullanıcının gizlilik kaygıları bu teknolojiye bir dezavantaj olarak görülebilmektedir.

Savunma Amaçlı Yapay Zekâ (Defensive Artificial Intelligence - AI)

Siber suçlular, geleneksel siber güvenlik araçlarına nazaran tespiti çok daha zor olan ofansif yapay zekâ ve saldırgan makine öğrenmesi gibi teknolojileri kullanmaktadırlar. Siber güvenlik uzmanları, ofansif yapay zekânın, sistemin veya ağın nasıl çalıştığının öğrenilmesini, ölçülmesini veya test edilmesini engellemek için savunma amaçlı olarak da yapay zekâyı kullanırlar.

Savunma amaçlı yapay zekâ, algoritmaları güçlendirerek kırılmalarını zorlaştırmakta, bu sayede siber güvenlik uzmanları, makine öğrenimi modellerinde daha kapsamlı güvenlik açığı testleri gerçekleştirebilmektedirler.

Savunma amaçlı yapay zekâ kullanımında diğer bazı alanlar; kötücül yazılımların gelişmiş tespiti, güvenlik raporlarını basitleştirme, daha güvenilir erişim kontrolü ve yetkilendirme, ortalama tespit ve engelleme, tehdit tahmini, otomatik sızma testi, tehdit avcılığı, güvenlik kurallarının uygulanmasını sağlama olarak sıralanabilir³⁴.

Kapsamlı Tespit ve Müdahale (Extended Detection and Response - XDR)

Genişletilmiş ya da kapsamlı tespit ve müdahale (XDR), güvenlik tehditlerini ve olaylarını algılayan ve bunlara yanıt veren bir tür gelişmiş siber güvenlik teknolojisidir. Daha basit ve geleneksel uç nokta tespit ve müdahale sisteminden (EDR) evrilen XDR uç noktalarda olduğu gibi bulutta ve ağlarda da çalışabilir.

XDR, farklı yerlerdeki veriler arasında bağlantı kurarak daha bütünsel bir resim sağlar. Bu teknoloji, siber güvenlik çalışanlarının tehditleri, otomatik bir şekilde daha üst seviyeden tespit ve analiz etmesine olanak tanır.

Siber güvenlik uzmanları, hedefli saldırılara yanıt vermek ve bunları tespit etmek, uyarıları otomatik olarak onaylamak, ilişkilendirmek ve kapsamlı analizler oluşturmak için XDR'yi kullanabilir. XDR'nin faydaları arasında tekrarlanan görevlerin otomasyonu, güçlü otomatik algılama ve incelenmesi gereken olay sayısının azaltılması yer alır.

Üretici Kullanım Tanımı (Manufacturer Usage Description - MUD)

Üretici Kullanım Tanımı (MUD), küçük işletme ve ev ağlarındaki IoT cihazlarının güvenliğini güçlendirmek amacıyla IETF (Internet Engineering Task Force) tarafından oluşturulan bir standarttır.

IoT cihazları ağ tabanlı saldırılara karşı savunmasızdır. Bu saldırılar özel verilerin kaybına veya cihazın servis dışı kalmasına neden olabilir. IoT cihazlarının çok fazla maliyet gerektirmeden veya çok karmaşık işlemlere gerek olmadan güvenli hâle getirilmesi gerekir.

MUD kullanmanın IoT cihazları için kullanımı basit ve uygun fiyatlı bir güvenlik çözümü olarak yer alır. Siber güvenlik uzmanları, bu cihazları DDoS saldırılarına karşı daha güvenli hâle

³⁴ Alexander L., 09.01.2024. <https://www.linkedin.com/pulse/emerging-cybersecurity-threats-breakthrough-overview-2024-leschik-om47f/>

getirmek için MUD'u kullanabilir. MUD, bir saldırı durumunda hasarın ve veri kaybının azaltılmasına yardımcı olabilir.

Sıfır Güven (Zero Trust)

Geleneksel ağ güvenliği, bir kuruluştaki ağ içindeki kullanıcıların kötü niyetli olmadığını varsayarak "güven ama doğrula" prensibiyle çalışmaktadır. Zero Trust ise "asla güvenme, her zaman doğrula" sloganıyla hareket eder.

Sıfır Güven konsepti, ağ güvenliğine yönelik taze bir yaklaşım ve yeni bir çerçeve olarak, bir kuruluşun verilerine veya uygulamalarına erişmeden önce tüm kullanıcıların kimlik doğrulamasını sağlar.

Sıfır Güven, ağ içindeki kullanıcıların diğerlerinden daha güvenilir olduğunu varsaymaz. Tüm kullanıcılara yönelik gerçekleştirilen sıkı inceleme, kuruluş için daha fazla güvenlik anlamına gelmektedir.

Siber güvenlik uzmanları, uzaktaki çalışanlarla ve fidye yazılımı tehditleri gibi zorluklarla daha güvenli bir şekilde başa çıkmak için Sıfır Güven'i kullanabilir. Sıfır Güven çerçevesi, çok faktörlü kimlik doğrulama, veri şifreleme ve uç nokta güvenliği dâhil olmak üzere çeşitli araçları birleştirebilir.

Biyometrik ve Çok Faktörlü Kimlik Doğrulama (Biometrics and Multi-Factor Authentication - MFA)

Parmak izi, retina tarama, yüz tanıma gibi biyometrik özellikler için etkin yöntemlerden en önde gelenidir. Ancak, mahremiyet kaygıları, maliyetten kaçınma ve/veya kullanılan donanımların verimsiz çalışması gibi gerekçelerle kullanımı ve yaygınlığı sınırlı kalmıştır. Altyapı iyileştirmeleri ve maliyetlerin azalmasıyla özellikle kritik sistemlerde kullanılmasında yarar bulunmaktadır. Diğer bir alternatif olarak parola kullanımının diğer bazı yöntemlerle (SMS, token, akıllı kart vb.) tamamlanması ikili hatta üçlü çapraz doğrulama yapılması (MFA) hassas bilgilerin etrafında aşılmaz bir kale oluşturabilir.

Aldatma Teknolojileri (Deception Technologies)

Siber güvenlik bir satranç maçı gibidir ve aldatma teknik ve araçlarının kullanımı bu alanda bir ustalık düzeyine işaret etmektedir. Kurum ve kuruluşlar, saldırganları yanıltacak sahte cezbedici varlıklar (*Bal küpü*) oluşturarak yetkisiz erişimleri proaktif bir şekilde saptayarak saldırganın daha fazla ilerlemesini engelleyebilir.

Veriye Dayalı Siber Tehdit Tahmini

Mevcut ve geçmiş olay verilerinin analizi yoluyla gelecekteki siber tehditleri tahmin etmeye yönelik bir yaklaşımdır. Bu yöntem, büyük miktarda veriyi işleyerek, siber tehditlerin ortaya çıkma olasılığını ve potansiyel etkilerini belirlemeye çalışır.

Veriye dayalı siber tehdit tahmini, bilgisayar korsanlarının ve kötü amaçlı yazılımların yayılma eğilimlerini, saldırı vektörlerini ve hedefleri belirlemek için makine öğrenimi, yapay zekâ ve veri analitiği gibi teknikleri insan akli ve sezgisiyle birleştirmeye dayanır. Bu sayede, organizasyonlar gelecekteki siber tehditlere daha etkili bir şekilde hazırlanabilir ve savunma stratejilerini geliştirebilirler.

Siber Güvenlik Örgüsü (Cyber Security Mesh - CSM)³⁵

Gartner tarafından ortaya atılan ve modern siber güvenlik yaklaşımlarını tanımlayan bir konsepttir. Bu yaklaşım, giderek dağıtık hâle gelen dijital varlıkların ve kullanıcıların güvenliğini sağlamak için esnek, modüler ve uyarlanabilir bir güvenlik yapısı sunmayı hedefler.

Siber Güvenlik Örgüsü (CSM), geleneksel güvenlik sınırlarının ötesine geçen bir güvenlik mimarisi modelidir. Geleneksel güvenlik yaklaşımları, merkezi bir güvenlik duvarı veya ağ sınırı etrafında güvenlik sağlamayı hedeflerken, siber güvenlik ağı yaklaşımı, dijital varlıkların (veriler, kullanıcılar, cihazlar ve uygulamalar) farklı konumlarda ve bulut ortamlarında dağılmış olduğu bir dünyada güvenliğini artırmayı amaçlar. CSM, bu dijital varlıkların her birini, merkezi bir yönetim altında güvence altına alacak şekilde, bir "güvenlik ağı" olarak düşünür.

Gartner, Cyber Security Mesh yaklaşımını, organizasyonların giderek daha dağınık hâle gelen ve bulut tabanlı çalışan ortamlarında güvenliğini daha etkili bir şekilde yönetmek için bir yol olarak tanımlamaktadır. Gartner'a göre, 2024 yılına kadar, siber güvenlik ağı mimarisini benimseyen kuruluşlar, güvenlik ihlallerinin maliyetini %90'a kadar azaltabilecektir. Bu nedenle,

³⁵ Gartner, Cyber Security Mesh. <https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh>

CSM, dijital dönüşüm sürecinde, özellikle uzaktan çalışma ve bulut bilişim kullanımının arttığı bir ortamda, modern siber güvenlik stratejilerinin kritik bir unsuru olarak öne çıkmaktadır.

2.6. Ulusal Siber Güvenlik Yönetişimi

Aşağıda bazı ülkelerdeki siber güvenlik yönetim yapıları incelenerek, konunun çerçevesi oluşturulmuştur. Bu kısımda amaç, incelenen ülkelerin ulusal sistemlerini tüm detaylarıyla öğrenmekten ziyade, çalışmanın ilerleyen bölümlerinde istifade etmek üzere, yapıların ülkemize benzeyen ve benzemeyen taraflarını ortaya koyarak fazlalık ve/veya eksikliklere dikkat çekmek ve olabildiğince doğru istikamette ilerlemektir.

İncelenen ülkelere ilişkin kavram ve kurumlar, sunumda anlaşılabilirliği kolaylaştırmak adına ihtiyaç durumunda sadeleştirilmiş, ülkemizde benzer yapılar varsa yakın anlamlarıyla tarife gidilmiştir.

ABD

ABD'de siber güvenlik yönetişimi federal ve eyalet düzeyinde bir dizi kurum, kuruluş ve inisiyatifin dâhil olduğu karmaşık bir yapıya sahiptir.

Bunlardan başlıcaları; İç Güvenlik Bakanlığı (DHS) bünyesinde bulunan Siber Güvenlik ve Altyapı Güvenliği Kurumu (CISA), Savunma Bakanlığı (DoD), Adalet Bakanlığı (DoJ), Ticaret Bakanlığı (DoC), Enerji Bakanlığı (DoE), Ulusal Güvenlik Ajansı (NSA), Federal Soruşturma Bürosu (FBI), Gizli Servis (USSS), Ulusal Standartlar Enstitüsü (NIST), Ulusal Siber Direktör Ofisi (ONCD), Millî Güvenlik Kurulu (NSC), Sektörel Risk Yönetim Kurumları (SRMAs), Sektör Odaklı Bilgi Paylaşım ve Analiz Merkezleri (ISACs), Müşterek Siber Savunma İş Birliği Merkezi (JCDC), Ulusal Siber Soruşturmalar Müşterek Görev Gücü (NCIJTF), Siber Tehdit İstihbaratı Birleştirme Merkezi (CTIIC) ve Siber Emniyet Gözden Geçirme Kurulu (CSRB) olarak sıralanabilir³⁶.

³⁶ Piret Pernik et al., US National Cybersecurity Strategy (2023), The White House.

Her biri değişik misyon ve işleve sahip söz konusu aktörlere ilave olarak; bilgi üretimi, paylaşımı ve iş birliğini artırmaya yönelik burada sıralı olmayan devlet destekli araştırma merkezleri ve STK'ları da içeren önemli sayıda platform ve girişim de ayrıca bulunmaktadır³⁷.

ABD İç Güvenlik Bakanlığına bağlı olarak faaliyet gösteren CISA ve NCCIC, ABD'nin siber güvenlik stratejisinin belirlenmesinde ve uygulanmasında kilit roller üstlenmektedirler. Siber olaylara müdahale konusunda koordinatör de CISA bünyesindeki US-CERT'dir³⁸.

Siber Güvenlik Bilgi Paylaşım Kanunu (CSISA), Siber Güvenlik Çerçeve Kanunu (CFA) ve Siber Güvenlik ve Altyapı Güvenliği Kurumu (CISA) Kanunu, Kritik Altyapılar İçin Siber Olay Raporlama Kanunu (CIRCIA), IoT Siber Güvenliğini Artırma Kanunu (2020, ICIA) belli başlı yasal düzenlemeler olarak göze çarpmaktadır.

Güncel ABD Siber Güvenlik Stratejisi (2023) incelendiğinde ise; kamu, özel sektör ve sivil girişimler arasındaki iş birliği ve koordinasyon konuları ile enerji ve savunma sanayi altyapısı başta olmak üzere kritik altyapıların korunması, insan kaynağı sorunu ve post-kuantuma hazırlık hususlarına büyük önem verildiği anlaşılmaktadır.

Bunun yanında, Ulusal Siber İş Gücü ve Eğitimi Stratejisi belgesi, iş gücü sağlanması ve farkındalık oluşturulmasına yönelik faaliyet alanındaki başlıca girişimleri içermekte, bu kapsamda ayrıca ABD Savunma Bakanlığı Siber İş Gücü geliştirme planı bulunmaktadır³⁹.

Eğitim ve farkındalık anlamındaki eylemler içerisinde ise; Siber Güvenlik Eğitimi Ulusal İnisiyatifi (NICE), Devlet Burs Programı (The CyberCorps), Ulusal Akademik Siber Güvenlik Mükemmeliyet Merkezleri Programı, Siber Güvenlik Eğitim ve Onaylı Çıraklık programları sayılabilir.

Uluslararası iş birlikleri ve ortaklıklar kapsamında çok fazla oluşumun içerisinde yer alan ABD, 30 ülkenin katıldığı Karşı Fidyeye (CRI) isimli uluslararası inisiyatifin de parçasıdır.

ÇİN⁴⁰

³⁷ National Cyber Security Organisation: United States, CCD CoE, 2016.

³⁸ CISA, Cybersecurity Governance, <https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance>

³⁹ ABD Savunma Bakanlığı, Siber İşgücü Geliştirme Strateji ve Uygulama Planı. <https://dodcio.defense.gov/Cyber-Workforce/CWS/>

⁴⁰ Mik Raud, China and Cyber: Attitudes, Strategies, Organisation, NATO CCD CoE, 2016

Çin siber güvenlik yönetiřimi, hükümetin ve askerî kurumların bir karışımından oluşmaktadır. Ülkenin siber güvenlik politikaları ve stratejileri, hükümete bağı çeřitli araştırma merkezleri, üniversiteler ve askerî kurumlar tarafından geliştirilmektedir. Özellikle, devlet başkanınca, Merkezi İnternet Güvenliğı ve Bilgi Yönetimini Yönlendirme Küçük Grubu'nun oluşturulması, ülkenin siber stratejisine kişisel bir sorumluluk atfetmesi yönüyle dikkat çekmektedir.

Askerî açıdan, Çin Halk Kurtuluş Ordusu'nun siber casusluk ve istihbarat birimleri, Genelkurmay Başkanlığı'nın 3. ve 4. departmanları altında faaliyet göstermekteyken yakın zamanda oluşturulan Stratejik Destek Kuvveti altında yeniden yapılandırılması beklenmektedir. Ayrıca, ülkenin siber güvenlik politikalarının geliştirilmesi için askerî bilim akademileri ve üniversiteler de önemli bir rol oynamaktadır.

Çin'de siber güvenlik politikalarının oluşturulması ve uygulanması, devlet konseyi ve merkezi askerî komisyon gibi en üst düzey karar vericiler tarafından gerçekleştirilmektedir. Politika oluşturma sürecinde devlet konseyi genellikle yeni girişimleri benimsemekte ve uygulamaktadır. Ancak, politikaların uygulanmasından birçok hükümet kurumu sorumludur.

Sonuç olarak, Çin'in siber güvenlik yönetiřimi, hükümet kurumları, askerî birimler ve araştırma kurumları arasında bir karışımı içermekte ve liderlik merkezli bir yaklaşımla yönlendirilmektedir.

ALMANYA

Almanya, siber güvenlik alanında oldukça gelişmiş bir yapıya sahiptir ve önemli adımlar atmaktadır. Siber güvenlik yönetiřimi hem devlet hem de özel sektörün aktif katılımıyla oluşturulan geniş bir ağdan meydana gelmektedir. Bu yapıyı oluşturan bazı ana unsurlara dair bilgi aşağıda sunulmuştur.

Siber Güvenlik Stratejisi, ilk olarak 2011 yılında yayınlanmış, 2016 ve 2021 yıllarında güncellenmiştir. 2021'de yayınlanan stratejide temel hedefler; siber güvenliğı herkes için ortak bir görev hâline getirmek, dijital egemenliğı güçlendirmek, dijital dönüşümü güvenli şekilde sağlamak, hedefleri ölçülebilir ve şeffaf hâle getirmek olarak sıralanmıştır.

Bu hedeflere ulaşmak için gerekli eylem alanları ise; toplumu harekete geçirmek, kamu-özel sektör iş birliği, sürdürülebilir bir siber güvenlik mimarisi ve AB ile NATO başta olmak üzere uluslararası inisiyatiflerde güçlü konumlanmak ana başlıkları altında detaylandırılmıştır⁴¹.

Federal Bilgi Teknolojilerinde Güvenliğin Güçlendirilmesi ya da kısaca BSI Yasası⁴² olarak bilinen ve 2009'da yürürlüğe giren kanun, ülkedeki siber güvenlik çalışmalarına temel teşkil etmektedir. Bu yasa haricinde konuyla ilgili diğer mevzuat; Bilgi Güvenliği Kanunu (BSIG, 2015), Telekomünikasyon Yasası (TKG, 2004), Veri Koruma Yasası (BDSG, 2018), Kritik Altyapıların Korunması Hakkında Kanun (*KRITIS - Gesetz*, 2015) olarak sıralanabilir. Ayrıca Avrupa Birliği NIS Direktifi serisi ile Genel Veri Koruma Yönetmeliği (GDPR) Almanya'nın bu alandaki hukuki düzenlemelerine etki etmektedir.

Almanya'da siber olay yönetimi, genellikle çeşitli kurumlar ve paydaşlar arasında koordineli bir şekilde gerçekleştirilmektedir. Özellikle siber olayların türüne ve etkilerine bağlı olarak farklı kurumlar devreye girebilmektedir. Bu kapsamda rol oynayan bazı önemli kurumlar; Bilgi Güvenliği Ofisi (BSI), Asayiş Polisi (BKA), Bölgesel Emniyet Teşkilatları (LKA), İçişleri Bakanlığı (BMI), Savunma Bakanlığı (BMVg) olarak sıralanabilir. Bunlara ek olarak özellikle kritik altyapı sahibi şirketler ve telekomünikasyon sağlayıcıları gibi özel sektör kuruluşları da kendi siber güvenlik ekipleriyle siber olaylara müdahale etmektedirler.

Bu kapsamda en bilinen inisiyatif Savunma Bakanlığı tarafından 2016'da başlatılan ve 2021'de tam harekât kabiliyetine ulaşan Siber ve Bilgi Etki Alanı Servisi (Siber Komando Komutanlığı) adıyla anılan projedir. Çoğunluğu hâlihazırda görevli sivil ve askerî 11.600 kişilik personelden oluşan ve merkezi Bonn'da bulunan bu yapı, siber alandaki tehditleri ele almak ve Alman askerî operasyonlarına katılmak amacıyla görev yapmaktadır⁴³.

Kritik Altyapılara yönelik olarak ise bir Koruma Planı yayınlanmış ve bunun için özel bir program olan "*Kritische Infrastrukturen*" girişimi başlatılmıştır. Bu program, enerji, su, iletişim, sağlık gibi kritik sektörlerdeki kuruluşların siber tehditlere karşı korunmasını sağlamaktadır.

⁴¹ Veri Güvenliği, Almanya İçişleri Bakanlığı, <https://www.bmi.bund.de>

⁴² Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes, 14 August 2009

⁴³ Siber Güvenlik Teşkilatı, Almanya, <https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum>

Almanya'da siber güvenlik alanındaki kamu-özel iş birliği kapsamında önemli inisiyatifler bulunmaktadır. Bunlardan biri, strateji kapsamında oluşturulan Siber Güvenlik İttifakı (*Allianz für Cyber-Sicherheit*, AfCS) adlı girişimdir. Bu girişim, Bilgi Güvenliği Ofisi (BSI) ve Almanya'nın dijital birliği (BITKOM) tarafından başlatılmıştır. AfCS, kamu ve özel sektör temsilcilerinin bir araya gelerek siber güvenlik konusunda iş birliği yapmasını sağlamaktadır. Bu girişim, siber güvenlik bilincinin artırılmasına ve şirketlerin siber güvenliği desteklemesine olanak tanımaktadır.

Siber güvenlik alanında birçok üniversite, araştırma enstitüsü ve teknoloji firması bulunmaktadır. Bu kurumlar, siber güvenlik üzerine araştırmalar yapmakta, yeni teknolojiler geliştirmekte ve uzmanlar yetiştirmektedirler. Araştırma, geliştirme ve inovasyon alanında en dikkat çekici girişim Siber Ajans'tır. Siber güvenlik alanında araştırmalar ile çığır açan yenilikler ve iç ve dış güvenlik alanındaki ilgili kritik teknolojileri geliştirmek maksadıyla içişleri ve savunma bakanlıkları tarafından ortaklaşa olarak 2020 yılında kurulan ve savunma ve güvenlik politikalarına odaklanan Siber Ajans (*Cyberagentur*) bu alanda devlet destekleri sunmaktadır.

Almanya'daki siber güvenlik yönetişimi, devletin liderliğinde birçok paydaşın katılımını içeren kapsamlı bir yapıya dayanmaktadır. Değişen tehditler ve teknolojik gelişmeler doğrultusunda bu yapı sürekli olarak güncellenmekte ve gözden geçirilmektedir⁴⁴.

FRANSA⁴⁵

Fransa, 2008'den bu yana siber tehditleri ciddiye almaktadır ve 2011 yılında bir siber güvenlik stratejisi oluşturmuştur. Ülke, siber güvenlik politikalarını koordine etmek ve uygulamak için 2009 yılında Ulusal Ağ ve Bilgi Güvenliği Ajansı (ANSSI) isimli ulusal bir kurum oluşturmuştur. ANSSI, Fransız hükümetinin siber güvenlik politikalarını koordine etmek ve uygulamakla görevlidir. ANSSI'nin bütçesi ve personel sayısı zamanla artırılmıştır. 2013 yılında kabul edilen Askerî Planlama Kanunu da kritik altyapı işletmecilerine siber güvenlik standartlarına uyma yükümlülüğü getirmektedir.

Fransa'nın ulusal savunma sistemi, ülkenin siber saldırılara ve siber tehditlere karşı hazırlıklı olmasını sağlamayı hedefleyen *Piranet* adlı bir planla donatılmaktadır. 2012 yılında

⁴⁴ Sebastian Cymutta, National Cybersecurity Organisation: Germany, NATO CCD CoE, 2020

⁴⁵ Pascal Brangetto, National Cybersecurity Organisation: France, NATO CCD CoE, 2015

ayrıca, Fransız ordusunun siber vatandaş rezervi olan (Réserve Citoyenne Cyberdéfense) RCC'nin oluşturulması için bir girişim başlatılmıştır. Söz konusu girişim ilk etapta 50 kişiden oluşmaktadır. Bilahare operasyonel yönünün güçlendirilmesi ve sayının artırılması hedeflenmektedir.

Fransa'nın bilgi ve iletişim teknolojilerine dayalı ekonomisi, ulusal siber güvenlik stratejisi ve siber tehditlere karşı alınan önlemlerle güçlü bir konumda bulunmaktadır. Bu önlemler, Fransa'nın siber güvenlik alanındaki çabalarını artırmayı ve ulusal savunma sistemini güçlendirmeyi amaçlamaktadır⁴⁶.

Fransa, 2008 ve 2013 yıllarında iki ayrı Ulusal Savunma ve Güvenlik Beyaz Kitabı yayınlamıştır. Bu belgeler, siber tehditleri ciddi bir tehdit olarak tanımlamış ve bu tehditlerle başa çıkmak için çeşitli eylem planları önermiştir.

2011 yılında, Fransa'nın ilk siber savunma strateji belgesi yayınlanmış, sonraki yıllarda güncellenen ve 2015'te Ulusal Dijital Güvenlik Stratejisi adını alan belgede genel olarak dört ana hedef belirlenmiştir. Bunlar; dünya çapında bir siber savunma gücü olmak, Fransa'nın egemenliği ile ilgili bilgilerin korunması yoluyla karar alma yeteneğini güvence altına almak, kritik ulusal altyapıların siber güvenliğini güçlendirmek ve uluslararası iş birliğini geliştirmek olarak sıralanmaktadır⁴⁷.

Fransa, NATO'nun siber savunma faaliyetlerine aktif olarak katılmaktadır. 2011 yılında NATO Siber Savunma Yönetim Kurulu (CDMB) ile ANSSI arasında imzalanan bir Mutabakat Muhtırası bulunmaktadır.

İNGİLTERE

İngiltere'de siber güvenlik yönetişimi, bir dizi yasal düzenleme, kamu politikaları ve özel sektör girişimleriyle desteklenen kapsamlı bir çerçeveden oluşmaktadır. Yönetişimde ana aktörler, hükümetin yanı sıra özel sektör ve akademik ortaklardır.

Devlet Muhabere Ana Karargâhı (GCHQ) gibi istihbarat kurumları ve Millî Güvenlik Kurulu gibi organizasyonlar aracılığıyla siber güvenlik stratejilerini belirlemekte ve uygulamaktadır.

⁴⁶ Siber Güvenlik Stratejisi, Fransa, <https://cyber.gouv.fr/en/french-approach-cyber-0>

⁴⁷ French National Digital Security Strategy, 2015

Ayrıca, özel sektör ve akademik ortaklar, siber güvenlik konusunda bilinçlendirme çalışmaları yapmak, mükemmelliği sürdürmek ve siber güvenlik ittifakları oluşturmak gibi konularda hükümetle iş birliği hâlinindedir. Özellikle, özel sektör siber güvenlikte önemli roller üstlenmekte, kritik altyapıyı finanse etmek ve belirli önlemleri hayata geçirmek konusunda sorumluluk almaktadır. Dolayısıyla, siber güvenlik yönetiminde hükümet, özel sektör ve akademik ortaklar önemli roller üstlenmektedir⁴⁸.

2022 yılında yayınlanan ve 2030'a kadarki dönemi kapsayan Siber Güvenlik Strateji Belgesi'nde; siber ekosistemin güçlendirilmesi, siber dayanıklı ve zengin bir dijital yapının inşası, siber güç olmak için gerekli hayati teknolojilere liderlik etme, İngiltere'nin küresel etki ve liderliğinin ilerletilmesi ve düşmanları tespit, bozma ve caydırma ana konuları bulunmaktadır.⁴⁹ Stratejide belirlenen hedeflere ulaşmak için yapılan işler ve geline nokta yıllık değerlendirme raporları şeklinde kamuoyu ile şeffaf bir şekilde paylaşılmaktadır⁵⁰.

Siber güvenlikle ilgili olarak İngiltere'de ana otorite, Ulusal Siber Güvenlik Merkezi (NCSC)'dir. NCSC, siber tehditleri izlemekte, önlemler geliştirmekte, siber olaylara müdahalede bulunmakta, kamu ve siber güvenlik konusunda özel sektöre rehberlik etmektedir.

İngiltere'de siber güvenlikle ilgili yasa ve düzenlemeler arasında; Siber Suçlar Kanunu (*Computer Misuse Act*), Veri Koruma Kanunu (*Data Protection Act*) ve Haberleşme Kanunu bulunmakta, ayrıca Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) ve NIS Direktifine (*Network and Information Security Directive*) uyumluluk aranmaktadır.

Siber güvenlik, kamu ve özel sektörün iş birliği içinde çalışmasını teşvik eden ortaklıklarla desteklenmektedir. Özellikle, İngiltere'deki kritik altyapı sağlayıcılarıyla iş birliği içinde, siber güvenliği artırmak için çeşitli programlar ve girişimler bulunmaktadır.

Eğitim ve Farkındalık Programları kapsamında, siber güvenlik bilinci oluşturmak için çeşitli eğitim ve farkındalık programları mevcuttur. Bu programlar, birey ve kuruluşların siber tehditlere karşı nasıl korunacaklarını öğrenmelerine yardımcı olmaktadır.

⁴⁸ Anna-Maria Osula, National Cybersecurity Organisation: United Kingdom, NATO CCD CoE, 2015

⁴⁹ UK National Cyber Strategy 2022

⁵⁰ National Cyber Strategy 2022 Annual Progress Report 2022-2023

İngiltere'de siber güvenlik standartları ve sertifikasyonları, endüstri standartlarının benimsenmesi ve en iyi uygulamaların denetlenmesi gibi konuları içermektedir. Örneğin, "*Siber Güvenlik için 10 Adım*" gibi belgeler, bu alandaki standartların benimsenmesini teşvik etmekte ve örnek uygulamalara göre denetimlerin yapılmasını sağlamaktadır.

Ayrıca, Siber Güvenlik Bilgi Paylaşım Ortaklığı (*Cyber Security Information Sharing Partnership*, CISP) gibi girişimler, siber güvenlik bilgilerinin paylaşılmasını teşvik etmektedir. ISO/IEC 27001, Siber Güvenliğin Temelleri (*Cyber Essentials*), KOBİ'ler için Bilgi Güvencesi Belgesi IASME (*Information Assurance for Small and Medium Enterprises*) ve NIST Çerçevesi (ABD) sektörde kullanılan belli başlı standartlardır.

Bu belgeler ve inisiyatifler, özel sektörün siber güvenlik konusunda bilinçlenmesini ve siber tehditlere karşı daha dirençli olmasını sağlamak amacıyla hükümet tarafından desteklenmektedir. Ayrıca, siber güvenlikle ilgili endüstri standartları ve sertifikasyonlar, siber güvenlik sektörünün büyümesini teşvik etmekte ve siber güvenlik sektöründe faaliyet gösteren kuruluşların belirli normlara uygunluğunu göstermelerine yardımcı olmaktadır.

Bu unsurlar, İngiltere'deki siber güvenlik yönetişiminin temel bileşenlerini oluşturmakta ve siber tehditlere karşı etkili bir mücadele ve siber güvenliği güçlendirmek için sürekli olarak güncellenmekte ve geliştirilmektedir⁵¹.

JAPONYA⁵²

Japonya siber güvenlik yönetişimi, Ulusal Olay Hazırlık ve Siber Güvenlik Strateji Merkezi (NISC) konuyla ilgili ana otorite olmak üzere, kamu ve özel sektörden çok çeşitli kurumların dâhil olduğu eski ve köklü bir yapı olarak görülmektedir. Bu anlamda Japonya, 1990'lerden bugüne, siber güvenlik konusunda ulusal düzeyde strateji ve mekanizmalar geliştirmiştir.

Konuya ilişkin olarak en temel yasal düzenleme, 2014'te yayınlanan Siber Güvenlik Temel Kanunu'dur. Kanun, orta ve uzun vadede yönetim yapısı ve yönlendirici hususları içermektedir. NISC'in kuruluş, görev ve sorumluluklarına altyapı teşkil eden söz konusu yasa, teşkilat ve görevlerdeki zamanla gelişen dönüşüm ihtiyaçları doğrultusunda 2016 ve 2018 yıllarında

⁵¹ Cyber Security Governance, <https://www.ncsc.gov.uk/collection/risk-management/cyber-security-governance>

⁵² Hidetoshi OGAWA et al., Cybersecurity Governance in Japan, 2021

güncellenmiştir. Söz konusu yasayı tamamlayıcı nitelikteki devlet belgelerinden biri olarak Ulusal Savunma Programının 2018 yılında duyurulan sürümünde, Japonya’da ilk defa savunma odaklı yaklaşımdan uzaklaşılarak acil durumlarda saldırı yeteneği kazanılması hususu dikkat çekici bir gelişme olarak yer almıştır.

Japonya’da siber güvenlik alanında ilk strateji belgesi 2010 yılında ‘Ülkenin Korunması için Bilgi Güvenliği Stratejisi’ ismiyle yayınlanmış, bilahare olayın sadece teknik bir konu olmadığı ve daha geniş perspektiften yaklaşılması gerektiği anlaşıncı isim Siber Güvenlik Stratejisi olarak değiştirilmiş, 2013, 2015, 2018 ve 2021 yıllarında güncellenerek yeni sürümleri yayınlanmıştır.

İlk belgeden bugüne ‘dünyaya öncü, dinamik ve dayanıklı’ bir siber uzay oluşturma hedefine vurgu yapılmış, özellikle dayanıklılık kavramına çokça değinilmiştir. Yürürlükte olan güncel strateji belgesinde; siber tehditlerle mücadele etmek, kritik altyapıyı korumak, siber saldırılara karşı dirençli bir toplum oluşturmak ve uluslararası iş birliğini güçlendirmek gibi hedefler, ‘siber güvenlikle dijital dönüşüm’ teması ana başlığında işlenmiştir.

Yönetişimdeki ana aktörler, organizasyon yapısı ile görev ve sorumluluklar kapsamında ise sırasıyla;

Siber Güvenlik Stratejik Karargâhı (CSHQ): Temel politikaları belirleyen ve başbakanlık müsteşarının liderlik ettiği, düzenli olarak bakan seviyesinde toplanan, 2005’te kurulduğu adıyla Bilgi Güvenliği Politikaları Kurulu, 2014 sonrasında ise Siber Güvenlik Stratejik Karargâhı olarak isimlendirilen yapıdır. Kurul, 7 kamu (Müsteşar, Ulusal Kamu Güvenliği Başkanı, Polis Teşkilatı Müdürü, İçişleri ve Haberleşme Bakanı, Dışişleri Bakanı, Ekonomi, Ticaret ve Sanayi Bakanı ve Savunma Bakanı) ve 7 özel sektör/akademi temsilcisinden oluşmaktadır.

Ulusal Olay Hazırlık ve Siber Güvenlik Strateji Merkezi (NISC): Yaklaşık 200 çalışanı ile siber güvenlik politikalarının belirlenmesi yanında operasyonel görevlerde de bulunmaktadır. Kamu sistemlerinin korunması için GovCERT olarak görev yapmakta, ayrıca ulusal SOME (CSIRT) olarak JPCERT/CC (*Japan Computer Emergency Response Team/Coordination Center*) ile birlikte koordinatör makam konumunda bulunmaktadır. 2005’te Ulusal Bilgi Güvenliği Merkezi ismiyle 22 personel ile kurulmuş, 2015’ten sonra teşkilatındaki düzenleme ve

değişikliklerle bugünkü ismini almıştır. Aynı zamanda Millî Güvenlik Kurulu Sekreter Yardımcılığı görevini de yürüten Başbakanlık Müsteşar Yardımcısı tarafından yönetilmekte, Polis Teşkilatı Asayiş Büro ile de dirsek temasında çalışmaktadır. 2020 mali yılı için 102 milyar JPY (yaklaşık 750 milyon ABD doları) bütçe kullanmıştır.

Siber Suçlar Kontrol Merkezi: Suçla ve suçluyla mücadele haricinde istihbaratı da kapsayan bir görev tanımıyla, 2014'te Japon Polis Teşkilatı bünyesinde kurulmuştur. Söz konusu merkezde; özel sektör, akademi ve kolluk kuvvetleri arasında bilgi, istihbarat ve tecrübe paylaşımı yapılmaktadır.

İçişleri ve Haberleşme Bakanlığı: 2001'de iki bakanlığın birleştirilmesiyle oluşan bakanlığın, pek çok ülkedeki uygulamanın aksine kolluk veya istihbarat görev ve birimleri bulunmamaktadır. Bilgi ve Haberleşme Genel Müdürlüğü, 2017'de Bilgi Güvenliği Genel Müdürlüğüne, 2018'de ise Siber Güvenlik Genel Müdürlüğüne dönüştürülmüştür. Japon merkezi yönetimindeki bu değişim, siber güvenliğe doğrudan tahsis edilmiş en yüksek makam olarak görülen ilk olaydır.

Ekonomi, Ticaret ve Sanayi Bakanlığı: Bünyesinde bir Siber Güvenlik Birimi bulunan bakanlık, başlangıçta bilgisayar, cep telefonu gibi cihazlar kapsamında donanım ve OT güvenliğine ilişkin otorite ve onay makamı iken, zaman içerisinde görev kapsamı genişlemiş ve mevcut durumda Japonya'da tanımlı 14 kritik altyapıdan 5'inin (elektrik, gaz, kimya, kredi kartı ve petrol) güvenliğinden sorumlu hâle gelmiştir. Buna ek olarak güncel ve önemli risk alanlarından biri olan tedarik zinciri güvenliğinden de sorumludur.

Savunma Bakanlığı: 2014 yılında bakanlık bünyesinde, görevi Savunma Bakanlığı ağ ve sistemlerini korumak olarak açıklanan ve 100 kişiden oluşan bir siber savunma birimi oluşturulmuş, 2018'de mevcudu 150'ye çıkarılmıştır. Kara, deniz ve hava kuvvetlerinde siber güvenlik alanında görev yapan personel ile birlikte toplam sayının 430 civarında olduğu tahmin edilmektedir.

Kamu ile özel sektör arasındaki iş birliklerine ilişkin faaliyetlerden en önde geleni, siber olaylara müdahale konusudur. Japonya'da siber olaylara müdahale görevi çift başlı olarak yürütülmektedir. Devlet ve kritik altyapılara yönelik saldırı ve olaylarda NISC, özel sektör ve

vatandaşa yönelik olanlarda ise JPCERT/CC görevlidir. NISC'ten çok daha önce 1996'da kurulan JPCERT/CC, görevini yasal çerçevede ve devlet desteğiyle sürdürmektedir. Bu ortaklığın haricinde, 254 üyesiyle Japon Ağ Güvenliği Derneği, Japon İş Dünyası Birliği (*Keidanren*), 2002'de kurulan Bilgi ve Haberleşme Teknolojileri Bilgi Paylaşım ve Analiz Merkezi (ICT ISAC) ve bilahare bunu takip eden Finans ISAC başlıca ortak mekanizmalardır.

Uluslararası iş birlikleri ve girişimler anlamında Japonya, 2004'te kurulan BM Uluslararası Güvenlik Bağlamında Bilgi ve Haberleşme Teknolojilerinde Yaşanan Gelişmeler Uzman Grubuna 2012'den bu yana katılım sağlamakta, siber güvenlik kapsamında ayrıca, ikili, çok taraflı ve bölgesel diyalog ve inisiyatiflere genel olarak Batı perspektifinden iştirak etmektedir.

GÜNEY KORE

Güney Kore'de siber güvenlik alanındaki yönetim muhtelif yasal düzenleme ve kurumlar aracılığıyla sağlanmaktadır. Başkan ve Millî Güvenlik Kurulu (NSC), ulusal güvenlik konularında en üst düzeyde karar alma yetkisine sahiptir.

Bilim, Bilgi ve Haberleşme Teknolojileri Bakanlığı (MSIT), Bilgi Güvenliği Yönetim Sistemi sertifikası veren büyük şirketleri denetlemekten ve telekomünikasyon cihazları için gönüllü güvenlik sertifika programlarını işletmekten sorumludur.

Bunların yanı sıra, Güney Kore hükümeti özel sektörle teknik konularda güvenlik önlemleri geliştirmek ve siber tehdit bilgilerini paylaşmak için iş birliğini artırmıştır. Bu çerçevede, Güney Kore'nin siber güvenlik yönetişimini sağlama sürecinde çeşitli kurumlar aktif bir rol oynamakta, en önemli üç aktör Millî Güvenlik Kurulu, Siber Komutanlık (Savunma Bakanlığı, MND), Siber Güvenlik Merkezi (Ulusal İstihbarat Teşkilatı-NIS) ile Bilim, Bilgi ve Haberleşme Teknolojileri Bakanlığı (MSIT) olarak sıralanmaktadır⁵³.

2011 yılında Siber Güvenlik Ana Planı ile başlayan alandaki strateji dokümanları serisinin en yenisi ve günceli 2023 yılı Haziran ayında yayınlanmıştır. Söz konusu strateji belgesinde G. Kore, Kuzey Kore'nin artan siber tehditlerine karşı "önleyici" ve "saldırı" yeteneklerini güçlendirmeye odaklı bir politikaya geçiş yapma niyetini vurgulamaktadır⁵⁴.

⁵³ Evan A. Feigenbaum, *The Korean Way With Data*, Carneige Endowment for International Peace, Ağustos 2021

Güney Kore'de kamu ve özel sektör arasında siber güvenlik konusunda çeşitli iş birlikleri bulunmaktadır. Örneğin, Kore İnternet ve Güvenlik Ajansı (KISA), özel sektöre güncel güvenlik önerileri sunmakta, kişisel bilgisayarlar ve IoT cihazları için güvenlik kontrolleri sağlamakta, küçük ve orta ölçekli işletmelere danışmanlık hizmetleri vermekte, web sitesi güvenliğini artırmaya yardımcı olmakta ve özel sektörle birlikte siber tatbikatlar düzenlemektedir. Ayrıca, özel şirketlere ve akademik çevrelere yönelik siber tehdit bilgilerini paylaşarak kötü amaçlı yazılımları izlemektedir.

KISA, 2014 yılında 'Siber Tehditler Analiz Sistemi' (C-TAS) adlı otomatik tehdit bilgi paylaşım sistemini kullanmaya başlamıştır. Bu sistem aracılığıyla, özel şirketlerle ve akademik çevrelerle tehdit bilgilerini paylaşmaktadır. Ayrıca, kamu e-hizmetlerinin güvenliğini sağlama konusunda ve Kişisel Bilgi Koruma Komisyonu'na (PIPC) ilgili yasada belirtilen faaliyetler kapsamında teknik yardım sağlamaktadır.

G. Kore'de siber olaylara müdahale yetki ve sorumluluğu, yukarıda sıralı ana aktörler tarafından yürütülmektedir. NSC, ulusal güvenlik ile ilgili krizleri yönetmek ve siber güvenlikle ilgili önlemler almakla sorumludur. NIS ise, ulusal siber güvenlik bilgilerinin toplanması, analizi ve derlenmesi konusunda görevlidir ve hükümetin ve kamu sektörünün güvenliğini sağlamakla yükümlüdür. Bakanlıklar, kendi sektörlerinde güvenlik ve koruma faaliyetlerinden sorumlu olup, diğer bakanlıklar ve kurumlarla yakın iş birliği içinde çalışmaktadırlar. MND ise ulusal savunma alanında siber güvenlik önlemlerini uygulamaktadır⁵⁵.

ESTONYA

Estonya, siber güvenlik denildiğinde, 2007 yılında maruz kaldığı Rusya Federasyonu kaynaklı siber saldırılardan sonraki dönemde ilk akla gelen ülkelerden biri olmuştur. Gerek saldırılardan önceki yıllarda dijital dönüşümde dünyanın geri kalanına nazaran aldığı önemli mesafe, gerekse saldırılardan sonraki eylemleri ve NATO içerisindeki konumu bu 'küçük' ülkeyi ölçeğiyle orantısız ama hak ettiği bir noktaya taşımıştır.

⁵⁴ NK News, 02.02.2024. <https://www.nknews.org/2024/02/south-korea-unveils-new-cyber-strategy-to-counter-north-korean-threats/>

⁵⁵ Sungbaek Cho, National Cybersecurity Organisation: Republic of Korea, NATO CCD CoE, 2022,

Ülke, çevrimiçi oylama, dijital imzalar ve e-vergi iadeleri gibi çeşitli kamu e-hizmetlerini uzunca bir zamandır günlük hayata dâhil etmiş durumdadır. Estonya'nın ileri e-devlet uygulamalarıyla öne çıkması siber güvenliğe verdiği önemi de beraberinde artırmış ve 2008 yılında ulusal bir siber güvenlik stratejisi benimseyen ilk örneklerden biri olmuştur⁵⁶. Bilahare 2014, 2017, 2019 ve 2022 yıllarında bilgi sistemlerinin sürekli işleyişini ve kritik bilgi altyapılarının siber tehditlere karşı korunmasını sağlama amacını taşıyan yenilenmiş bir dizi siber güvenlik stratejisi sırasıyla yürürlüğe girmiştir.

2011 yılına kadar Savunma Bakanlığı tarafından yürütülen siber güvenliğin genel siyasi sorumluluğu daha sonra Ekonomi İşleri ve İletişim Bakanlığı'na devredilmiştir. Kurumlar arası siber güvenliğin koordinasyonu ve stratejik hedeflere ulaşma durumu ise Siber Güvenlik Kurulu tarafından takip edilmektedir.

Estonya'da siber tehditlerin tespit edilmesi ve önlenmesi, yani siber tehdit istihbaratı konusunda sorumlu makam, '*Kaitsepolitseiamet*' (KAPO) olarak bilinen İç Güvenlik (İstihbarat) Servisi'dir. KAPO, ana aktörlerden biridir. İstihbarat ve adli soruşturmalar yoluyla ulusal ve uluslararası ortaklarla çalışmaktadır. KAPO ayrıca; siber istihbarat, aşırıılık, terörizm ve sabotaj girişimlerinden kaynaklanan siber tehditleri tespit etmek ve önlemekle görevlidir. Bu kapsamda, KAPO, siber olaylara müdahalede önemli bir rol oynamaktadır⁵⁷.

Estonya Bilgi Sistemleri Otoritesi (*Riigi Infosüsteemi Amet*, RIA), Ekonomik İşler ve Haberleşme Bakanlığı'nın altında Estonya'nın merkezi siber güvenlik merkezi olarak 2011 yılında kurulmuştur. RIA, devlet bilgi sistemlerinin geliştirilmesi ve idaresinden, ayrıca ilgili politika ve stratejilerin hazırlanmasından, güvenlik standartlarının uygulanmasının koordine edilmesinden, siber güvenlikle ilgili faaliyetlerin organize edilmesinden ve Estonya ağlarında bildirilen veya meydana gelen güvenlik olaylarının ele alınmasından sorumludur. Devlet sistemleri ile kritik altyapıların gözetimi görevi bulunan merkezin para cezası uygulama yetkisi de bulunmaktadır.

RIA bünyesinde, Estonya Bilgisayar Acil Durum Müdahale Ekibi (CERT-EE), bilgisayar ağlarındaki güvenlik olaylarını ele almaktan, güvenlik olaylarını önlemek için uyarılarda bulunmaktan, kullanıcıların güvenlik farkındalığını artırmaktan, kamu kurumları ve özel sektör

⁵⁶ Gül Nazik ÜNVER, Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye ve İngiltere Örneği, 2023

⁵⁷ Anna-Maria Osula, National Cybersecurity Organisation: Estonia, NATO CCD CoE, 2015

arasında güvenli ve şeffaf veri alışverişi sağlayan *X-Road'u* ve devlet portalı '*esti*'yi yönetmekten sorumludur. 2013 yılından bu yana, devlet kurumları olay durumlarında yasa gereği derhal CERT-EE'ye rapor vermekle yükümlüdür.

Estonya, uluslararası alanda siber güvenlik konusunda aktif bir savunucu olmanın önemini farkında olarak; NATO, AB, Birleşmiş Milletler, Avrupa Konseyi, AGİT, ITU ve diğer uluslararası kuruluşlarda bu konudaki girişimleri teşvik eden öncü ülkelerden biri olmuştur. Ayrıca, başkent Tallinn'de NATO Müşterek Siber Savunma Mükemmeliyet Merkezi'ne ev sahipliği yapmaktadır.

RUSYA

Rusya Hükümetinin kendi takdirine bağlı olarak Küresel İnternet bağlantısını kesmesine olanak tanıyan 'Rusya'nın Egemen İnterneti' yasası Ekim 2019'da yürürlüğe girmiştir. Bu yasayla Kremlin, 2024 yılına kadar Rusya'ya ait İnternet trafiğinin yalnızca %10'unun yabancı sunucular üzerinden yönlendirilmesini hedeflemektedir. Bilgi sistemlerine yönelik bir saldırıyı Rusya'ya yönelik bir tehdit olarak algılamakta, bilgi alanı üzerindeki kontrolün gerekli olduğunu düşünmekte ve dijital egemenliği (*tsifrovoy suverenitet*) hedeflemektedir.⁵⁸

Rusya'nın siber güvenlik yönetişi, büyük oranda Federal Güvenlik Servisi (FSB)'nin merkezinde olduğu bir yapıdır. KGB'nin devamı olarak görülebilecek Rus İstihbarat Teşkilatı FSB, yine aynı kurumdan türemiş FSO'nun altında bulunan ve kripto analiz/şifreleme ile bilgi güvenliği konularından sorumlu Özel İletişim ve Bilgi Servisi ile koordineli çalışmakta, 1990'ların başlarından bu yana bağımsız hacker ve uzmanları siber operasyonlara dâhil etmek için birtakım ilişkiler geliştirerek bu alandaki insan kaynağının canlılığını muhafaza etmektedir. FSB'nin bu süreçte yürüttüğü teknolojik araştırmaları, istihbarat teşkilatı SVR ile koordineli olarak yürüttüğü ofansif siber yetenek geliştirme faaliyetlerinde önemli bir avantaj sağlamıştır. Bünyesinde bulundurduğu siber istihbarat ve siber güvenlik birim ve merkezleriyle FSB'nin, siber uzayı; elektronik, sinyal, açık kaynak ve insan istihbaratı ile birlikte bir bütün olarak gördüğü anlaşılmaktadır.

Bu bilgiler, Rusya'nın siber güvenlik yönetişimine ilişkin genel bir düşünceye sahip olunması için yeterli olsa da Rusya Federasyonu'ndaki siber güvenlik konusu sadece savunma ve

⁵⁸ Janne Hakal et al., *Russia's Strategy In Cyberspace*, NATO SC CoE, 2021

alınan tedbirler yönüyle incelendiğinde eksik kalmaktadır. Konuya ilişkin olarak, bilgi harekâtından diplomasiye, dijital egemenlikten yapay zekâya kadar uzanan başlıklarda yürürlüğe giren birtakım strateji, konsept, kanun, yönetmelik, direktif ve alt seviye rehber dokümanlar fikir vermesi açısından aşağıda sıralanmıştır⁵⁹.

Kanun, Kararname ve Diğer Düzenlemeler

- Bilgi ve Bilgi Teknolojilerinin Korunması Kanunu (2006)
- Ulusal Güvenlik Kanunu (2010)
- Kritik Bilgi Altyapısının Güvenliği Kanunu (2018)
- Kritik Bilgi Altyapısı Güvenliğinin Devlet Gözetimine İlişkin Hükümet Kararnamesi (2018)
- İnternet Egemenliği Kanunu (2019)
- Kritik Bilgi Altyapısının Çalışmasını Sağlamak İçin Telekomünikasyon Ağı Kaynaklarının Hazırlanması ve Kullanımına İlişkin Hükümet Kararnamesi (2020)
- Bilgi Güvenliğine Yönelik Tehdit Değerlendirme Yöntemleri Kılavuzu (2021)

Ulusal Güvenlik ve Savunma Stratejileri

- Rus Askerî Doktrini (2014)
- Bilgi Güvenliği Doktrini (2016)
- Dış Politika Konsepti (2016)

⁵⁹ NATO CCS CoE, Russian Federation. <https://ccdcoc.org/library/strategy-and-governance/?search=russia>

- Ulusal Güvenlik Stratejisi (2021)

Siber Güvenlik Strateji Belgeleri

- Silahlı Kuvvetler Bilgi Konsepti (2011)
- Siber Güvenlik Strateji Konsepti (2014)
- Bilgi sistem ağlarına yapılan saldırıların tespiti, engellenmesi ve sonuçlarının değerlendirilmesi konsepti (2014)
- Bilgi Güvenliği Doktrini (2016)
- Bilgi Toplumu Kalkınma Stratejisi 2017-2030 (2017)
- 2030'a Kadar Yapay Zekâ Geliştirme Stratejisi (2019)
- Uluslararası Bilgi Güvenliğine İlişkin Devlet Politikası (2021)
- Finans Sektöründe Bilgi Güvenliği Trendleri ve Gelişmeleri Stratejisi 2019-2021 (2019)

Rusya’da siber olaylara müdahale konusunda yetkili birim RU-CERT (*Russian Computer Emergency Response Team*)’dir. CERT-RU olarak da bilinen ve 2001’den bu yana FIRST üyesi olan kurum, olaylara yanıt vermek, tehditleri analiz etmek ve bilgi paylaşmak için kurulmuştur. Güncel olmadığı anlaşılan İnternet sayfasında⁶⁰ hemen hiçbir bilgi bulunmayan RU-CERT, ulusal siber güvenlik çabalarını koordine etmek ve siber tehditlere karşı etkili bir şekilde yanıt vermek amacıyla faaliyet göstermektedir.

⁶⁰ RU-CERT. <https://www.cert.ru/en/about.shtml>

Rusya, devlet ile özel sektör arasındaki iş birlikleri konusuna ise son derece cüretkâr ve girişken birtakım inisiyatifler almaktadır. Yakın zaman önce basına çıkan *Vulkan* dosyası buna örnek olarak verilebilir. Çoğunluğu asker kökenli bir grup girişimci tarafından siber güvenlik danışmanlık şirketi olarak kurulan Vulkan'dan sızan kimi belgelerde şirketin, Rus askerî istihbarat birimi GRU ile siber saldırı, siber espionaj ve otomatikleştirilmiş dezenformasyon yoluyla algı yönetimi de dâhil olmak üzere çok kapsamlı bilgi operasyonlarının içerisinde yer aldığı görülmektedir⁶¹.

İSRAİL⁶²

İsrail, siber güvenlik konusunu ulusal bir öncelik olarak belirlemiş ve alanda birçok önemli gelişme kaydetmiştir. Ülkenin yüksek siber güvenlik teknolojileri geliştirme ile geniş kapsamlı İnternet hizmetlerinin erişilebilirliği ve kullanımı konusunda iyi örnekler arasında olduğu ve öncü bir rol oynadığı görülmektedir.

Bu anlamda *Thalia* adı verilen e-devlet platformu ilk olarak 1997'de açılmış olup 2011'de oluşturulan Bilgi ve Haberleşme Teknolojileri (ICT) Otoritesinin kontrolü altında hizmet vermeye devam etmektedir. Pek çok devlet hizmetini barındıran platform içerisinde, güvenlik kurumları arası raporlama sistemi olan *Magna* ve devlet kaynak planlama yazılımı (ERP) çözümü *Merkava* da sayılabilir. 2009'da *Knesset* isimli Biyometrik Veri Tabanı Kanunu'nun çıkmasıyla, adı geçen yöntemle kimlik doğrulama seçeneği de sisteme dâhil edilmiştir.

İsrail'in İnternet teknolojileri alanındaki görece ileriden gitmesine rağmen, ulusal siber güvenlik stratejisi ve politikalarının belirlenmesinde ancak 2010 önemli bir yıl olarak göze çarpmaktadır. O yıl içerisinde, Başbakan'ın, Bilim Bakanlığı altındaki Ulusal Ar-Ge Kurulu'na Ulusal Siber İnişiyatif direktifi ile çalışmalar somut bir hâl almıştır. Askeriye, bakanlıklar, akademi ve özel sektör temsilcilerinden oluşan 80 kişilik bir grubun altı ay çalışması sonucunda ortaya koyduğu 12 öneri bilahare 2011'de 3611 sayılı Hükümet Kararı olarak yayınlanmış ve ilk siber güvenlik danışma ve koordinasyon makamı olarak Ulusal Siber Büro (INCB) kurulmuştur.

⁶¹ The Guardian. 30.03.2023. <https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics>

⁶² Deborah Housen-Couriel, National Cybersecurity Organisation: Israel, NATO CCD CoE, 2017

2016 sonrasında Siber Büro, yanına Ulusal Siber Güvenlik Otoritesi de (NCSA) eklenerek Siber Güvenlik Direktörlüğü (Ma'arach) altında birleştirilmiştir. NCSA, reaksiyonel ve ofansif kabiliyetler de dâhil olmak üzere siber olaylara ilişkin her türlü müdahale, siber istihbarat edinim ve analizini güvenlik güçleriyle yakın çalışma içerisinde yerine getirmekle görevlendirilmiştir.

İsrail Siber Olaylarına Müdahale Ekibi (SOME/CERT-IL) de NCSA bünyesinde görev yapmaktadır. CERT-IL, kamu ve özel sektör için siber olaylar hakkında ülke içerisindeki ana koordinatör olmanın yanında uluslararası olay müdahaleler kapsamında da tek irtibat noktasıdır. Günümüzde İsrail'de siber güvenlikten sorumlu ana koordinatör makam Siber Güvenlik Direktörlüğü'dür.

Konuya ilişkin bir diğer önemli aktör olarak İsrail Savunma Kuvvetleri (IDF) uzun yıllardır siber tehditler ve işlerle uğraşmasına rağmen ancak 2015'te yayınlanan IDF Stratejisi ile siber güvenlik konusuna geniş yer ayırarak önceliklendirmiş ve stratejik, operatif ve taktik seviyede yetenek sahibi bir siber komutanlık teşkilatlanmasına gitme niyetini belirtmiştir.

Siber güvenlik birimleri kapsamında ayrıca bir siber suçlarla mücadele teşkilatı Ulusal Polis bünyesindeki *Lahav* elit biriminin içerisinde 2012'de kurulmuştur. Kritik altyapıların korunması ise başlangıçta Ulusal Bilgi Güvenliği Kurumu (NISA) görevliyken, zaman içinde bu görevlerin Siber Güvenlik Direktörlüğüne devredilmesi beklenmektedir.

Kritik altyapı olarak koruma altına alınan kurumlar arasında; bakanlıklar, mahkemeler, cezaevleri, Merkez Bankası ve diğer bankalar, belirlenmiş savunma sanayi kuruluşları, gaz, enerji ve su şirketleri, hastaneler, iletişim sağlayıcıları ve sosyal güvenlik kurumu bulunmaktadır.

Acil durum ve kriz yönetimi; Savunma Bakanlığı, Kamu Güvenliği Bakanlığı ve İç Güvenlik Komutanlığı (*Home Front Security*), NCSA ve NISA tarafından yürütülmekte olup ana sorumluluk Acil Durum Yönetim Otoritesindedir.

Ulusal Güvenliğe ilişkin düzenlemeler kapsamında başlıca yasa, yönetmelik, strateji, doktrin ve diğer resmî belgeler; Bilgisayar Kanunu (1995), Gizlilik Koruma Kanunu (1981) ve kanuna ilişkin düzenlemeler, Endüstriyel Araştırma ve Geliştirmeyi Teşvik Kanunu (1984), Savunma Ürünlerinin İhracatı Kontrol Kanunu (2007), Haberleşme Kanunu (1982), Kamu

Kurumlarında Güvenliğin Düzenlenmesi Kanunu (1998), Elektronik İmza Kanunu (2001) olarak sıralanmaktadır.

Siber Güvenlik alanını düzenleyen resmî dokümanlar arasında ise; B/84 sayılı Devlet Bilgisayar Ağlarının Korunması Kararı (2002), Siber Güvenlik Stratejisi (2011), *Şafran* Komitesi Raporu (2014), İsrail Savunma Kuvvetleri Stratejisi (2015), Siber Güvenlik Profesyonellerinin Nitelikleri (INCB, 2015), Siber Güvenlik Stratejisi (2017) ve Uluslararası Siber Strateji (2021) yer almaktadır.

İsrail'de yaklaşık 470 civarında siber güvenlik şirketi bulunmaktadır ve 2016 yılında sektörün küresel pazar finansmanı ve ihracatının yaklaşık 6 milyar dolar olduğu tahmin edilmektedir. Bu başarı, akademi ve hükümetle iş ilişkilerine, ayrıca daha olgun şirketlerin yeni başlayanlara (start-up) akıl hocalığı (mentorluk) yapmalarına dayanmaktadır. Örneğin, İsrail Elektrik Şirketi, 2013 yılında genç girişimcilerle ortaklık yaparak başarılı bir siber savunma eğitim ve danışmanlık firması olan CyberGym'i kurmuştur.

Ayrıca, İsrail'de çok uluslu şirketler tarafından küresel pazar için güvenlik çözümleri geliştirmek üzere yaklaşık 20 siber güvenlik Ar-Ge merkezi bulunmaktadır. Bu merkezler arasında PayPal, IBM, VMWare, General Electric, Cisco, CA Technologies, McAfee ve Ciscom gibi şirketler mevcuttur.

Siber güvenlik alanında iş birliğine iyi uygulama örneği olarak verilebilecek *CyberSpark* İnovasyon Projesi, 2014 yılında Beerşeba'da kurulmuş bir girişimdir. Proje, İsrail Millî Siber Güvenlik Otoritesi (INCB), Beerşeba Belediyesi, Ben Gurion Üniversitesi'nin öncülüğünde, EMC (RSA), Lockheed Martin, IBM, Deutsche Telekom, JVP Cyber Labs ve Elbit gibi sektör temsilcilerinin de desteğiyle müştereken hayata geçirilmiştir. Bilahare, İsrail Savunma Kuvvetleri (IDF) ve İsrail SOME (CERT-IL) de *CyberSpark* girişimine dâhil olmuştur.

CyberSpark, dünya çapında siber güvenlik personeline yönelik yürütülen seminerlerinin yanı sıra, hükümet, akademi, endüstri, yerel yönetim ve sivil toplum için çok paydaşlı bir ekosistem oluşturmuştur. Bu girişim, İsrail'in siber güvenlik alanındaki ulusal politikalarını, organizasyon yapısını ve stratejilerini desteklemektedir⁶³.

⁶³ HSD, Cyberpark. <https://securitydelta.nl/partners/overview-partners/cyberspark>

İsrail’de, 2’si dünya sıralamasında ilk 100’de olmak üzere 9 araştırma üniversitesi bulunmaktadır. INCB, 7 üniversitede siber mükemmeliyet merkezleri oluşturulması, Tel Aviv Üniversitesinde ise bir siber araştırma merkezi kurulması konusunda ilgili üniversiteler ile 2014 yılında anlaşmaya varmıştır.

Akademik alanda, İsrail’in araştırma ve geliştirme çalışmalarına verdiği öncelik, ülkeyi ICT ile ilgili patentlerde OECD ülkeleri arasında 7’nci sıraya yerleştirmiştir. Ayrıca, Dünya Ekonomik Forumu’nun 2015-2016 Küresel Rekabet Raporu’na göre, İsrail, 144 küresel ekonomi arasında inovasyon yeteneği olarak 3’üncü sırada ve teknolojik hazırlık açısından 15’inci sırada yer almaktadır. Ülke, *Next Generation İnternet*, ABD’nin *İnternet 2 Network*, AB’nin araştırma ve eğitim topluluğu için *GEANT* veri ağı, Avrupa Birliği Yedinci Çerçeve Programı (FP7) gibi küresel araştırma ve geliştirme ağlarıyla bağlantılıdır.

Bu bilgiler ışığında, İsrail’deki siber güvenlik sektörünün akademik kurumlarla ve özel sektörle olan iş birliği oldukça güçlüdür ve ülke, siber güvenlik alanında ulusal düzeyde farkındalığı artırma rolü üstlenmektedir. Bu kapsamda; ilköğretim düzeyinde *Gvahim*, ortaöğretim 10 ila 12’nci sınıf öğrencilerini kapsayan ise *Magshimim*⁶⁴ siber farkındalık programları Eğitim Bakanlığı koordinesi, IDF ve INCB’nin desteği ile sürdürülmektedir.

Uluslararası düzeyde Birleşmiş Milletler’in Hükümet Uzmanları Grubu (GGE) üyesi olarak İsrail, ayrıca, Avrupa Konseyi’nin 2001 Siber Suçlar Sözleşmesi’ne resmen katılmış ve birçok ülke ve uluslararası kuruluşlarla siber güvenliği teşvik etmek için ikili iş birlikleri kurmaktadır.

Küresel çapta siber güvenlik endekslerinde önde görünen birçok ülke kritik altyapılar, siber kriz yönetimi, siber tehdit istihbarat, siber güvenlik kapasitesinin geliştirilmesi, siber güvenlik ekosisteminin geliştirilmesi, yeni nesil teknolojilerin siber güvenliği gibi pek çok alanda hızlı bir şekilde düzenlemeler yayınlayıp devreye alabilmektedir.

Yukarıda yapılan incelemeler çerçevesinde, idari yapının merkezi olduğu ülkelerde siber güvenlik organizasyonunun da çoğunlukla merkezi bir yapıda kurgulandığı dikkat çekmektedir.

⁶⁴ Rashı Foundation, Magshimim. <https://rashı.org.il/en/programs/magshimim/>

İncelenen ülkelerin çok büyük çoğunluğunda siber güvenlik alanında merkezi bir yönetim ve eşgüdüm otoritesinin bulunduğu, Türkiye'nin bu alanda konudan müstakilen sorumlu bir makam bulunmayan örnekler arasında yer aldığı görülmektedir.

Yine bu ülkelerin birçoğunda siber güvenlik ekosisteminin geliştirilmesine yönelik çalışmalara büyük önem atfedilmekte bu maksatla kurulmuş mekanizmalar bulunmaktadır.

Dijital/Siber dayanıklılık hususu siber güvenlik başlığı altında ele alınmış olup siber saldırılardan kaynaklı afet durumları için yine ülkelerin çoğunda acil durum yönetim ekiplerinin oluşturulduğu, sorumlulukların belirlendiği ve siber kriz tatbikatlarının yapıldığı görülmektedir.

Ulusal seviyedeki siber olaylarla mücadele fonksiyonları için ülkeler “Bilgisayar Acil Müdahale Ekibi (CERT)” organizasyonları kurmuş durumdadırlar. Hatta bazı ülkelerde kamu kurumlarına özel işlemleri yürüten gov-CERT, sivil kurumlar için ayrı bir müdahale yapısı ve askerî kritik sistemler ve belirli savunma sanayi kuruluşları için bunlara özel yapılanmaların da bulunduğu görülmektedir.

Siber güvenlik alanında gerek toplumsal farkındalığın oluşturulması gerekse nitelikli insan kaynağı yetiştirilmesi konusunda ilk veya ortaöğretimden başlayarak siber güvenlik konusunun müfredata alındığı, ilerleyen dönemde ise profesyonel yetiştirilmesi kapsamında tedbirler geliştirildiği ülke örneklerine sıkça rastlanmaktadır.

BULGARİSTAN

Bulgaristan'ın siber güvenlik yapılanması, ulusal güvenlik stratejilerinin bir parçası olarak son yıllarda gelişme göstermiştir. Ülke, dijital altyapısını korumak ve siber tehditlere karşı dirençli bir yapı oluşturmak amacıyla çeşitli yasal düzenlemeler, teşkilatlanma çalışmaları ve yönetim mekanizmaları geliştirmiştir. Bu kapsamda, ülke genelinde siber güvenliğin sağlanması için devlet kurumları, özel sektör, akademi ve sivil toplum kuruluşlarının birlikte çalıştığı bir yapı oluşturulmuştur.

Büyük oranda AB çatı mevzuatı altında konuyu ele alan Bulgaristan'ın siber güvenlik alanındaki yasal çerçevesi, özellikle 2018'de kabul edilen Siber Güvenlik Kanunu⁶⁵ ile şekillenmiştir. Bu yasa, ülkenin kritik altyapılarını ve dijital varlıklarını korumak için gerekli olan

⁶⁵ Siber Güvenlik Yasası, Bulgaristan. <https://cms-lawnow.com/en/ealerts/2018/11/bulgaria-adopts-new-cyber-security-act>

tedbirleri tanımlamaktadır. Yasanın yürürlüğe girmesiyle birlikte ülke, Avrupa Birliği'nin Ağ ve Bilgi Güvenliği Direktifi'ne (NIS) uyum sağlamış ve bu alandaki yükümlülüklerini yerine getirmiştir. Yasa, kamu ve özel sektördeki tüm ilgili tarafların belirli siber güvenlik standartlarına uymalarını ve olası güvenlik ihlalleri durumunda bildirimde bulunmalarını zorunlu kılmaktadır.

Bu alanda, siber güvenlik stratejisi olarak değerlendirilebilecek ilk resmî belge ise 2016 yılında 'Siber Dayanıklı Bulgaristan 2020' ismiyle yayımlanmıştır. Belge, Bulgaristan'ın ulusal siber güvenlik alanında karşı karşıya olduğu tehdit ve zorluklara yanıt vermek ve siber dayanıklılık seviyesini artırmak amacıyla geliştirilmiş olup, ulusal güvenliğin korunması, ekonomik ve sosyal kalkınmanın desteklenmesi için bir dizi hedef ve tedbiri kapsamaktadır.

Stratejinin ana hedefleri, Bulgaristan'ın kritik iletişim ve bilgi altyapılarının korunması ve kamu kurumları, işletmeler ve vatandaşların güvenli bir dijital ortamda özgürce veri alışverişi yapabilmesinin sağlanmasıdır. Bunun yanı sıra, ulusal kapasitenin geliştirilmesi ve uluslararası iş birliklerinin artırılması da stratejik hedefler arasında yer almaktadır. Belgede 9 eylem alanı, 18 hedef ve 100 madde hâlinde yer alan konu başlıkları ve öncelikler şu şekilde özetlenebilir⁶⁶⁶⁷.

- *Ulusal Siber Güvenlik Sistemi Kurulması ve Geliştirilmesi:* Siber güvenlik politikaları, stratejileri ve planları oluşturularak ulusal siber güvenlik sisteminin kurulması ve operasyonel koordinasyonun sağlanması hedeflenmekte, ayrıca, siber kriz yönetim sistemleri geliştirilerek devlet kurumlarının rol ve sorumlulukları artırılmaktadır.
- *Ağ ve Bilgi Güvenliği:* Devlet kurumları, özel sektör ve toplum genelinde yüksek bir ağ ve bilgi güvenliği seviyesine ulaşılması için gerekli güvenlik ve dayanıklılık önlemlerinin uygulanması hedeflenmektedir. Bu alan, kritik altyapıların korunması ve dijital bağımlılığın azaltılmasına yönelik çalışmaları içermektedir.
- *Kritik Altyapıların Korunması ve Dayanıklılığı:* Dijital bağımlı kritik altyapıların korunması, devlet ile altyapı operatörleri arasındaki iş birliğinin geliştirilmesi ve altyapı yönetim sistemlerinin modernizasyonu konuları öne çıkmaktadır. Yeni tehdit alanlarına

⁶⁶ Siber Dayanıklı Bulgaristan 2020. <https://www.cyberwiser.eu/bulgaria-bg>

⁶⁷ Krasimir Simonski, Dr. George Sharkov, 29-30.11.2016, Sofya. Siber Güvenlik Stratejisi Sunumu.

karşı zamanında koruma sağlanması stratejinin önemli bir bileşeni olarak göze çarpmaktadır.

- *Bilgi Paylaşımı ve İş Birliği:* Devlet, özel sektör ve toplum arasındaki iş birliğinin artırılması, bilgi paylaşım mekanizmalarının geliştirilmesi ve tüm paydaşların siber güvenlik alanında katılımının sağlanması stratejik bir öncelik olarak görülmüştür.
- *Yasal Çerçevenin Geliştirilmesi:* Siber güvenlik alanındaki yasal ve düzenleyici çerçevenin güncellenmesi, etkin bir düzenleme ve sertifikasyon mekanizmasının oluşturulması hedeflenmektedir.

Söz konusu strateji belgesi, yukarıdaki ana konu başlıklarına ilave olarak, belirlenen hedeflerin ve tedbirlerin uygulanması için bir yol haritası ve plan da içermektedir. Bu planın, Bulgaristan hükümetinin gelişim programları ve ulusal sektör stratejileri ile uyumlu bir şekilde yürütülmesi ve elde edilen yeteneklerin, düzenli tatbikatlar, simülasyonlar ve uluslararası iş birlikleri aracılığıyla periyodik olarak test edilerek doğrulanması hedeflenmiştir.

Strateji belgesindeki 9 ana eylem alanından birisi olan siber suç konusunda ise 2005 yılından itibaren birtakım tedbirler geliştirilmiş, girişimlerde bulunulmuştur. Bu kapsamda Bulgaristan, AB Konseyi Budapeşte Sözleşmesi'ni onaylayarak⁶⁸ gereklerini kendi mevzuatına (Ceza Kanunu, Ceza Muhakemesi ve Usul Kanunu, Elektronik Haberleşme Kanunu, Elektronik Belge ve E-İmza Kanunu, E-Ticaret Yasası vb.) ithal etmiştir.

Ceza Hukuku kapsamında ele alınan siber suçlar; bilgisayar sistemine hukuka aykırı erişim, yasadışı dinleme, veri kesintisi, sistemlere yetkisiz müdahale, cihazın kötüye kullanımı, bilgisayar yoluyla sahtecilik ve dolandırıcılık, çocuk pornografisi ve telif haklarıyla ilgili konular olarak sıralanmaktadır⁶⁹.

Söz konusu strateji belgesinin gösterdiği istikamette gerçekleştirilen teşkilat kapsamında, siber güvenlik konusundaki koordinasyon ve uygulama sorumluluğu, Devlet E-Hükûmet Ajansı (State e-Government Agency - SEGA) tarafından yürütülmektedir. SEGA, ulusal siber güvenlik

⁶⁸ Budapeşte Konvansiyonu Taraf Ülkeler. <https://www.coe.int/en/web/cybercrime/parties-observers>

⁶⁹ Octopus Siber Suç Topluluğu, AB Konseyi, Bulgaristan hk. <https://www.coe.int/en/web/octopus/-/bulgaria>

politikasının geliştirilmesi, uygulanması ve denetlenmesinden sorumlu ana kurumdur⁷⁰. Bu kurum aynı zamanda, kritik altyapıların korunması için gerekli standartları belirlemekte ve ulusal siber güvenlik olay müdahale ekibine (CERT-BG) ev sahipliği yapmaktadır. CERT-BG, Bulgaristan'ın dijital altyapılarına yönelik tehditleri izlemekte ve siber olaylara müdahale etmektedir⁷¹.

Siber suçlara ilişkin olarak ise İçişleri Bakanlığı bünyesindeki Organize Suçlarla Mücadele Genel Müdürlüğü - Siber Suç Birimi 7/24 ulusal irtibat noktası olarak görev yapmaktadır.⁷² Konuya dair öne çıkan diğer bir kurum, telekomünikasyon, posta hizmetleri, elektronik belge ve elektronik imza alanında düzenleyici işlevlere sahip ve değişik isimlerle 1998'den beri faaliyette bulunan bir organ olan İletişim Düzenleme Komisyonu'dur⁷⁴. Kişisel Verileri Koruma Komisyonu da bu kapsamda göze çarpan bir aktör olarak sıralanabilir⁷⁵.

Ülke, siber güvenliğin sağlanması konusunda Avrupa Birliği ve NATO ile uyum içinde bulunmakta, siber güvenlik strateji belgesi de Bulgaristan'ın uluslararası güvenlik normları ve uygulamalarıyla uyumlu hareket etmesi ve bölgesel iş birliğini güçlendirmesine işaret etmektedir.

⁷⁰ SEGA, Bulgaristan. <https://e-gov.bg/wps/portal/agency-en/about-us>

⁷¹ CERT Bulgaristan. <https://www.govcert.bg/en/>

⁷² Organize Suçlarla Mücadele Genel Müdürlüğü, Bulgaristan. www.gdbop.bg

⁷³ Siber Suçlarla Mücadele Birimi, Bulgaristan. www.cybercrime.bg

⁷⁴ İletişim Düzenleme Komisyonu, Bulgaristan. <https://www.crc.bg/index.php/bg/rubriki/742/istoriq-na-krs>

⁷⁵ Kişisel Verileri Koruma Komisyonu, Bulgaristan. www.cdpd.bg/en

3. Türkiye’deki Gelişmeler, Eğilimler ve Beklentiler

Dijital egemenliğe ulaşma yolunda, mevcut durumda ülkemizde bugüne kadar önemli ve hatırı sayılır çalışma ve girişimlere imza atılmıştır. Bunlardan ilk akla gelenleri ulusal siber güvenlik stratejileri ve eylem planları, siber güvenlikte yerli ve millî çözümler, dijital okuryazarlık projeleri, kamu altyapılarının güçlendirilmesi ve diğer yaygın eğitim ve bilinçlendirme faaliyetleri olarak sıralanabilir.

Buna rağmen hâlen gidilmesi gereken yol ve alınması gereken bir hayli mesafe bulunduğu görülmektedir. Dijital dünyanın canlı ve dinamik doğası, sürekli takip ve güncel kalmayı gerektirir de esasında peşinden koşanı değil onu tutup sürükleyeni ödüllendirmektedir.

Bu kapsamda; egemen ve bağımsız bir ülke olma ilkesini kurulduğu günden bu yana koruyan ve gözetilen ülkemiz, bu alanda da egemen olmayı hedeflemektedir. Anılan çerçevede yakın geçmişte konuya ilişkin yürütülen çalışmalar aşağıdaki konu başlıklarında sunulmuştur.

3.1. Güvenli Dijital Teknolojilerin Geliştirilmesi ve Sürdürülebilirliği

Dijital Türkiye, devlet hizmetlerinin vatandaşlara sunulmasında geleneksel bürokratik süreçlerden daha verimli, kullanıcı odaklı elektronik platformlara geçişte bir paradigma değişimini temsil etmektedir. Bu girişim, vatandaşlar ve kamu kurumları arasındaki etkileşimi kolaylaştırmak için Bilgi ve İletişim Teknolojilerinden (BİT) yararlanarak devlet hizmetlerini erişilebilir, verimli ve güvenli bir şekilde sağlamayı amaçlamaktadır.

Dijital Türkiye'nin temel özellikleri ve hedefleri şunlardır:

- *Erişilebilirlik:* Devlet hizmetlerinin, konumları veya fiziksel hareketlilikleri ne olursa olsun, elektronik platformlar aracılığıyla tüm vatandaşların erişimine açık hâle getirilmesi.
- *Verimlilik:* Bürokratik engelleri azaltarak ve süreçleri otomatikleştirerek hizmet sunumunun verimliliğini artırmak, vatandaşlar için daha hızlı geri dönüş süreleri sağlamak.

- *Kalite:* Devlet tarafından sağlanan dijital hizmetlerin yüksek kalite, güvenilirlik ve doğruluk standartlarını karşılamasını sağlamak.
- *Hız:* Hizmetlerin dijital kanallar aracılığıyla sunulmasını hızlandırmak, gecikmeleri en aza indirmek ve genel hizmet yanıt verme hızını artırmak.
- *Kesintisiz Hizmet:* Vatandaşların ihtiyaçlarının tutarlı bir şekilde karşılanmasını sağlamak için minimum kesinti ile devlet hizmetlerine sürekli erişimin garanti edilmesi.
- *Emniyet ve Güvenlik:* Vatandaşların verilerini ve mahremiyetini korumak için güçlü güvenlik önlemleri uygulamak, elektronik işlemlerin güvenli bir şekilde yapılmasını sağlamak.
- *Geleneksel Kavramların Değiştirilmesi:* Geleneksel bürokratik yönetim modellerinden dijital teknolojilerin mümkün kıldığı daha çevik ve vatandaş merkezli yaklaşımlara geçiş.
- *Evrensel Erişim:* Her kurum ve bireyin devlet hizmetlerine dijital kanallardan kolayca erişebilmesinin sağlanması, kapsayıcılık ve eşitliğin teşvik edilmesi.

Genel olarak Dijital Türkiye, kamu hizmetlerinin sunumunu geliştirmek, idari süreçleri kolaylaştırmak ve vatandaş memnuniyetini artırmak için teknolojiden yararlanan, yönetime yönelik dönüştürücü bir yaklaşımı temsil etmektedir. Türkiye, dijitalleşmeyi benimseyerek, dijital çağda vatandaşlarının değişen ihtiyaçlarını karşılayan, daha duyarlı, şeffaf ve erişilebilir bir hükümet yaratmayı hedeflemektedir.

Dijital Türkiye

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 1 Sayılı Cumhurbaşkanlığı Kararnamesi'nde belirtildiği üzere, Cumhurbaşkanının belirlediği hedef, politika ve stratejiler doğrultusunda kamu hizmetlerinin dijital dönüşümüne öncülük etmekle görevlidir. Kamu hizmeti sunumunu kolaylaştırmayı, kurumlar arası iş birliğini geliştirmeyi ve dijital alanda koordinasyonu sağlamayı

amaçlayan Dijital Türkiye (e-Devlet)⁷⁶ girişiminin geliştirilmesinde önemli bir rol oynamaktadır. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin temel hedefleri ve girişimleri şunları içerir:

- *Dijital Dönüşüme Öncülük Etmek:* Kamu sektöründe dijital dönüşüm girişimlerini yönlendirmek için proaktif bir yaklaşım benimsemek, hizmetlerin kullanıcı odaklı ve ulusal hedeflerle uyumlu olmasını sağlamak.
- *Dijital Hizmetlere Aracılık Etmek:* Dijital Türkiye (e-Devlet) hizmetlerinin sunulmasını kolaylaştırmak, vatandaşlar için daha erişilebilir ve verimli hâle getirmek.
- *Kurumlar Arası İş Birliğinin Artırılması:* Dijital hizmetlerin sunumunu geliştirmek ve idari süreçleri kolaylaştırmak için devlet kurumları arasındaki iş birliğinin teşvik edilmesi.
- *Veri Odaklı Yaklaşım:* Hizmet sunumunda veri odaklı bir yaklaşımı benimsemek, süreçleri basitleştirmek ve vatandaşlara yüksek değer sağlayan hizmetlerin kullanılabilirliğini artırmak.
- *Kullanıcı Memnuniyetinin Artırılması:* Kullanıcı dostu arayüzler geliştirerek ve vatandaşların geri bildirimlerini dikkate alarak e-Devlet hizmetlerini sürekli olarak geliştirerek kullanıcı memnuniyetini ön planda tutmak.
- *Entegre Hizmetler:* Vatandaşların hayatlarını kolaylaştırmak için Araçlarım, İkametgahım, Çalışma Hayatım, Hac İşlemleri, Askerliğim gibi entegre hizmetler sunmak ve sürekli olarak yeni entegre hizmetler geliştirmek.
- *Veri Paylaşımı ve Mimarisi:* Devlet bilgi sistemleri arasında veri paylaşımını kolaylaştıracak veri sözlüğü ve kurumsal mimari çalışmalarının yapılması, böylece daha kaliteli ve katma değerli hizmet sunumunun sağlanması.

⁷⁶ T.C. CB DDO. <https://cbddo.gov.tr/dijital-tr/>

- *Teknoloji Üreticisi Olmak:* Türkiye'de teknoloji inovasyonu ve girişimcilik kültürünün geliştirilmesi, teknoloji tüketicisi olmaktan üreticiye geçişin sağlanması.
- *İş Birlikçi Yaklaşım:* Dijital Türkiye hedeflerine ulaşmak ve ülkenin kapsayıcı dijital dönüşümünü sağlamak için kamu, özel sektör, üniversiteler ve sivil toplum kuruluşlarından paydaşlarla bir araya gelmek.

Özetle, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, kamu hizmetlerinin iyileştirilmesine, vatandaşların yararına teknolojiden yararlanmaya ve Dijital Türkiye vizyonunu gerçekleştirmek için sektörler arası iş birliğini teşvik etmeye odaklanarak Türkiye'nin dijital dönüşüm gündemini yönlendirmede önemli bir rol oynamaktadır.

Dijital Türkiye Platformu

TBV (Türkiye Bilişim Vakfı), TÜBİSAD (Türkiye Bilişim Sanayicileri Derneği) ve TESİD (Türk Elektronik Sanayicileri Derneği) tarafından Mart 2011'de kurulan Dijital Türkiye Platformu, alanlarda iş birlikçi bir girişim olarak hizmet vermektedir. Türkiye'de⁷⁷ bilgi, iletişim ve elektronik sektörlerdeki zorlukları ele almayı, çözümler geliştirmeyi ve ilgili sorunları ilerletmeyi amaçlamaktadır. Dijital Türkiye Platformunun temel hedefleri arasında şunlar yer almaktadır:

- *Strateji ve Politika Geliştirme:* Türkiye'de bilgi, iletişim ve elektronik sektörlerindeki zorluklara ve fırsatlara yönelik strateji ve politika önerileri üretmek.
- *Ortak Vizyon ve Eylem:* Bu sektörlerde büyüme ve ilerlemeyi teşvik edecek ortak vizyon ve eylem planının belirlenmesi ve uygulanması.
- *Uluslararası İş Birliği:* Uluslararası kurumlarla ortaklıklar kurmak ve geliştirmek, Türkiye'nin bilgi, iletişim ve elektronik alanlarının küresel sahnede temsilcisi olarak hizmet vermek.

⁷⁷ Dijital Türkiye Platformu. <https://dijitalturkiyeplatformu.org/>

- *Savunuculuk ve Farkındalık:* Kamu kurumları ve politika yapıcılar için bilgi, iletişim ve elektronik sektörlerinin öneminin savunulması ve bu sektörlerdeki zorluklar ve fırsatlar hakkında farkındalık yaratılması.

Ayrıca Dijital Türkiye Platformu, çalışmalarını Avrupa Birliği içinde çok sayıda şirket ve STK'yı kapsayan kapsayıcı bir organizasyon olan Dijital Avrupa gündemiyle uyumlu hâle getirmektedir. Dijital Türkiye Platformu, Avrupa Birliği'nin dijital gündemini takip ederek, Türkiye'ye yönelik uluslararası standartlara ve en iyi uygulamalara uygun dijital stratejiler hazırlamayı amaçlamaktadır. Özetle Dijital Türkiye Platformu, iş birliğini teşvik ederek, stratejiler geliştirerek, politika savunuculuğu yaparak, uluslararası standart ve gündemlere uyum sağlayarak Türkiye'de bilgi, iletişim ve elektronik sektörlerinin geleceğini şekillendirmede önemli bir rol oynamaktadır.

3.2. Kritik Dijital Altyapıların Dayanıklılığı ve İş Sürekliliği

Kritik altyapıların dayanıklılığı ve iş sürekliliği, bir ülkenin temel işlevlerini sürdürebilmesi için hayati önem taşıyan sistemlerin güvence altına alınmasıyla doğrudan ilgilidir. ENISA⁷⁸'ya (European Union Agency for Cybersecurity) göre, bu altyapılar enerji, telekomünikasyon, ulaşım, su temini, sağlık ve finans gibi kilit sektörleri kapsar. Bu tür altyapıların ciddi hasar alması, ekonomik istikrarsızlık, kamu güvenliğinde zafiyetler ve hizmetlerde kesintilere yol açabilir.

Bu bağlamda, kritik altyapıların korunması ve sürekliliği, hem fiziksel güvenliği hem de siber tehditlere karşı korunmayı gerektirir. ENISA, siber güvenlik önlemleri geliştirerek Avrupa genelinde bu altyapıların korunmasına yönelik politikalar oluşturur. Özellikle, risk yönetimi ve tehditlere karşı dirençli sistemlerin geliştirilmesi için stratejiler sunar. Türkiye'de de benzer stratejiler, kritik altyapıların korunmasına yönelik olarak Ulusal Bilgi Güvenliği Programı çerçevesinde ele alınmaktadır. Bu stratejilerde siber güvenlik tehditlerine karşı dayanıklılık artırılmakta ve kritik altyapıların sürdürülebilirliği hedeflenmektedir. Bu şekilde, Türkiye'nin siber güvenlik stratejileri ve kritik altyapılar konusundaki politikaları, ENISA'nın önerdiği kapsamla paralel bir yaklaşım sergilemektedir. Kritik altyapıların korunması ve siber güvenlik politikalarının

⁷⁸ <https://www.enisa.europa.eu>

önemi, hem uluslararası düzeyde ENISA gibi kuruluşlar tarafından hem de Türkiye'de belirlenen stratejik programlar aracılığıyla vurgulanmaktadır. Kritik altyapılar kavramı, Türkiye'de ilk kez Ulusal Bilgi Güvenliği Programı ile gündeme gelmiştir. Bu program, bilgi teknolojileri altyapılarının ve sistemlerinin güvenliğini artırmak amacıyla oluşturulmuştur. Ancak, kavramın net bir şekilde belgelendiği ve uygulanabilir stratejilerin tanımlandığı temel kaynaklardan biri, Türkiye Ulusal Siber Güvenlik Stratejisi ve 2012-2014 Eylem Planı⁷⁹ olmuştur. Bu plan, kritik altyapıların korunmasının ulusal güvenlik açısından taşıdığı önemi ve gerekli tedbirlerin alınması gerektiğini açıkça ifade etmektedir.

Özellikle, Türkiye'de siber güvenlik stratejilerinin belirlenmesinde BTK (Bilgi Teknolojileri ve İletişim Kurumu) ve TÜBİTAK gibi önemli kurumların katkılarıyla geliştirilen bu belgeler, Ulusal Siber Güvenlik Stratejisi ve Ulusal Bilgi Güvenliği Eylem Planı gibi çalışmalarla desteklenmiştir. Bu süreçte, kritik altyapılar sadece fiziksel tehditlere değil, aynı zamanda siber tehditlere karşı da korunmaya başlamıştır. Bu eylem planları, kritik altyapıların korunmasında siber güvenlik tedbirlerinin alınmasını ve kamu ile özel sektör iş birliğini teşvik eden stratejik rehberler sunmaktadır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Türkiye'nin siber güvenlik alanındaki ilk ulusal planıdır ve kritik altyapıların korunmasına büyük önem vermektedir. Bu plan, kamu ve özel sektöre ait kritik altyapıların siber tehditlere karşı korunması için bir dizi hedef ve önlem sunar. Kritik altyapılar, enerji, ulaştırma, finans, sağlık, su temini gibi hayati hizmetler sağlayan sistemleri kapsar. İşte planın kritik altyapılar açısından önemli noktaları:

- **Kritik Altyapıların Tanımlanması ve Korunması:** Plan, kamu ve özel sektöre ait altyapıların güvenliğini sağlanması gerektiğini vurgular. Bu altyapılar, ülkenin ekonomik ve sosyal yapısı için hayati öneme sahiptir ve siber tehditlere karşı korunmalıdır.
- **İş Birliği ve Koordinasyon:** Kritik altyapıların korunmasında kamu ve özel sektörün iş birliği içinde çalışması gerektiği belirtilmiştir. Bu kapsamda, altyapı sahipleri ve

⁷⁹ T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2013.

işletmecilerinin güvenlik önlemlerini alması ve devlet kurumlarıyla koordinasyon içinde çalışması beklenir.

- Siber Olaylara Müdahale Kapasitesinin Geliştirilmesi: Kritik altyapılarda meydana gelebilecek siber saldırılara karşı etkili ve hızlı müdahale edebilmek için bir "Siber Olaylara Müdahale Ekipleri"nin (SOME) kurulması planlanmıştır. Bu ekipler, saldırıların erken tespiti ve önlenmesinde kilit rol oynar.
- Risk Analizi ve Yönetimi: Plan, kritik altyapıların güvenliğini artırmak için risk analizleri yapılmasını ve bu analizlere dayalı olarak güvenlik önlemlerinin geliştirilmesini öngörmektedir.
- Ulusal ve Uluslararası İş Birliği: Türkiye'nin kritik altyapılarının güvenliği için uluslararası siber güvenlik kurumlarıyla iş birliği yapılması gerektiği vurgulanmıştır. Bu iş birliği, uluslararası en iyi uygulamaların Türkiye'de uygulanmasını sağlayacaktır.

20.06.2013 Tarih ve 2 Sayılı Siber Güvenlik Kurulu Kararı⁸⁰

20.06.2013 tarihinde yayınlanan 2 sayılı Siber Güvenlik Kurulu kararı ile Türkiye’de kritik altyapı sektörleri olarak aşağıdaki 6 sektör belirlenmiştir:

- Elektronik Haberleşme
- Enerji
- Bankacılık ve Finans
- Kritik Kamu Hizmetleri
- Ulaştırma
- Su Yönetimi

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ

UAB tarafından hazırlanan ve 11.11.2013 tarihli ve 28818 sayılı Resmî Gazete’de yayınlanarak yürürlüğe giren “Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul

⁸⁰ Resmî Gazete. (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. Yayımlanma Tarihi: 20 Haziran 2013, Sayı: 28683.

ve Esaslar Hakkında Tebliğ”⁸¹ ile de USOM koordinasyonunda faaliyet gösterecek şekilde kritik sektörlerde Sektörel Siber Olaylara Müdahale Ekipleri’nin (Sektörel SOME) kurulması, kurumlar bünyesinde de Kurumsal SOME’lerin kurulması düzenlenmiş olup kurulacak olan SOME’lerin yapısı ve görevlerine yönelik de düzenlemeler getirilmiştir. Böylece ülkemizdeki teknik seviyedeki siber güvenlik yapılanması USOM, Sektörel SOME’ler ve Kurumsal SOME’ler olarak şekillenmiştir. Hâlihazırda, USOM koordinasyonunda görev yapan kritik altyapı sektörleri başta olmak üzere 2000’den fazla Sektörel ve Kurumsal SOME ülkemizin siber sahasının korunmasına yönelik çalışmaları gerçekleştirmektedir.

BTK Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği

13.07.2014 tarih 29059 sayılı Resmî Gazete’de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği⁸²; şebeke ve bilgi güvenliğinin sağlanmasına yönelik olarak işletmecilerin uyacakları usul ve esasları düzenlemektedir.

Yönetmelik; bilgi güvenliğinin en temel gereksinimleri olan “gizlilik”, “bütünlük” ve “erişilebilirlik” ilkelerini sağlamayı amaçlayan TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemini temel alan, TS ISO/IEC 27002 bilgi güvenliği kontrol ve uygulama adımlarını içeren ve telekomünikasyon kuruluşları için TS ISO/IEC 27011’e dayalı bilgi güvenliği denetimleri için uygulama prensiplerini dikkate alan bir düzenleme olup, ülkemizde sadece (AB) 2016/1148 sayılı NIS Direktifi ile değil, (AB) 2022/2555 sayılı NIS2 Direktifinin siber güvenlik risk yönetimi tedbirleri ile de en uyumlu düzenleme konumundadır.

Yönetmelik, BTK tarafından regüle edilen işletmecilere;

- BGYS’nin kurulması, kapsamı, politikası ve yönetimi
- Bilgi güvenliği grubu ve faaliyetleri
- Varlık yönetimi
- Risk değerlendirme ve işleme
- İş sürekliliği
- Bilgi güvenliği ihlal olaylarının ve güvenlik açıklarının yönetimi

⁸¹ Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, <https://hgm.uab.gov.tr/>

⁸² Resmî Gazete. (2014). Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği. Yayımlanma Tarihi: 13 Temmuz 2014, Sayı: 29059.

- Denetim
- İnsan kaynakları, gizlilik, eğitim ve disiplin
- Fiziksel erişim, çevresel tehditlere karşı korunma
- Ekipman ve çalışma ortamı güvenliği
- Elektronik ortam yönetimi
- Şebeke güvenliği
- Değişim yönetimi ve planlama
- Görevlerin ve ortamların ayrılması, erişim ve parola yönetimi
- Zararlı kodlara karşı korunma
- Yedekleme
- Zaman senkronizasyonu
- Sistem kayıt dosyalarının tutulması
- Bakım ve onarım, sistem ve yazılım temini veya geliştirilmesi
- Siber saldırılara yönelik tedbirler
- Belgelendirme, raporlama ve bildirim yükümlülükleri
- Felaket kurtarma merkezi gibi

yükümlülükler getirmektedir.

ISO 22301 İş Sürekliliği Yönetim Sistemi

Türk Standartları Enstitüsünün (TSE) belirlediği ve yönettiği “TS EN ISO 22301 İş Sürekliliği Yönetim Sistemi” iş sürekliliği yönetim standardıdır⁸³. Bu standart, bir kuruluşun yıkıcı bir olayın ardından faaliyetlerini kabul edilebilir seviyelerde sürdürebilmesini sağlamak için sağlam süreçler, prosedürler ve planlar oluşturma ve planların önemini vurgular. Kuruluşlar proaktif ve reaktif davranarak hem krizleri önleyebilir hem de etkilerini azaltabilir, sonuçta olumsuzluklarla karşı karşıya kaldığımızda normale hızlı bir şekilde dönüşü kolaylaştırabilir. Bu yaklaşım, kuruluşların dayanıklılıklarını artırmalarına ve ürün veya hizmetlerinin sürekliliğini sağlamalarına, böylece itibarlarını korumalarına ve müşteri güvenini sürdürmelerine yardımcı olur. Yaşanabilecek aksatıcı olaylara karşı iş sürekliliğini sağlamak için süreç ve prosedürler aşağıda maddeler hâlinde özetlenmiştir:

⁸³ ISO 22301 Standardı Komitesi, (2012). ISO 22301 Toplumsal Güvenlik-İş Sürekliliği Yönetim Sistemi

- Organizasyonel ihtiyaçlarla uyumlu politika ve hedefleri oluşturmak.
- Kesintilerden kurtulmayı kolaylaştırmak için süreçleri ve müdahale yapılarını işletmek ve sürdürülebilirliğini sağlamak.
- BCMS performansını ve etkililiğini izlemek ve gözden geçirmek.
- Niteliksel ve niceliksel ölçümlere dayalı sürekli iyileştirme.
- Mevcut ve potansiyel tehditleri tanımlamak ve yönetmek.
- Stratejik hedefleri, rekabet avantajını, itibarı ve güvenilirliği desteklemek.
- Olayların etkilerini en aza indirmek için proaktif önlemler almak.
- Kesintiler sırasında etkinliği artırmak ve operasyonel güvenlik açıklarını ele almak.
- Krizlerde kritik fonksiyonların devamını sağlamak.
- Kurtarma sürecini iyileştirmek ve aktivite kesintilerini en aza indirmek.
- Müşteri ve tedarikçi taleplerini karşılayacak esneklik sağlamak.
- Can, mal ve çevreyi korumak ve ilgili tarafların beklentilerini dikkate almak.
- Yasal ve finansal risklerin yanı sıra kesinti maliyetlerini azaltmak.
- İş sürekliliğini sağlamak için sistematik bir yaklaşım sunmak.
- Yapılandırılmış organizasyonel unsurlar ve kaynaklar aracılığıyla idari kolaylık sağlamak.
- İyi iş sürekliliği uygulamalarıyla müşteri güvenini ve memnuniyetini artırmak.

Bu noktalar toplu olarak ISO 22301 standardının kuruluşların yıkıcı olaylara hazırlanmalarına, müdahale etmelerine ve bu olaylardan kurtulmalarına yardımcı olma, böylece iş sürekliliğini sağlama ve genel dayanıklılığı artırma konusundaki kapsamlı doğasını vurgulamaktadır.

Değişen tehditlere ve teknolojik gelişmelere yanıt olarak politikaların ve mevzuatın sürekli olarak değerlendirilmesi ve güncellenmesi de önemlidir. Kritik altyapı sektörlerinin olgunluğunun düzenli olarak değerlendirilmesi ve düzenlemelere uyumun raporlanması, iyileştirme alanlarının belirlenmesine ve sürekli iyileştirme çabalarının desteklenmesine yardımcı olabilir. EPDK'nın enerji sektörüne yönelik siber güvenlik modelinin uygulamaya konulması, otomasyon ve kontrol sistemlerinin siber tehditlerden korunmasının kritik önemini vurgulamaktadır. OPSWAT gibi siber güvenlik firmaları bu konuda hayati bir rol oynamakta ve kritik altyapıları saldırılara karşı güçlendirecek çözümler sunmaktadır. Ancak siber tehditlerin gelişen karmaşıklığı, enerji şirketlerinin dayanıklılığını sağlamak için sürekli dikkatli olmayı ve proaktif önlemleri gerektirmektedir.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023

2012 yılından itibaren sürdürülen çalışmalar kapsamında, UAB koordinasyonunda ulusal siber güvenlik organizasyonu oluşturulmuş, 2013-2014 ve 2016-2019 dönemlerini kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları hazırlanarak hayata geçirilmiştir. İlgili kurum ve kuruluşların katkılarıyla gerçekleştirilen çalışmalar neticesinde; günümüze dek elde edilen kazanımların daha ileriye taşınması, siber tehditlerin etkilerinin azaltılması, güvenli bir siber ortamın oluşturulması ve ülkemizin siber güvenlik alanında uluslararası seviyede en üst sıralarda yer alması hedeflenerek "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)"⁸⁴ oluşturulmuş ve hayata geçirilmiştir.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)'ün amaçlarından biri kritik altyapıların korunması ve mukavemetin artırılması olup bu amaç kapsamında kritik altyapılarımızın ve siber uzaydaki tüm ulusal varlıklarımızın siber tehditlere karşı etkin şekilde korunmasına yönelik çalışmalar yürütülmüştür. Ayrıca; siber olaylara müdahale kabiliyetlerimizin

⁸⁴ T.C. Ulaştırma ve Altyapı Bakanlığı Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), 2020.

daha da güçlendirilmesi ve kritik altyapı sektörleri ile Sektörel SOME'lerin güncellenmesini hedefleyen eylemler kapsamında çalışmalar yürütülmüştür.

Yine UAB koordinasyonunda paydaşlarla beraber hazırlanan ve yayınlanmak üzere Cumhurbaşkanlığı'na gönderilen 2024-2028 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda da kritik altyapıların korunmasını ve dayanıklılığının artırılmasını amaçlayan eylemlere yer verilmiştir.

EPDK Siber Güvenlik Yeterlilik Modeli Yönetmeliği

EPDK'nın 100 MW ve üzeri kapasiteye sahip enerji şirketlerine siber güvenlik modeline uyum sağlama talimatı, kurumlara bir hazırlık süreci sağlamaktadır. OPSWAT, bu düzenlemeye karşılık olarak 2023 yılında EPDK Siber Güvenlik Yeterlilik Modeli Yönetmeliğini titizlikle inceleyerek ürünlerini belirlenen gereklilikleri karşılayacak şekilde uyarlamıştır. Genelgede özetlenen dokuz kriter için OPSWAT, bunlardan beşini ele alacak teknolojileri kolaylıkla sağlayabilir. OPSWAT'ın kapsamı dışında kalan alanlar için kurumlar, gerekli gereklilikleri yerine getirmek amacıyla diğer şirketlerin ürünlerini keşfetme esnekliğine sahiptir. Enerji şirketleri, EPDK'nın siber güvenlik modeline bağlı kalarak ve OPSWAT gibi siber güvenlik firmalarının uzmanlığından yararlanarak siber tehditlere karşı dayanıklılıklarını artırabilir ve kritik altyapı varlıklarını etkin bir şekilde koruyabilir. Bu proaktif yaklaşım, enerji sistemlerinin gelişen siber riskler karşısında güvenli, güvenilir ve dirençli kalmasını sağlar.

Nitekim enerji sektörü için geliştirilen siber güvenlik yetkinlik modeli, sektörün siber tehditlere karşı direncini önemli ölçüde artıracak çok sayıda avantaj ve fayda sunmaktadır.

- *Altyapı Güvenliği:* Enerji sektörü, modeli uygulayarak kritik altyapıların güvenliğini artırabilir, onları siber tehditlere karşı daha dayanıklı hâle getirebilir ve temel hizmetlerin kesintisiz sağlanmasını sağlayabilir.
- *Tehdit Tespiti ve Yanıtı:* Model, siber tehditleri anında tespit etmek, analiz etmek ve engellemek için gelişmiş yetenekler sağlar. Bu, enerji şirketlerinin tehditleri daha hızlı tespit edip bunlara yanıt vermesini sağlayarak olası zararları ve operasyonlardaki aksamayı en aza indirir.

- *Uyumluluk ve Mevzuat Gereksinimleri:* Model, enerji şirketlerinin güvenlik standartlarını ve mevzuat gerekliliklerini karşılamalarına, uyumluluk süreçlerini kolaylaştırmalarına ve sektör düzenlemelerine uyumu sağlamalarına yardımcı olur.
- *Risk Yönetimi:* Etkin risk yönetimi, siber saldırılardan kaynaklanan operasyonel aksaklıkları ve maliyetleri en aza indirmek için büyük önem taşımaktadır. Model, enerji şirketlerinin riskleri etkili bir şekilde tahmin etmesine ve azaltmasına yardımcı olarak siber tehditlere karşı genel dayanıklılığı artırmaktadır.
- *Farkındalık ve Eğitim:* Siber güvenlik konusunda farkındalığın artırılması ve eğitim verilmesi, güvenlik açıklarının azaltılması açısından önemlidir. Model, çalışanları ve paydaşları eğitmek, kuruluş çapında siber güvenlik farkındalığını ve hazırlıklılığını artırmak için kaynaklar ve destek sunar.
- *Veri Koruma:* Enerji şirketleri, müşteri bilgileri ve operasyonel veriler gibi hassas verileri yetkisiz erişime ve ihlallere karşı korumalıdır. Model, veri koruma stratejilerini güçlendirir ve hassas bilgilerin gizliliğinin ve bütünlüğünün sağlanmasına yardımcı olur.

Genel olarak enerji sektörüne özel olarak hazırlanan siber güvenlik yetkinlik modeli, altyapı güvenliğinin, siber tehditlere karşı hazır bulunuşluğun ve operasyonel sürekliliğin artırılmasında önemli bir rol oynamaktadır. Modelin etkili bir şekilde uygulanmasıyla sektör, işlerini daha güvenli ve sağlam bir temel üzerinde yürütebilir, kritik varlıkları koruyabilir ve paydaşlar arasında güven ve güvenilirliği koruyabilir.

On İkinci Kalkınma Planı (2024-2028)

Cumhuriyetimizin yüzüncü yılı 2023 yılında T.C. Cumhurbaşkanlığı Strateji ve Bütçe Bakanlığı, ülkemizin sürdürülebilir ve kapsayıcı büyüme hedeflerini kapsayan On İkinci Kalkınma Planı'nı (2024-2028) yayınlamıştır⁸⁵. “Afetlere Dirençli Yaşam Alanları, Sürdürülebilir Çevre” başlığı ile afet riskinin azaltılmasına ve etkili afet yönetimi stratejilerine öncelik vererek toplumları

⁸⁵ T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi On İkinci Kalkınma Planı (2024-2028), 2023.

afetlerin yol açtığı zorluklara karşı daha dayanıklı ve daha hazırlıklı hâle getirecek politika ve tedbirler yayınlanmıştır. Yayınlanan belgede “Türkiye Afet Yönetimi Strateji Belgesi” hazırlanacak, “İl Afet Risk Azaltma Planları (İRAP)” güncellenecek, “Türkiye Afet Risklerinin Azaltılması Platformu” etkinliği aktif hâle getirilecek, uluslararası iş birlikleri artırılacak gibi birçok hedef yayınlanmıştır.

Risk yönetimi ve iş sürekliliğine yönelik artan farkındalık ve yatırım, altyapı dayanıklılığı için çok önemlidir. Güvenlik olgunluk düzeyleri BT ve OT altyapıları arasında farklılık gösterir ve özel stratejiler gerektirir. İletişim yedekliliğini artırmak, operatörden bağımsız yapılar oluşturmak ve riskleri haritalamak, altyapı dayanıklılığı açısından kritik öneme sahiptir. Çoklu altyapı gelişiminin vurgulanması, Kahramanmaraş depremleri sırasında ortaya çıkan eksikliklerin de gösterdiği gibi, gelecekteki riskleri azaltmak için kapsamlı önlemlerin aciliyetinin altını çizmektedir. Telekomünikasyondaki afet ve salgınlara karşı dayanıklılık, açık kaynak ve ulusal kaynaklara hâkimiyetin vurgulanmasını gerektirir. Dayanıklılığın artırılması için açık kaynaklı ve yerel çözümler savunulmaktadır. Bilgi Teknolojisi (BT) ile Operasyonel Teknolojinin (OT) ayrılmasının altı çizilmekte, ancak aralarındaki ortak noktaların tanınması etkili siber savaş hazırlığı için çok önemlidir. Risk yönetiminin güçlendirilmesi ve kurumsal farkındalığın geliştirilmesi büyük önem taşımaktadır.

3.3. Veri Egemenliği Politikaları ve Kriptoloji

Türkiye’de Veri Egemenliği Politikaları

Veri egemenliği aslında bireylerin veya kuruluşların, verilerinin nasıl yönetileceğini, saklanacağını ve işleneceğini belirleme yetkisine ve hakkına sahip olduğu kavramdır. Günümüzün dijital dünyasında veri egemenliği hem bireyler hem de işletmeler için inanılmaz derecede önemlidir. Bu aslında kendi verileriniz üzerinde kontrole sahip olmak anlamına gelir. Bireyler için bu kontrol, kişisel bilgilerin güvende tutulmasını ve yetkisiz erişime veya kötüye kullanıma karşı korunmasını sağlar. Ayrıca bireylere, gizliliğin korunması için gerekli olan, verilerinin nasıl kullanılacağına, paylaşılacağına ve işleneceğine karar verme hakkı verir. Benzer şekilde işletmeler için veri egemenliği, müşteri bilgileri ve mali kayıtlar gibi hassas kurumsal verilerin korunması

açısından hayati öneme sahiptir. İşletmeler, verileri üzerinde kontrol sahibi olarak veri ihlallerini önleyebilir ve veri koruma ve gizlilikle ilgili düzenlemelere uyum sağlayabilir.

Dijital teknolojilerin büyük miktarda veri toplama ve işlemeyi kolaylaştırdığı bir çağda, veri egemenliği giderek daha kritik hâle gelmektedir. Veri güvenliği, gizlilik ve yasal ve düzenleyici gerekliliklere uyumla ilgili endişelerin giderilmesine yardımcı olur. Bireyler ve kuruluşlar, verileri üzerinde kontrol sahibi olarak riskleri azaltabilir ve veri yönetimi uygulamalarının kendi değerleri ve hedefleriyle uyumlu olmasını sağlayabilir.

Günümüzün dijital çağında veri merkezleri, sürekli genişleyen bilgi teknolojileri ortamını ve her gün üretilen verilerin katlanarak büyümesini desteklemede çok önemli bir rol oynamaktadır. Bağlantılı dünyamızın omurgası olan veri merkezleri, dijital altyapımızın temelini oluşturarak işletmeler, kuruluşlar ve bireyler için kritik öneme sahip büyük miktarda verinin depolanmasını, işlenmesini ve dağıtımını kolaylaştırır. Veri odaklı toplumumuzun artan taleplerini karşılamak için veri merkezlerini geliştirmeye ve optimize etmeye devam etmemiz zorunludur.

Ülkemiz, stratejik coğrafi konumu, teknolojiye meraklı genç nüfusu, hızla büyüyen dijital ekonomisi ve yenilikçi zihniyeti sayesinde veri merkezleri alanında büyük bir potansiyele sahiptir. Türkiye'deki veri merkezlerinin gelişimini besleyerek ve destekleyerek dijital ekosistemimizi güçlendirebilir ve hem yerli hem de uluslararası yatırımcıları çekebiliriz. Bu da ekonomik büyümeyi teşvik edecek, katma değeri yüksek işletmelerin kurulmasını teşvik edecek ve istihdam olanakları yaratacaktır.

Türkiye'yi veri depolama ve işleme alanında bölgesel bir merkez olarak konumlandırma vizyonu doğrultusunda, ilgili hedefler 2019-2023 dönemini kapsayan 11. Kalkınma Planı'na dâhil edilmiştir.⁸⁶ Bu hedefler, ülkemizde veri merkezi altyapısının büyümesi ve genişletilmesi için elverişli bir ortam oluşturma konusundaki kararlılığımızın altını çizmektedir. Veri merkezlerinin geliştirilmesine yatırım yaparak güçlü yönleri değerlendirmek, dijital ekonomideki fırsatları yakalamak ve Türkiye'yi küresel veri ortamında bir lider olma yolunda ilerletmek hedeflenmektedir.

⁸⁶ T.C. Strateji ve Bütçe Başkanlığı, B. (2019). On Birinci Kalkınma Planı (2019-2023). Erişim adresi: https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Plani-2019-2023.pdf (Erişim tarihi: 14.02.2021).

Dijital egemenliğe ulaşmak hem teknolojik üstünlüğü hem de destekleyici mevzuatı birleştiren dengeli bir yaklaşım gerektirir. Teknolojik gelişmeler egemenliğin temelini oluştururken mevzuat da dijital varlıkların uygun şekilde yönetilmesini ve korunmasını sağlar. Çevik yetenek kazanımı yapıları oluşturmak ve teknolojik yetenekleri geliştirmek için yazılım fabrikaları gibi girişimleri teşvik etmek çok önemlidir. Eş zamanlı olarak, gelişen dijital zorlukları ele almak ve uluslararası standartlara uygunluğu sağlamak için yasal çerçevelerin sürekli olarak güncellenmesi gerekmektedir. Sonuçta teknolojik üstünlük ile mevzuatın uyumlu entegrasyonu, sürdürülebilir dijital egemenliğin yolunu açmaktadır.

Veri egemenliği politikaları geliştirmek, dikkatli değerlendirme ve stratejik planlama gerektiren çeşitli zorlukları beraberinde getirir. Önemli zorluklardan biri, sürdürülebilirliği sağlarken ülkenin rekabetçi özelliklerini dinamik bir şekilde aktaran bir politika oluşturma mekanizması vücuda getirmektir. Ayrıca bürokratik engellerin, sınıflandırma sistematığının ve kapsamlı bir veri yaşam döngüsünün eksikliğinin de ele alınmasına ihtiyaç vardır. Diğer bir engel ise dışa bağımlılık sorunlarının yönetilmesi ve veri paylaşımına ilişkin sınırların belirlenmesidir. Veri güvenliği maliyetlerini veri kritikliğiyle dengelemek, mevzuata ve teknolojik gelişmelere uygunluğu sağlamak daha fazla karmaşıklığa yol açmaktadır. Dahası, kurumlar içinde uzmanlığın teşvik edilmesi ve sektörlerin ve STK'ların katılımının sağlanması, etkili politika geliştirme ve uygulama açısından çok önemlidir. Genel olarak, veri egemenliğine ulaşmak, çeşitli sektörlerde iş birliğini ve yeniliği teşvik ederken bu zorlukları ele alan çok boyutlu bir yaklaşımı gerektirir.

Kuşkusuz gerçek ve tüzel kişiler nezdinde veri egemenliğinin sağlanması öncelikli hedeflerden olmakla birlikte, kamu nezdinde veri egemenliğinin sağlanması millî güvenliğimizin sağlanması için elzemdir. 5809 sayılı Elektronik Haberleşme Kanunu'nun "Bakanlığın görev ve yetkileri" başlıklı 5'inci maddesinde "ı) *Ulusal kamu entegre veri merkezlerine yönelik politika, strateji ve hedefleri belirlemek, eylem planlarını hazırlamak, eylem planlarını izlemek, e-Devlet hizmetlerinde kullanılan verilerin ve sistemlerin barındırıldığı veri merkezlerini kamu entegre veri merkezlerinde toplamak amacıyla verilerin transferi de dâhil gerekli altyapıları kurmak, kurdurmak, işletmek, işlettirmek ve tüm bu faaliyetlere yönelik uygulama usul ve esaslarını belirlemek, kurulum, uygulama ve işletim süreçlerini planlamak, yürütmek ve koordine etmek.*" hükmüne binaen, kamu veri egemenliğini sağlama görevi Ulaştırma ve Altyapı Bakanlığına tevdi edilmiştir.

Türkiye’de Veri Merkezlerine Yönelik Verilen Teşvikler

Türkiye, veri merkezlerinin gelişimini desteklemek ve ülkenin bilişim sektörünün yanı sıra dijital altyapısını güçlendirmek amacıyla çeşitli düzenleme ve teşvikleri hayata geçirmiştir. Bu tedbirlerin amacı yenilikçiliği teşvik etmek, yatırım çekmek, ekonomik büyümeyi teşvik etmek ve Türkiye'nin dijital ekonomisinin rekabet gücünü artırmaktır.

Sanayi ve Teknoloji Bakanlığı, Türkiye’de minimum 5.000 metrekare beyaz alan gereksinimini karşılayan veri merkezlerine, %18 kazanç sağlayan KDV muafiyeti, %2 kazanç sağlayan gümrük vergisi muafiyeti ve %40 kazanç sağlayan vergi indirimi, yaklaşık %35 kazanç sağlayan sigorta primi işveren hisse desteği, yatırım yeri veya alan tahsis ve faiz veya temettü desteği sağlamaktadır.

Ticaret Bakanlığı, gelirlerin en az %20’sini yurt dışından elde eden veri merkezi işletmecilerine belirli gider kalemlerinin %60’ını ve 2 yıl süreyle maksimum 24.000.000 TL destek sağlamaktadır. Bunlara ek olarak satın alınacak veya kiralanacak makineler için ek olarak %10 teşvik sağlanmaktadır.

Bu destekler yurt dışı faaliyetlerini teşvik etmek ve yerli veri merkezlerimizi uluslararası pazarda desteklemek içindir. Böylelikle Türkiye’nin dijital ekonomisi geliştirilerek yurt dışı gelirlerinin artması amaçlanmaktadır. Bugün için 20’nin üzerinde veri merkezi ile işlemler yürütülmektedir.

Turkcell Genel Müdürlüğü tarafından, Türkiye'nin verilerini Türkiye'de tutma hedefiyle veri merkezleri pazarındaki lider konumunu korumak için 330 milyon avro yatırım yapıldığı açıklanmıştır. Açıklamaya göre, şirketin planları arasında yeni bir veri merkezi şirketi kurmak da bulunmaktadır. Bu bağlamda, şirketin Türkiye'ye "hyper-scaler" küresel bir marka getirmeyi hedeflediği belirtilmiştir.

Turkcell'in İngiliz rakibi Vodafone, Edgnex Data Centers ile DAMAC tarafından bir ortak girişim şirketi kurarak 2025’in ilk çeyreğinde faaliyete geçecek olan İzmir’de 100 milyon dolarlık bir veri merkezi kuracağını duyurmuştur.

KVKK

6698 Kişisel Verilerin Korunması Kanunu (KVKK), kişisel verilerin işlenmesini düzenlemek ve bireylerin gizlilik haklarına saygı duyulmasını sağlamak için tasarlanmıştır. KVKK ile veri egemenliği politikaları arasındaki ortak nokta, bireylerin verilerinin ve gizlilik haklarının korunması yönündeki ortak hedeflerinde yatmaktadır. Hem KVKK hem de veri egemenliği politikaları, kişisel bilgilerin hukuka uygun, şeffaf ve güvenli bir şekilde işlenmesini sağlamak amacıyla verilerin işlenmesini düzenlemeyi amaçlamaktadır. Ek olarak, bireylerin verilerini kontrol edebilmeleri ve veri denetleyicileri ile işleyiciler üzerinde hesap verebilirliği uygulayabilmeleri için mekanizmalar kurmayı amaçlamaktadırlar. Özetle, KVKK ve veri egemenliği politikaları, farklı açılardan da olsa, kişisel verilerin korunmasına ve bireylerin veri koruma ve mahremiyet haklarının desteklenmesine odaklanmaktadır.

3.4. Toplumsal Dijital Dayanıklılık

İnternet Kullanımı ve Dijital Okuryazarlık

Türkiye’de günün 7 saat 24 dakikasının ekrana bakarak geçirildiği (Dünya ortalaması 6 saat 37 dakika) 2023 yılında yayımlanan bir çalışma raporunda belirtilmektedir. Aynı araştırmaya göre vatandaşlarımız, bu sürenin 4 saat 26 dakikasını cep telefonu, 2 saat 58 dakikası bilgisayar başında olmak üzere, günde yaklaşık 3 saatini sosyal medya için harcamakta ve dünya sıralamasında bu konuda 10’uncu sırada yer almaktadır⁸⁷.

2023 yılında yayımlanan konuyla ilgili bir OECD raporuna göre ise, Türkiye'deki kamu görevlilerinin dijital okuryazarlığı ve 21’inci yüzyıl becerileri kapsamında, kuruluşların %73’ünün kendilerini ortalama düzeyde gördüğü, %15’inin ise çok iyi olarak değerlendirdiği belirtilmektedir.⁸⁸

Yine aynı raporda Türkiye'deki insanların alışveriş için İnternet'i seçme tercihlerinin Avrupa Birliği'ne kıyasla daha düşük bir görünüm arz ettiği; 2021'de nüfusun yalnızca %49'u çevrimiçi bir şey satın alırken bu oranın AB27 içerisinde %74 olduğu, yaş gruplarına göre ise ülkemizde 55-74 yaş arası vatandaşların %17'sinin İnternet'i bir şey satın almak için kullandığı belirtilirken bu oranın, 25-54 yaş arası için ise %50 olarak kaydedildiği belirtilmektedir.

⁸⁷ Electronics Hub, 26.08.2024, <https://www.electronicshub.org/the-average-screen-time-and-usage-by-country/>

⁸⁸ Digital Government Review of Türkiye, OECD, 2023

OECD'nin üye ülke öğrencilerinin dijital okuryazarlık durumuna odaklı olarak 2021 yılındaki raporunda, dijital ortamda ulaştığı bir bilginin taraflı olup olmadığını nasıl anlayacağı konusunda okulda eğitim aldığı bildirilen ülkemiz öğrencilerinin oranının yarıdan az olduğu görülmektedir. Diğer yandan rapor, Türkiye'deki öğrencilerin dijital ortamda gerçek olanı fikirden ayırt edebilme becerisinin OECD ortalamasının üzerinde olduğunu ortaya koymaktadır. Ayrıca, OECD ülkelerinin çoğunda olduğu gibi Türkiye'de de dijital cihaz kullanımı için harcanan zaman ile okuma performansı arasında ters orantı bulunmaktadır⁸⁹.

Global Vodafone Vakfı'nın IPSOS Almanya iş birliğiyle her ülkeden bin olmak üzere toplam on bin kişiyle gerçekleştirdiği ve 2023'te yayınladığı anket çalışması⁹⁰ sonuçlarına göre Türkiye'de ebeveynlerin;

- %87'si çocuklarının geleceği açısından dijital becerilerin önemli olduğuna inanmakta ve sınıflarda dijital teknoloji kullanımını desteklemekte,

- %87'lik bir çoğunluğu, dijital okuryazarlığın okullarda temel öğrenim hedeflerinden biri olması, %70'lik bir kesim de dijital teknoloji kullanımı konusunda Avrupa genelindeki standartların aynen geçerli olması gerektiğini düşünmekte,

- %61'i, çocuklarının dezenformasyona maruz kalmasından endişe etmekte, %46'sı, okullara dışarıdan uzmanların gelerek çocuklara eğitim vermesi, %45'i de ebeveynler için bilgilendirme etkinliklerinin yapılması gerektiğini belirtmekte,

- %50'si, sınıflarda dijital araç kullanımı konusunda devlet tarafından öğretmenlere daha fazla eğitim verilmesi, %45'i, sınıfta dijital eğitime yaklaşımlar konusunda okullara rehberlik hizmeti verilmesi ve %43'ü de dijital teknolojiler için daha fazla finansman sağlanması gerektiğini ifade etmektedir.

Toplumsal Dijital Dayanıklılık İçin Kapasite Geliştirme

⁸⁹ 21st Century Readers-Developing Literacy Skills In A Digital World, OECD, 2021

⁹⁰ Türkiye Vodafone Vakfı, 26.07.2023. <https://turkiyevodafonevakfi.org.tr/haberler/global-vodafone-vakfi-ndan-dijital-yetenek-egitimi-arastirmasi>

Millî Eğitim Bakanlığının örgün ve yaygın programlarına (ilk ve ortaöğretim) ilişkin müfredatları içerisinde güvenli İnternet ve siber güvenlik farkındalığına yönelik kazanımların tanımlandığı ve ders içeriklerinin bulunduğu bilinmektedir. Bu kapsamda ayrıca MEB bünyesinde teknik eğitim veren liselerin bilişim teknolojileri alanında ağ yönetimi ve güvenliğine ilişkin dersler bulunmaktadır.

Dijital okuryazarlığın, bilgi güvenliği farkındalığının ve daha ileri seviye siber güvenlik yeteneklerinin geliştirilmesi suretiyle toplumsal dijital dayanıklılık kapasitesinin artırılması için başta devlet olmak üzere çeşitli kurum ve kuruluşlar tarafından ülkemizde yapılan diğer çalışmalar ve yürütülen projeler aşağıda sunulmuştur.

Fırsatları Artırma ve Teknolojiyi İyileştirme Hareketi (FATİH) Projesi

2012 yılında başlatılan proje ile Millî Eğitim Bakanlığı okullarındaki dersliklerin akıllı sınıf formuna dönüştürülmesi planlanmış, projenin üç yıl içerisinde tamamlanması öngörülmüştür. Dizüstü bilgisayar ve tabletler, fotokopi cihazları, akıllı tahtalar ve geniş bant İnternet bağlantısı gibi hizmetlerin yer aldığı projede, öğrencileri dijital güncel teknolojilerle buluşturması ve eğitim öğretimde teknolojinin geniş bir şekilde yer alması hedeflenmiştir⁹¹.

Eğitim Bilgi Ağı (EBA)

Millî Eğitim Bakanlığı tarafından işletilmekte olan uzaktan yaygın eğitim aracı olarak EBA, her bir bireyin kullanımına ücretsiz olarak sunulmuş çevrimiçi bir sosyal eğitim platformudur. EBA’da bulunan e-içerikler, alanında uzman ekipler tarafından üretilmekte; ayrıca Türkiye’de ve dünyada dijital yayıncılık alanında önde gelen eğitim firmaları tarafından sağlanan içeriklerle de sistem zenginleştirilmektedir. Aynı zamanda öğretmen ve öğrenci kullanıcı kitlesinin yaptığı paylaşımlarla birlikte gittikçe büyüyen bir kaynak havuzu hâline gelmektedir. Televizyon yayınlarıyla da hedef kitleye ulaşan EBA’da hâlihazırda yaklaşık 3000 ders, 65.000 içerik, 85.000 soru ve 4.300 adet kitap bulunmaktadır.

Siber Yıldız⁹²

⁹¹ T.C. MEB Fatih Projesi, <http://fatihprojesi.meb.gov.tr/>

⁹² Siber Yıldız, <https://www.siberyildiz.com/>

Siber Yıldız yarışması, 2016 yılından bu yana Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından düzenlenen ve bugüne kadar 18.000’den fazla kişinin başvurmuş olduğu bir etkinliktir. Katılımcılar, Türkiye Cumhuriyeti vatandaşı olmak kaydıyla siber alanda yeteneklerini sergileyebilirler. Yarışmaya bireysel olarak veya en fazla dört kişilik gruplar hâlinde katılma imkânı bulunmaktadır. Katılım için cep telefonu ve e-posta onayı dışında herhangi bir şart aranmamaktadır. Yarışmanın amacı, siber güvenlik alanında ilgi ve yetenek sahibi bireyleri bulmak, onlara kendilerini geliştirme fırsatı sunmak ve Türkiye’de siber güvenlik farkındalığını artırmaktır. Yarışma İnternet üzerinden gerçekleştirilmekte ve bir gün sürmektedir. Siber kapasite geliştirmeye matuf söz konusu yarışmada dereceye giren yarışmacılara çeşitli ödüller verilmektedir.

Yarışmaya hazırlık için, sanal bir Kali Linux işletim sisteminin hazır olması önerilmekte, yarışma başlangıcında sorular tüm katılımcılara açılmakta, belirli bir puana ulaşan yarışmacılara ise yeni sorular sorulmakta, bu sayede yarışmacıların yetenekleri ve bilgi düzeyleri görülebilmektedir.

USOM tarafından organize edilen Siber Yıldız yarışmasının beşincisi olan “Siber Yıldız 2024” yarışması 8-9 Mart 2024 tarihlerinde gerçekleştirilmiştir.

FETİH Siber Talimhane⁹³

FETİH Siber Talimhane, ağda bulunan makineler üzerinde çeşitli zafiyetler bulunan ve katılımcılardan bu zafiyetleri istismar ederek sistemleri ele geçirmeleri beklenen “bayrağı yakala” (*Capture the Flag*) tarzı pratiğe yönelik bir siber güvenlik eğitim platformudur.

Fetih Siber Talimhane projesi ile Türkiye’nin siber güvenlik uzmanlarının keşfedilmesi veya yeteneklerinin geliştirilmesi için laboratuvar imkânı sunulmaktadır. Kendini siber güvenlik alanında geliştirmek isteyen katılımcılara bu platform aracılığıyla eğitim verilerek siber güvenlik ekosistemine katkı sağlanmaktadır. An itibarıyla söz konusu eğitimi alan 807 kişi bulunmaktadır.

Siber Kalkan

Siber güvenlik tatbikatları tehditlere karşı alınan tedbirlerin etkinliğini ve bu tedbirleri işleten iş gücünün yetkinliğini ölçmek için kullanılan ana araçlardan biridir. Türkiye’de, Ulaştırma

⁹³ Fetih, Siber Talimhane. <https://www.fetih.gov.tr/>

ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu tarafından “Ulusal Siber Kalkan” tatbikatları gerçekleştirilmektedir.

Siber güvenliğin ulusal paydaşlarını bir araya getiren Ulusal Siber Kalkan Tatbikatı, siber olaylara müdahale yeteneklerini geliştirmeyi ve iş birliğini geliştirmeyi amaçlamaktadır. Etkinliğe Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu ev sahipliği yapmaktadır. Siber Kalkan tatbikatlarında kullanılan tüm altyapı ve senaryolar USOM tarafından hazırlanmaktadır.

Tatbikat, en yaygın gözlemlenen ve gerçekçi tehditleri içeren farklı senaryolar ile katılımcı ekipler arasındaki iletişimin artırılması için kurgulanmaktadır. Ayrıca, kurum ve kuruluşların karşılaşılabileceği kritik altyapının korunması ve gelişmiş siber güvenlik tehditlerini de ele almaktadır.

Ulaştırma ve Altyapı Bakanlığı koordinasyonu ve BTK-USOM ev sahipliği ile gerçekleştirilen siber kalkan tatbikatları 7 ulusal ve 2 uluslararası olmak üzere toplamda 9 kez gerçekleştirilmiştir. Örnek olarak:

- 2019 yılında “Cyber Shield” uluslararası tatbikatı Ulaştırma ve Altyapı Bakanlığı ve BTK-USOM iş birliğinde gerçekleştirilmiştir. Cyber Shield tatbikatına 17 farklı ülkeden 87 katılımcı dâhil olmuştur.
- 2021 yılında “Ulusal Siber Kalkan” tatbikatı Ulaştırma ve Altyapı Bakanlığı ve BTK-USOM iş birliğinde gerçekleştirilmiştir. 36 kurumdan 135 uzmanın katılımıyla gerçekleşmiştir.
- 2022 yılında düzenlenen “Ulusal Siber Kalkan” tatbikatı kapsamında 55 kamu kurumundan 250’ye yakın siber güvenlik uzmanının katılımıyla gerçekleşmiştir.
- 2022 yılında Finans Sektörü’ne özel düzenlenen “Finans Sektörü Siber Kalkan” tatbikatı kapsamında 36 farklı finans kuruluşundan 150’den fazla siber güvenlik uzmanının katılımıyla gerçekleştirilmiştir.

Diğer USOM Farkındalık Faaliyetleri

2020-2023 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisinde “SOME Olgunluk Modeli” geliştirilmesi ile yer almakta olan eylem maddesi kapsamında hazırlanan SOME Olgunluk

Modeli Anketi'nin ilki 2022 yılında yapılmıştır. Hazırlanan SOME Olgunluk Modeli Anketinde 6 ana kategoride toplam 49 soru yer almıştır.

Üniversite bilgi işlem sorumlularına siber güvenlik farkındalığını artırmak amacıyla temel siber güvenlik farkındalığı konularını içeren bir eğitim programı hazırlanıp ilgili personellere BTK/USOM bünyesinde eğitimler verilmiştir. Siber farkındalığın artması ile birlikte, üniversiteler genelinde siber olayların tespit ve engellenme oranlarında artış görülerek, maddi ve manevi kayıpların önüne geçilmesi amaçlanmıştır.

USOM ve BTK Akademi iş birliği ile ülke genelindeki tüm SOME personellerine siber güvenlik bilgilerinin ve olgunluk seviyelerinin yükseltilmesi amacıyla "SOME Online Eğitim Serisi" hazırlanıp hizmete sunulmuştur. Eğitimler çeşitli içerik ve seviyelerde toplam 172 dakika olup 8 bölüm, 76 video ve 40 adet etkileşimli sorudan oluşmaktadır. SOME Eğitimine BTK Akademi Online Eğitim Platformu üzerinden ulaşılabilir.

Siber güvenlik alanında uzman personel yetiştirilmesi, yani kapasite inşası adına siber güvenlik tatbikatları ve yarışmalar, sektör spesifik eğitimler gibi çalışmaların yanı sıra BTK-USOM tarafından toplumun değişik kesimlerine bilgilendirme ve farkındalık eğitimleri verilmektedir. Bu eğitimlere örnek olarak; Huzurevi Yaşlı Bakım ve Rehabilitasyon Merkezi Siber Güvenlik Farkındalık Eğitimi (14 Eylül 2022), Üniversitelerin Bilgi İşlem Daire Başkanları ve SOME Yöneticileri Siber Güvenlik Farkındalık Eğitimi (20-21 Aralık 2022), Hava Kuvvetleri Komutanlığı FETİH Siber Talimhane Eğitimi (Nisan 2023), Görme Engelliler Rehabilitasyon Merkezi Siber Güvenlik Farkındalık Eğitimi (2023) olarak verilebilir.

Güvenli İnternet Çalışmaları

İnternetin güvenli ve bilinçli kullanımı konusunda ise BTK tarafından;

- İnternetin doğru ve güvenli kullanımı konusundaki farkındalığı artırmak için “Güvenli İnternet Merkezi” kurulmuş, “Güvenli İnternet Bilgi Destek Hattı” faaliyete geçirilmiş ve “Güvenli Web” İnternet sayfası yayına alınmıştır.
- Oluşturulan 'ALO 141 Güvenli İnternet Bilgi Destek Hattı' ile dijital ortamlarda yaşanan sorunlara ilişkin destek sağlanmakta olup geçen yıl 70 binden fazla çağrıya cevap verilmiştir.

- Öte yandan; Aile ve Sosyal Hizmetler Bakanlığı, Millî Eğitim Bakanlığı, Sağlık Bakanlığı, Gençlik ve Spor Bakanlığı ve Erişim Sağlayıcılar Birliği ile geçtiğimiz süreçte güvenli İnternet kullanımına ilişkin çeşitli konularda protokol imzalanarak öğrenci, öğretmen ve velilerle birlikte eğitimcilere yönelik eğitimler, seminerler düzenlenmektedir.
- Eğitimlerin sürekliliğinin sağlanması ve daha geniş kitlelere ulaşılabilmesi amacıyla diğer kamu kurum ve kuruluşlarıyla ve sivil toplum kuruluşlarıyla düzenli olarak eğitici eğitimi projeleri gerçekleştirilmektedir.
- İnternetin bilinçli ve güvenli kullanımına ilişkin öğrenci, öğretmen ve ebeveynlere yönelik olarak Güvenli İnternet Merkezinin kurulduğu 2017 yılından beri 1300’den fazla eğitim/seminer düzenlenmiş ve yaklaşık 210 bin kişiye ulaşılmıştır.
 - 2023 yılında yüz yüze ve çevrim içi olmak üzere 168 eğitim düzenlenmiş ve 25 binden fazla kişiye ulaşılmıştır.
 - 2024 yılında Ağustos ayı itibarıyla 110 eğitim düzenlenmiş ve 22 binden fazla kişiye ulaşılmıştır. Bu eğitimlerde Güvenli İnternet Hizmetinin de tanıtımı yapılmıştır.
- Güvenli İnternet Hizmetine (GİH) ilişkin olarak Bağımlıkla Mücadele Yüksek Kurulu’nun 26.01.2021 tarihli ve 2021/1 sayılı kararı doğrultusunda alınan Bilgi Teknolojileri ve İletişim Kurulu’nun 08.06.2021 tarihli ve 2021/DK-İD/152 sayılı kararı ile “Yeni aboneliklerde aksi abone tarafından talep edilmedikçe, abonenin güvenli İnternet aile profilinden ücretsiz olarak istifade edeceği şekilde abonelik sözleşmesi tesis edilmesi” hüküm altına alınmıştır. Güvenli İnternet Hizmeti (GİH) kullanıcı abone sayısı 2024 yılı Ağustos ayı itibarıyla 47,5 milyondur.
- Ayrıca; ülke çapında çocukların ve gençlerin yeni teknolojilerle doğrudan etkileşimlerini sağlayarak, teknolojinin, İnternetin doğru kullanılmasını ve bu konuda bilinçlenmelerini sağlamak amacıyla hizmet veren gezici Güvenli İnternet Tırı ile 2018 yılından beri 200 okul ziyaret edilerek 80 binden fazla öğrenciye ulaşılmıştır. Güvenli İnternet Tırı ile okullarda tanıtım etkinlikleri gerçekleştirilmeye devam edilmektedir.
- Bununla birlikte; Bilgi Teknolojileri ve İletişim Kurumu tarafından bilinçli ve güvenli İnternet kullanımı konusunda farkındalık oluşturmak amacıyla her yıl Şubat ayında

düzenlenen 'Güvenli İnternet Günü' etkinliği 12-13 Şubat 2024 tarihlerinde 'Hep birlikte daha iyi bir İnternete' temasıyla BTK Merkez Yerleşkesi'nde gerçekleştirilmiştir. Bu kapsamda, BTK'ya davet edilen ortaokul ve lise öğrencileri ile katılımcılara, güvenli ve bilinçli İnternet kullanımı, İnternet yardım merkezi, İnternet destek hattı, siber zorbalık, siber saldırı, ebeveyn ve çocuklar için doğru İnternet kullanımı gibi konularda bilgilendirmeler gerçekleştirilmiştir. Ayrıca öğrenciler Güvenli İnternet Atölyeleri'ni ziyaret ederek, İnternetin bilinçli ve güvenli kullanımına yönelik düzenlenen eğitim ve yarışmalara katılmışlardır.

- İnternetin ve teknolojinin bilinçli ve güvenli kullanımına yönelik bilinçlendirme ve farkındalık oluşturma çalışmaları kapsamında Kurumumuz tarafından oluşturulan guvenliweb.org.tr, guvenlicocuk.org.tr, guvenlioyuna.org.tr, guvenlinet.org.tr ve internetyardim.org.tr İnternet siteleri bulunmaktadır.
- BTK proje yürütücülüğünde ve koordinasyonunda, Millî Eğitim Bakanlığı (MEB) ile iş birliği içerisinde yurt çapında ortaokul ve lise öğrencileri ile ebeveynlere ve eğitimcilere yönelik olarak İnternetin bilinçli ve güvenli kullanımı saha çalışmaları gerçekleştirilmektedir.
 - Türkiye'deki çocukların ve ebeveynlerin bilinçli ve güvenli İnternet kullanım, deneyim ve alışkanlıklarına yönelik 10.475 öğrenci ve bunların ebeveyni olan 10.475 ebeveyn ile saha çalışması yapılmış ve rapor hâline getirilmiştir. Rapor <https://www.guvenliweb.org.tr/dosya/slz6Q.pdf> adresinden erişilmektedir.
 - Türkiye'deki Ortaokul ve Lise Öğrencilerinin Dijital Oyun Oynama Alışkanlıklarına yönelik 11.891 öğrenci ve lise düzeyinde ise 8.493 olmak üzere toplam 20.384 öğrencinin katılımı ile saha çalışması gerçekleştirilmiş ve rapor hâline getirilmiştir. Rapor <https://www.guvenliweb.org.tr/dosya/msSgS.pdf> adresinden erişilmektedir.
- 2023 yılında yayın hayatına başlayan Bilgi Teknolojileri ve İletişim Dergisi (BTK Dergi), Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yayımlanan hakemli ve akademik dergidir. Dergide, Türkçe ve İngilizce olmak üzere; makale, çeviri, kitap tanıtımı ve araştırma raporları yayımlanmaktadır. Dergide; Yeni Medya ve İletişim, Siber Güvenlik, Haberleşme Teknolojileri, Yapay Zekâ, Bilgi Toplumu, Bilişim

Hukuku, Nesnelerin İnterneti, Büyük Veri, Dijital Mahremiyet, Blok Zinciri Teknolojisi, Dijitalleşme ve Toplum konularındaki çalışmalara yer verilmektedir.

- Çocukların ve Gençlerin Çevrimiçi Ortamda Korunmasına Yönelik Strateji Planı hazırlanmıştır. Strateji Belgesi 7 amaç ve 28 hedeften oluşmaktadır.

BTK Akademi⁹⁴

Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) bilimsel, teknolojik ve sürekli kendini yenileyen eğitim anlayışı ile kuruma, sektöre ve ülkemize katkı sağlayacak alanında öncü, tanınmış, güvenilir ve saygın bir eğitim merkezi oluşturmak maksadıyla 2017 yılında kurulmuştur.

BTK Akademi, BTK'nın alandaki deneyimi ile düzenleyici ve denetleyici rolüyle edindiği birikimi tüm paydaşlarına aktarmayı, sertifikasyon eğitimleri ile sektörün ihtiyaç duyduğu yetkin insan kaynağının artırılmasına katkıda bulunmayı amaç edinmiştir.

BTK Akademi, içinde bulunduğumuz yüzyılın teknolojik gelişmeleriyle değişen eğitim yöntem ve metotlarına uygun bir şekilde; bilgi ve iletişim teknolojileri alanındaki bilgiyi halka arz etmeyi, bu teknolojinin bilinçli ve etkin kullanılmasına yönelik bilinçlendirme çalışmaları yoluyla, başta genç ve çocuklar olmak üzere toplumun her kesiminde farkındalığı artırmayı, düzenlediği sınıf içi ve çevrimiçi eğitim sertifika programlarıyla, kamu ve özel sektörün ihtiyacı olan kaliteli iş gücünün üretilmesine katkı sağlamayı, ulusal ve uluslararası kurum, kuruluş ve üniversitelerle iş birliği yaparak bilginin yönetimi ve aktarımında söz sahibi olmayı, teknoloji dünyasının güncel bilgisini kendini sürekli yenileyen eğitim anlayışıyla halka aktarmayı amaçlayan bir eğitim merkezidir.

Özellikle bilgi teknolojileri alanında oluşturulan dijital eğitim portalı ile tüm vatandaşlarımıza ulaşılması hedeflenmektedir. Çevrimiçi eğitimlerin yanı sıra gerçekleştirdiği sınıf içi eğitimlerle de sektöre yönelik konularda eğitim almak isteyen her kesimin mesleki ve teknik ihtiyaçlarını mekân ve zamandan bağımsız olarak karşılamaktadır.

Ayrıca, BTK "Açık Kaynak İçerik Üretme Projesi" (<http://acikkaynak.gim.org.tr>) kapsamında; "Dijital Okuryazarlık: Metodolojiler, Uygulamalar ve Öneriler" ile "Dijital Oyunlar:

⁹⁴ BTK Akademi. <https://www.btkakademi.gov.tr/portal/public/hakkimizda>

Araçlar, Metodolojiler, Uygulamalar ve Öneriler” (2 cilt) isimli açık kaynak kitap serisi üretmiş ve tüm kamuoyuna açmıştır.

*Siber Ay*⁹⁵

Siberay, Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı bünyesinde Ocak 2020'de teknoloji bağımlılığını ve siber zorbalığın önüne geçmek, güvenli ve bilinçli İnternet kullanımını sağlamak amacıyla; maddi gelir hedeflemeden, bağış veya kazanç kaygısı gütmeyen kurulmuş bir kamuoyunu bilgilendirme platformudur. Pek çok sanatçı, sporcu ve bilim insanı da bu platformu desteklemekte ve uyarıcı kliplerde rol almakta ve bilgiler vermektedirler.

Ankara Emniyet Müdürlüğü Çocuk Şube Müdürlüğü bünyesinde uzman pedagoglarla, Bilgi Teknolojileri ve İletişim Kurumu (BTK), İçişleri Bakanlığı'na bağlı çeşitli Daire Başkanlıkları, Millî Eğitim Bakanlığı'na bağlı Talim ve Terbiye Kurulu Başkanlığı ve Gazi Üniversitesi ile iş birliğiyle çalışmalar devam etmektedir. Bu kapsamda tüm üniversitelerde öğrenci kulüplerinin açılması, ortak etkinlikler düzenlenmesi, kamuoyu farkındalığının ve dayanıklılığının artırılması hedeflenmektedir.

*Dezenformasyonla Mücadele Merkezi (DMM)*⁹⁶

Türkiye Cumhuriyeti İletişim Başkanlığı bünyesinde, yalan haberle mücadeleye yönelik olarak 2022 yılı Ağustos ayında oluşturulan birimdir. Yurt içi ve yurt dışı kaynaklı algı operasyonlarının, komplo teorilerinin ve manipölasyon girişimlerinin önemli bir parçası olan dezenformasyonun erken aşamada tespitini ve eş zamanlı olarak ele alınmasını hedeflemektedir.

*Siber Vatan*⁹⁷

Siber Vatan Programının ülke geneline Kalkınma Ajansları vasıtasıyla yaygınlaştırılması ve siber güvenlik alanında nitelikli insan kaynağının yetiştirilerek genç istihdamının artırılması amacıyla Kalkınma Ajansları Siber Vatan Programı geliştirilmiştir. Kalkınma Ajansları Siber Vatan Programı sadece eğitim programı olmayıp eğitimlerin yanında teknik geziler, usta çırak buluşmaları, konferanslar ve seminerler, mentor firmalar ile birebir çalışmalar, Bayrağı Yakala

⁹⁵ Siber Ay. <https://www.siberay.com/hakkimizda>

⁹⁶ Dezenformasyonla Mücadele Merkezi, T.C. İletişim Başkanlığı. <https://www.dmm.gov.tr/>

⁹⁷ Siber Vatan, Türkiye Kalkınma Ajansı. <https://www.sibervatan.org/kalkinma-ajanslari-sibervatan-programi>

(Capture the Flag - CTF) yarışmaları ile motivasyon oluşturulmakta ve inovatif fikirleri tetikleyen düşünme yapısının oluşmasına ve girişimcilik ruhunun gelişimine destek sağlanmaktadır.

Ayrıca, Bilgi Güvenliği Derneğinin de destekleyicileri arasında olduğu ülkemizde ilk kez düzenlenen ve çoğu konuşmacının üst düzey dernek yöneticisi olduğu “*Siber Vatan ve Savunma Ulusal Çalıştayı*” 31 Ekim 2022 Pazartesi günü ATO Meclis Salonu’nda geniş bir katılım ile gerçekleştirilmiştir.

Siber Güvenlik Eğitim Portalı

Portal, TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü (SGE) tarafından yürütülen Siber Güvenlik Eğitim ve Araştırma Merkezi Projesi - Siber Güvenlik Eğitim Altyapısı iş paketi kapsamında hayata geçirilmiştir.

Siber Güvenlik Eğitim Portalı ile; toplumun siber güvenlik ile ilgili konularda farkındalığının artırılması, yükseköğretim öğrencilerinin siber güvenlik teknolojileri konusunda teknik bilgi edinebilmeleri, siber güvenlik alanında çalışan uzmanların yetkinliklerinin geliştirilmesi için ihtiyaç duyulan eğitimlerin çevrim içi olarak sunulması planlanmıştır.⁹⁸

Güncelliğini yitirdiği gözlemlenen söz konusu portal, işlev ve içerik yönleriyle de gelişime açık bir görüntü arz etmektedir.

BÜSİBER⁹⁹

BÜSİBER (Boğaziçi Üniversitesi Yönetim Bilişim Sistemi Siber Güvenlik Merkezi) İstanbul Kalkınma Ajansı desteğiyle Bilgi Sistemleri Araştırma Merkezi bünyesinde, siber güvenliğin gerektirdiği uzmanlık ve odaklanmayı sağlamak amaçlı 1 Aralık 2016 tarihinde kurulmuştur.

Akademik bakış açısıyla siber güvenlik ve kişisel verilerin korunması konusunda bir farkındalık oluşturmak ve ülkemizde bu alanda ihtiyaç duyulan yetişmiş insan kaynağı açığını kapatmaya destek olmak hedeflenmektedir. Üniversite öğrencileri için ücretsiz siber kamplar

⁹⁸ Siber Akademi, TÜBİTAK. <https://siberakademi.bilgem.tubitak.gov.tr/mod/page/view.php?id=10>

⁹⁹ BÜSİBER, Boğaziçi Üniversitesi <https://cybersec.bogazici.edu.tr/tr/hakkimizda>

düzenlenmekte, siber güvenlik hizmetleriyle kamu ve özel sektörde siber güvenlik direncinin artırılması amaçlanmaktadır.

GAZİ AI CENTER

Gazi Üniversitesi Büyük Veri ve Yapay Zekâ Güvenliği Mahremiyeti Uygulama ve Araştırma Merkezi kısaca *Gazi AI Center*, ulusal stratejileri desteklemek amacıyla 2021 yılında kurulmuş olup, yapay zekâ, büyük veri ve siber güvenlik ile kişisel verilerin korunması konusunda bir farkındalık oluşturmak ve ülkemizde bu alanda ihtiyaç duyulan yetişmiş insan kaynağı açığını kapatmaya destek olmak maksadıyla hizmet vermektedir. Bu merkez, üniversite öğrencileri için ücretsiz eğitimler vermekte, etkinlikler düzenlemekte, açık kaynak içerik üretmekte, siber güvenlik hizmetleriyle kamu ve özel sektörde siber güvenlik ve yapay zekâ çalışmaları ile dayanıklılığının artırılmasına katkılar sağlamaktadır.

GlobalVodafone Vakfı Dijital Okuryazarlık Eğitimi

Vodafone şirketinin, faaliyet gösterdiği ülkelerde kurduğu vakıflar aracılığıyla toplumsal ve ekonomik gelişime katkıda bulunmayı hedefleyen GlobalVodafone Vakfı, Avrupa genelinde dijital okuryazarlık becerilerinin artırılmasına yönelik bir eğitim girişimi başlatmıştır. Bu çerçevede Türkiye ile birlikte Almanya, Macaristan, Hollanda, Portekiz, Romanya ve İspanya'nın da destek verdiği bir ortak girişimle, öğrencilerin ve eğitimcilerin dijital teknolojileri yenilikçi, yaratıcı ve özgüvenli bir biçimde kullanmalarını sağlamak amaçlanmıştır.¹⁰⁰

Dijital Okuryazar Türkiye (DOT)

MMA Türkiye (Mobil Mecralar Araştırma ve Pazarlama Derneği) tarafından tasarlanan projenin amacı özellikle 65 yaş üstü bireylerin İnternet kullanımı, çevrimiçi alışveriş, dijital bankacılık işlemleri (hesap açma, birikim yapma, para transferi gerçekleştirme, çevrimiçi ödemeler vs.), e-devlet erişimleri gibi dijital süreçleri kolaylıkla yönetebilmesini sağlamaktır. Akbank, Garanti BBVA, Türkiye İş Bankası ve Yapı Kredi Bankası'nın sponsorluğunda hayata geçirilmiştir.

Geleceğin Ekranı Projesi

¹⁰⁰ Türkiye Vodafone Vakfı. <https://turkiyevodafonevakfi.org.tr/vodafone-vakfinin-7-avrupa-ulkelerini-kapsayan-dijital-egitim-girisimine-turkiye-de-katildi/>

Proje, dijital vatandaşlık, dijital güvenlik ve dijital okuryazarlık kavramlarının toplumun geneline yayılmasını ve genç nesillerin bilinçli içerik tüketim alışkanlığı kazanmasını hedeflemektedir. Netflix, Milletlerarası Ticaret Odası (ICC) Türkiye Millî Komitesi ve Habitat Derneği ortaklığıyla yürütülen proje kapsamında, ebeveyn ve öğretmen buluşmaları gerçekleştirilmektedir. Ebeveyn Buluşmalarında dijital ebeveynlik kavramının etkili ve interaktif bir şekilde öğretilmesi amaçlanırken, Öğretmen Buluşmalarında çocuk gelişimi, dijital denge, dijital eğitim ve hukuk gibi konulara değinilmektedir. Bu buluşmalara ek olarak, proje kapsamında düzenli olarak bilgilendirici *podcastler* paylaşılmakta, Netflix Haber Merkezi İçerikleri yaygınlaştırılmakta ve her yıl Dijital Güvenlik Zirvesi düzenlenmektedir.¹⁰¹

Dijitalde Hayat Kolay

Dijitalde Hayat Kolay Projesi, sürdürülebilir ekonomik büyüme ve toplumsal kalkınma için temel itici güç olan bilişim teknolojilerinin herkes için erişilebilir olması hedefiyle yola çıkmıştır. Türkiye Odalar ve Borsalar Birliği (TOBB), Birleşmiş Milletler Kalkınma Programı (UNDP), Habitat Derneği ve Türk Telekom ortaklığıyla hayata geçirilen proje, kapsayıcı iş modellerine Türkiye’den örnek gösterilen ilk proje olma özelliğine sahiptir.

Kadınların bilgi ve iletişim teknolojileri, e-hizmetler ve e-ticaret gibi konularda bilgi birikimlerini geliştirmeyi ve bu sayede iş dünyasına katılımlarını teşvik etmeyi amaçlayan proje kapsamında, dijital okuryazarlık ve dijital pazarlama eğitimleri verilmektedir. Dijital pazarlama eğitimini tamamlayan üretici ve girişimci kadınlar, projenin ikinci aşaması olan Tasarım Odaklı Düşünme Atölyesi’ne kabul edilmektedir. Son aşamada, esnaf ve esnaf muafiyeti bulunan üretici ve girişimci kadınlara işlerini geliştirmeleri için mentorluk ve hibe desteği sağlanmaktadır.¹⁰²

Bir Milyon İstihdam Projesi¹⁰³

1 Milyon İstihdam Projesi, T.C. Hazine ve Maliye Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü tarafından yürütülmektedir. Projenin amacı, Türkiye’de iş arayan gençlerle, işverenleri bir araya getirerek istihdam sürecini hızlandırmak ve kolaylaştırmaktır. Proje, özellikle bilişim ve

¹⁰¹ Habitat Derneği, Geleceğin Ekranı: <https://habitatdernegi.org/dijital-donusum/gelecegin-ekrani/>

¹⁰² Habitat Derneği, Dijitalde Hayat Kolay: <https://habitatdernegi.org/kapsayici-ve-surdurulebilir-buyume/dijitalde-hayat-kolay/>

¹⁰³ 1 Milyon İstihdam Projesi: <https://1milyonistihdam.hmb.gov.tr/proje-hakkinda>

yazılım alanında yetenekli gençlere yönelik olup, bu alanlardaki açık iş pozisyonlarının doldurulması hedeflenmektedir.

Proje kapsamında, gençlerin kendilerini geliştirebilmeleri için çeşitli eğitim programları ve sertifika kursları sunulmakta ve bu sayede gençlerin iş gücü piyasasına daha donanımlı bir şekilde katılmaları sağlanmaktadır. Ayrıca, proje platformu üzerinden gençler ve işverenler arasında doğrudan iletişim kurulması ve iş görüşmelerinin organize edilmesi gibi imkânlar sunulmaktadır.

3.5. Siber Olayların ve Siber Olaylara Müdahalenin Dönüşümü

3.5.1. Ulusal Siber Olaylara Müdahale (USOM ve SOME'ler)¹⁰⁴

Ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel siber saldırı ve olayların etkilerinin azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) 2013 yılında kurulmuştur.

Ulusal SOME görevindeki USOM'un görev ve yetkileri aşağıdaki gibidir:

- Siber olaylara müdahale konusunda ulusal ve uluslararası koordinasyon çalışmaları yürütmek,
- Siber tehditlerle ilgili olarak alarm, uyarı, duyuru faaliyetleri yürütmek, yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesini sağlamak,
- Siber güvenlik olaylarına maruz kalan kritik altyapılara yönelik koruyucu tedbirlerin alınması konusunda koordinasyon sağlamak,
- Çalışmaları esnasında, konusu suç teşkil eden veriler ile karşılaşması hâlinde, adli makamlar ve kolluk kuvvetleri ile koordinasyon içinde hareket etmek,
- Güvenli bir iletişim kanalı üzerinden sektörel ve kurumsal SOME'ler ile bilgi paylaşımı yapmak, acil olarak alınması gereken tedbirleri bu iletişim kanalı vasıtasıyla çevrim içi paylaşmak,

¹⁰⁴ BTK USOM. <https://www.usom.gov.tr/hakkimizda>

- Zararlı yazılımları analiz etmek veya ettirmek,
- 7/24 esasına göre çalışmak,

Siber güvenlik olayını tespit etmesi hâlinde ilgililere bilgi vermesi, ilgililer tarafından talep edilmesi hâlinde uzaktan müdahale desteği sağlaması ve talep hâlinde kritik altyapılarda ortaya çıkan siber güvenlik zafiyetlerinin giderilmesi için yerinde müdahale desteği sağlaması, iş birliği ve eğitim faaliyetleri USOM'un diğer görevleri arasındadır.

Ayrıca UAB koordinasyonunda hazırlanan 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulmuştur. USOM ve SOME'ler siber olayları bertaraf etmede, oluşması muhtemel zararları önlemede veya azaltmada, siber olay yönetiminin ulusal düzeyde koordinasyon ve iş birliği içerisinde gerçekleştirilmesinde hayati önemi olan yapılardır.

Siber olaylara müdahale konusunda ulusal ve uluslararası koordinasyon çalışmaları 7/24 çalışma esasına göre USOM tarafından yürütülmekte, tespit edilen siber tehditlerle ilgili olarak ilgili taraflara ya da ülke çapında alarm, uyarı ve duyurular yaparak yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesini sağlamaktadır. Koruyucu tedbirlerin alınmasına ek olarak konusu suç teşkil eden bulgular ile karşılaşılması hâlinde adli makamlar ve kolluk kuvvetleri ile koordinasyon içerisinde hareket etmektedir.

Bu maksatla USOM tarafından hazırlanmış SOME İletişim Portalı (SİP) üzerinden ülkemiz siber güvenlik organizasyonunda yer alan Sektörel ve Kurumsal SOME'lere güvenlik bildirimleri, alarm, duyuru, mesaj ve ihbarlar gönderilmektedir. Aynı zamanda SOME'ler de SİP kanalı üzerinden tespit ettikleri ihbar ve olay bildirimlerini USOM'a iletebilmektedir. Gelen ihbar veya olay bildirimlerine konusuna göre inceleme ve değerlendirmeler yapılarak gerekli işlem yapılmakta, zararlı yazılım analiz çalışmalarında tespit edilen bulgular ilgililer ile paylaşılmaktadır.

SİP üzerinde Ağustos 2024 tarihi itibarıyla 2287 SOME ve 7846 SOME personeli kayıtlıdır. 2017 yılından bugüne kadar 30 binin üzerinde siber güvenlik ihbarı ilgili kurum ve kuruluşlara bildirilmiş olup aynı şekilde SOME'lerden USOM'a 38 binin üzerinde siber güvenlik bildirimi yapılmıştır.

KULE uygulaması ile ihbar, olay ve çalışma süreçleri yönetilebilmektedir. USOM personeli, bu platform üzerinden ihbarları, alınacak önlemleri ve analizleri planlayabilmekte, takip edebilmekte ve yönetebilmektedir. Aynı zamanda çalışma süreçlerini planlayabilmekte, ilerlemelerini takip edebilmekte ve çalışma programlarını düzenleyebilmektedir.

Öte yandan USOM, ülkemizdeki kamu kurum ve kuruluşları, İnternet servis sağlayıcıları, özel sektör kuruluşları ve diğer İnternet aktörleri ile birlikte etkileşim ve iş birliğini artırıcı görevler yerine getirmektedir. Siber güvenlik farkındalık faaliyetleri kapsamında Sektörel ve Kurumsal SOME'lere, üniversitelere, siber güvenlik topluluklarına yönelik olarak siber güvenlik eğitimi faaliyetlerinde bulunmakta, ulusal ve uluslararası siber güvenlik tatbikatlarına, konferanslara, çalıştaylara ve toplantılara katılım sağlamaktadır.

Farkındalık kapsamında ayrıca Siber Yıldız, FETİH Siber Talimhane gibi çeşitli etkinlikler ile Siber Kapasite İnşası hedefi doğrultusunda ülkemizin siber güvenlik konusunda ihtiyacı olan uzman personel yetiştirilmesine katkıda bulunmaktadır.

USOM'un, uluslararası CERT organizasyonlarına üyelikleri bulunmakta, uluslararası iş birliği çerçevesinde siber tehditlerin bertaraf edilmesi adına diğer CERT'lerle iş birliği yapılmaktadır.

3.5.2. Yeni Nesil Siber Güvenlik Teknolojilerine Yönelik Ar-Ge Çalışmaları

USOM¹⁰⁵

Gelişen teknolojiler paralelinde yeni nesil siber tehditlerin ve saldırı türlerinin bertaraf edilmesi yoluyla ulusal siber güvenliğin sağlanmasına ilişkin USOM bünyesinde yerli ve millî olarak geliştirilen kabiliyetlerden faydalanılmaktadır.

Siber Güvenlik ve Büyük Veri: Güvenlik için Yenilikçi Çözümler

USOM bünyesindeki Ar-Ge çalışmalarında; büyük veri analitiği ve yönetimi, özellikle risk analizi için önemli bir odak noktası olarak belirlenmiştir. Başta kritik sektörler ve kamu kurumları olmak üzere ülke verilerini korumak, tehditleri tespit etmek ve veri güvenliğini sağlamak için büyük veriyi kullanarak USOM uhdesinde yenilikçi çözümler geliştirilmektedir.

¹⁰⁵ BTK USOM. <https://www.usom.gov.tr/arge>

KASIRGA projesi kapsamında kritik kamu kurumları ile kritik altyapılar olmak üzere ülkenin İnternete açık kaynaklarına ilişkin servis taraması ve hizmet sürekliliğinin sağlanmasına yönelik izleme faaliyetleri gerçekleştirilmektedir. Toplamda 16.7 milyon IP adresinin ve 840 binden fazla kritik alan adının her biri için düzenli olarak yapılan taramalarla servislere ait bilgiler tespit edilebilmektedir.

ATMACA projesi, zafiyeti olan sistemlerin tespiti ve raporlama sürecini otomatikleştirmek, tespit ve raporlama sürelerini asgariye indirmek, elde edilen bilgi birikiminin kurumsal hafızaya katılmasını sağlamak ve zafiyet tarama planlamasını kolaylaştırmak amacıyla geliştirilmiştir.

KUZGUN projesi ile çeşitli siber istihbarat kaynaklarından toplanan veriler analiz edilerek, zararlı bağlantı adresleri tespit edilmekte ve siber tehdit istihbarat çalışmaları kapsamında yürütülen süreçler işletilmektedir.

Siber Güvenlik ve Yapay Zekâ: Zararlı Aktivitelerin Tespiti için İnovasyon

Siber güvenlik alanında, USOM bünyesindeki Ar-Ge çalışmalarında yapay zekâ teknolojileri zararlı aktivitelerin tespiti için kullanılmakta ve bu konuya büyük önem verilmektedir. Zararlı aktiviteler, günümüzde hızla gelişen siber tehditler arasında yer almaktadır. Bu aktiviteler, kötü niyetli kişiler veya gruplar tarafından ağlara, sistemlere veya kullanıcılara zarar vermek, veri sızdırmak veya hizmet kesintileri oluşturmak amacıyla gerçekleştirilmektedir.

USOM uhdesinde yapay zekâ teknolojileri kullanılarak zararlı aktivitelerin tespiti için yenilikçi çözümler geliştirilmektedir.

Makine öğrenmesi ve veri analitiği teknikleri, büyük veri setleri üzerinde eğitilerek zararlı aktivitelerin belirli davranış kalıpları veya özellikler temelinde tanımlanmasına yardımcı olmaktadır. Yapay zekâ algoritmaları, sürekli olarak güncellenerek ve yeni tehditlerin tanımlanmasıyla beslenerek, zararlı aktiviteleri saptamak ve bunlara karşı etkili bir savunma mekanizması oluşturmak için kullanılmaktadır.

AZAD projesi kapsamında doğal dil işleme ve yapay öğrenme teknikleriyle Türkiye'deki kullanıcıları hedef alan ortalama adresleri faaliyete geçmeden önce veya geçtiği anda tespit edilip engellenmesi sağlanmaktadır. AZAD projesi ile günde ortalama 1500'den fazla zararlı alan adı tespiti yapılmaktadır.

Zararlı Yazılım Analizi: Tehditlerin Tespiti ve Etkisiz Hâle Getirme

Zararlı yazılımlar, bilişim sistemlerine sızarak veri hırsızlığı, sistem bozulması veya yetkisiz erişim gibi zararlı etkileri gerçekleştiren kötü amaçlı yazılımlardır. Analiz süreçlerinde, zararlı yazılım örnekleri güvenli bir ortamda incelenir, davranış analizleri yapılır ve zararlı aktivitelerin tespiti için veri analizi teknikleri kullanılmaktadır.

USOM zararlı yazılım analizi laboratuvarı da siber güvenlikte zararlı yazılım tehditlerine karşı mücadelede etkin ve önemli bir rol oynamaktadır. Bu zararlı yazılım analizi laboratuvarı, sürekli olarak güncellenen veri tabanları ve tehdit istihbaratıyla desteklenerek, hızlı ve etkili bir şekilde zararlı yazılım tehditlerine karşı koruma sağlamak için gerekli çalışmalar yapılmaktadır.

AVCI projesi kapsamında zararlı yazılım bulaşmış sistemlerin ve komuta kontrol merkezlerinin tespiti gerçekleştirilmektedir.

TÜBİTAK¹⁰⁶

Siber güvenlik konusu, 2021 yılında Bilim Teknoloji ve Yenilik Kurulu (BTYK) tarafından yayımlanan Siber Güvenlik Teknoloji Yol Haritasının (TYH)¹⁰⁷ belirlediği istikametle uyumlu olarak, TÜBİTAK 2024-2025 dönemi öncelikli Ar-Ge ve yenilik çalışma konularından biridir. Bu maksatla geliştirilmesi hedeflenen teknoloji ve kabiliyetler Ar-Ge projeleri olarak ele alınacaktır.

Yeni nesil siber tehdit ve saldırılara karşı ülkemizi daha dayanıklı ve dirençli kılacak söz konusu çalışmalar, 12 teknolojik hedef ve 10 öncelikli sektörel alan şeklinde iki boyutlu ele alınarak düzenlenmiş ve çalışmalara dâhil edilmiştir. Konuya ilişkin TÜBİTAK tarafından duyurulan¹⁰⁸ öncelikli çalışma alanları şu şekilde sıralanmaktadır.

Teknolojik Hedefler

- Temel ağ ve iletişim güvenliği (5G, SDN, NFV dâhil)
 - Ağ anahtarı, kablolu / kablosuz yönlendirici
 - Derin paket inceleme altyapısı

¹⁰⁶ TÜBİTAK. <https://tubitak.gov.tr/tr/kurumsal/icerik-politikalar>

¹⁰⁷ T.C. Cumhurbaşkanlığı Bilim, Teknoloji ve Yenilik Politikaları Kurulu Siber Güvenlik Teknoloji Yol Haritası, Ekim 2021

¹⁰⁸ TÜBİTAK 2024-2025 Ar-Ge ve Yenilik Konu Başlıkları, Versiyon: 22.01.2024

- Uygulama katmanı destekli Web/VoIP/IoT/DB
 - İleri seviye veri sızıntısı önleme
 - Fidyeye yazılımları önleme
 - Güvenli haberleşme ile 5G ve ötesi için (SDN dâhil) güvenlik çözümleri
- Ağ ortamındaki cihazların kimlik yönetimi
 - Ağ cihazlarında yetki yönetimi ve kimlik doğrulama
- Kurumsal ağlarda BT sistemleri güvenliği
 - Ağ seviyesinde otomatik önlem ve güvenlik çözümleri orkestrasyonu
 - Dağıtık güvenlik yönetimi
- OT, IoT cihazlarının güvenliği
 - OT, IoT cihazlarının ağ yönetimi ve siber saldırıları önleme
 - Uygulama katmanında ara haberleşme protokolleri güvenlik kontrol modülü
- Otonom hareketli sistemler güvenliği
 - Otonom hareketli sistemler için siber saldırı önleme
- Son kullanıcı güvenliği
 - Son kullanıcı cihazları zararlı yazılım, oltalama, veri kaçağı önleme
 - EDR ve tarayıcı izolasyonu
 - Gerçek dışı çoklu ortam içeriklerin tespit edilebilmesi ve önlenmesi
- TEE destekli güvenilir işletim sistemi
 - TEE destekleyen güvenilir işletim sistemi
 - TEE kullanılan mobil cihaz güvenlik çözümleri
- Uygulama güvenliği

- Kod güvenlik analiz ve test teknolojileri
- Uygulamaların zafiyet yönetimi
- Bulut güvenliği
 - Bulut ortamındaki verilerin, güvenliği/mahremiyeti ile güvenli entegrasyonu
 - Bulut altyapılarından faydalanmak için bulut tabanlı siber güvenlik teknolojileri
- Kuantum/kuantum sonrası kriptografi
 - Kuantum kriptografi teknolojileri
 - Kuantum sonrası kriptografi teknolojileri
 - Açık kaynak kriptografik yazılımların güvenlik açıklarının tespiti
- Dijital adli analiz
 - Olay müdahale (DFIR) teknolojileri

Öncelikli Sektörel Uygulamalar

- 5G ve ötesi haberleşme teknolojileri, IoT protokolleri ve baz istasyonları için yerli siber güvenlik teknolojileri ve ürünleri
 - 5G ve ötesi için fiziksel katman güvenliği
 - 5G ve ötesi, IoT ve baz istasyonları için siber güvenlik (SDN/NFV tabanlı güvenlik ve SDN/NFV güvenliği)
- Akıllı üretim sistemlerinde ağ trafiğinin yönetimi, güvenli haberleşme, siber saldırı önleme teknolojileri
 - Akıllı üretim sis. ağ trafiği yönetimi ve anomali tespiti
 - Akıllı üretim sis. Güvenli haberleşme, itibar sis., veri kaçağı önleme, siber saldırı önleme
- Otomotiv ve Ulaşım sektörleri

- Otomotiv ve Ulaşım için temel güvenlik ürünleri
- Akıllı ve otonom araçlar siber saldırı önleme
- Enerji sektörü
 - Enerji sektörü için saldırı önleme, veri şifreleme, veri kaçağı önleme
- Kamu ihtiyaçlarına yönelik siber güvenlik çözümleri
 - Kamu için güvenlik duvarı, saldırı tespit, veri kaçağı önleme, vb.
 - Kamuda kullanılan millî işletim sis. güvenliğini artırıcı çözümler
- Kamu ve özel sektör verileri için güvenli bulut teknolojileri ve ürünleri
 - Kamu ve özel sektör verilerinin ve servisleri için bulut mimarilerinde güvenlik
 - Eğitim sektörü için çevrim içi eğitim sis. siber güvenlik ve kriptoloji teknolojileri
- Finans ve Ticaret sektörleri
 - Finansal hizmet sağlayıcılarını ataklara karşı koruyacak bulut tabanlı sistem
 - Finans ve Ticaret sektörleri için veri kaçağını engelleme/mahremiyeti koruma
- Kamuda (kritik kamu hizmetleri, e-devlet ve sağlık) veri şifrelemesinde güvenli kriptografi teknolojilerini kullanan ürünler
 - Kamuda verilerin şifrlenmesinde kuantum ataklara karşı güvenli kriptografi teknolojileri
 - Biyometrik ve çok aşamalı kimlik doğrulama
 - Büyük veri dâhil, veri koruma ve kriptoloji
- E-ticaret ve sanal alışveriş için dijital varlıkların kullanımına yönelik kriptografik çözümler ve bu sistemlere yönelik siber güvenlik çözümleri
 - E-ticaret ve sanal alışverişte dijital varlıklar için kriptografi

- E-ticaret ve sanal alışverişte dijital varlıklar siber güvenlik çözümleri
- Savunma, Havacılık ve Uzay sektörleri
 - Savunma sistemlerinde merkezi olmayan otonom siber güvenlik çözümleri
 - İHA'lar için EPM teknolojileri ve ürünleri
 - Savunma sektörü ürünleri ve uygulamaları için siber güvenlik çözümleri

Mevcut Yetenekler (SGE)

Yukarıda sıralı TÜBİTAK Ar-Ge projeleri haricinde hâlihazırda yine TÜBİTAK Siber Güvenlik Enstitüsü (SGE) tarafından kazanılmış birtakım siber güvenlik yetenekleri de bulunmaktadır. Bu kabiliyetler şu şekilde sıralanabilir.

ORION - Veri Güvenlik Platformu: Ortak yönetim paneli, ağ ve uç nokta ortamlarında kurulan ajan yazılımları ile hassas verilerin olası izinsiz erişimi, kullanımı veya paylaşımı senaryolarına karşı çözüm sunan bir veri kaçağı önleme sistemidir.

DERBENT - Güvenli Uzaktan Erişim Sistemi: Sıkılaştırılmış imaj, güvenlik araçlarının kurulumu (antivirüs, loglama ajanları vb.), kullanıcı ortamı yetkilerinin sınırlandırılması, sadece bu ortama uygun ajan yazılımı kurulumu gibi faaliyetlerin uzaktan erişim yoluyla yapılabilmesine olanak tanıyan bir yazılımdır.

SİBERLAB - Sanal Siber Güvenlik Laboratuvarı: Gelişen siber güvenlik teknolojileri; uygulama odaklı eğitimler, tatbikatlar ve analiz laboratuvarları için kullanıcıları hızlı ve kolay tasarlanabilir sanal ortamlara yönlendirmektedir. Sanal Siber Güvenlik Laboratuvarı Altyapısı ile ağ cihazları ve bilgisayarları içeren topolojiler tasarlanabilmekte ve kullanıcının tasarıma uygun ortamlara tarayıcı üzerinden (herhangi bir kaynak gereksinimi olmadan) hızlı bir şekilde erişebilmesi sağlanmaktadır.

Sanal Siber Güvenlik Laboratuvarı ve Tatbikat Altyapısı; siber güvenlik eğitim, test, tatbikat ve siber güvenlik analizi gibi faaliyetleri bulut üzerinde oluşturulmuş sanal ortamlar üzerinde hızlı, kolay ve düşük maliyetle oluşturabilmektedir.

BOT-SEGEN - Sızma Testi ve Güvenlik Denetimi Platformu: Uygulama ile, derin uzmanlık bilgisine ihtiyaç olmadan tek bir platform üzerinden sızma testlerini ve güvenlik denetimini otomatize ederek zaman ve maliyet tasarrufu sağlanmakta, hâlihazırda bu süreçleri işletmeyen kişi veya kurumların bu faaliyetleri işletebilir seviyeye gelmesi mümkün olmaktadır.

A3 - Adli Analiz Altyapısı: Çeşitli tiplerde telefon, dijital medya gibi cihazların otomatik olarak incelenmesine ve raporlanmasına imkân veren İmaj İnceleme Yazılımı (A3Analyzer) ve imajlarının alınabilmesini sağlayacak İmaj Alma Yazılımından (A3Imager) oluşmaktadır.

MERGE-N Entegre Uç Birim Güvenlik Platformu: MERGE-N, yerli siber güvenlik ürünlerinin tanıtımlarının etkin ve güvenli bir şekilde yapılmasını ve ürünlerin kullanımlarının yaygınlaştırılmasını amaçlayan bir web uygulamasıdır.

3.6. Ulusal Siber Güvenlik Yönetişi

Türkiye'nin, 1991'te bilişim suçlarının 765 sayılı Türk Ceza Kanunu'na ilk defa ithali ile başlayan ve bilahare Ulusal Enformasyon Altyapısı Ana Planının 1999'da oluşturulmasıyla hareketlenen siber güvenlik serüveninde bugüne kadar organizasyonel yapı ve mevzuat başta olmak üzere birçok konuda önemli adımlar atılmış, ekosistemin güçlendirilmesi, siber dayanıklılığın iyileştirilmesi, yerli teknolojilerin güçlendirilmesi ve iş gücünün geliştirilmesi gibi başlıklar altında hatırı sayılır mesafe alınmıştır.

2012 yılında Bakanlar Kurulunca alınan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararın yayınlanması ve ilk Ulusal Siber Güvenlik Stratejisi ve Eylem Planının 2013 yılında yayınlanmasıyla birlikte özellikle son 10 yılda ivme kazanan faaliyetlerin başlıcaları; Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkilerin verilmesi, USOM'un hayata geçirilmesi ve SOME'lerin teşkili, TSK Siber Savunma Komutanlığı ve EGM Siber Suçlar Daire Başkanlığının kurulması olarak sıralanabilir.

Konuya ilişkin olarak Türkiye'deki duruma dair değerlendirme, ulusal siber güvenlik yönetişiminin genel kabul görmüş ve ayrıntıları Ek-4'te tanımlanan 7 ana başlığı çerçevesinde çok boyutlu şekilde ele alınarak aşağıda sunulmuştur.

Bahse konu ana çerçeve ideal kabul edilerek, ülkemizin içerisinde bulunduğu durumun aynı şablonla analiz edilmesinin, eksik ve aksayan yönlerin tespitinde ve boşluk bulunan alanların belirlenmesinde kolaylık sağlayacağı değerlendirilmiştir.

3.6.1. Strateji ve Politikalar

Yasal düzenlemeler - 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar

Bakanlar Kurulunca alınan 11 Haziran 2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20 Ekim 2012 tarihli ve 28447 sayılı Resmî Gazete’de yayımlanarak yürürlüğe girmiştir. Bu karar gereğince Siber Güvenlik Kurulu oluşturulmuş, Ulaştırma Denizcilik ve Haberleşme Bakanlığı’na siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır.

5809 sayılı Elektronik Haberleşme Kanunu’nda 2014 ve 2016 yıllarında yapılan değişiklikler ile Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu’na ulusal düzeyde siber güvenlik görev ve yetkileri verilmiştir.

Siber Güvenlik Stratejisi ve Eylem Planları

Türkiye’de siber güvenlik alanında 2013-2014, 2016-2019 ve 2020-2023 dönemlerini kapsayan strateji belgeleri ve eylem planları hazırlanmış olup, 2024-2028 dönemini kapsayan güncel strateji ve eylem planı 06 Eylül 2024 tarihinde yayımlanmıştır.

Yukarıda da belirtildiği üzere bu alanda ilk devlet stratejisi dokümanı, Ulaştırma Denizcilik ve Haberleşme Bakanlığı koordinesinde hazırlanarak *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014* olarak 2013 yılında yayımlanmıştır.

Söz konusu planda; siber güvenliğin sağlanmasına dair temel ilkeler sıralanmış ve ana başlıklar olarak kamu kurumları ve kritik altyapıların korunması ile saldırı sonrası geri döndürme ve yasal idari/adli yapı konuları ele alınmıştır.

Eylem planı kapsamında ise Siber Güvenlik Kuruluna işlerlik kazandırılması, USOM ve SOME’lerin kurulması, insan kaynağı yetiştirilmesi, altyapının güçlendirilmesi, her düzeydeki

eğitim müfredatına konunun dâhil edilmesi, yerli teknolojiler geliştirilmesi gibi birçok alanda görev ve sorumluluklar tanımlanmıştır¹⁰⁹.

Birinci Siber Güvenlik Eylem Planının izlenmesine, sonuçların kamuoyuyla paylaşılmasına veya ilgili planın bütçesinin belirlenmesine yönelik herhangi bir açıklamaya rastlanılmamıştır. Planın uygulanması kapsamında ise Siber Güvenlik Kuruluna işlerlik kazandırılmış, bu kapsamda birtakım yasal düzenlemeler hayata geçirilmiş, Siber Olaylara Müdahale Ekipleri (SOME) kurulmuş, eğitim ve farkındalık çalışmaları yürütülmüş, insan kaynağının güçlendirilmesine yönelik altyapılar oluşturulmuş, yerli teknolojiler teşvik edilmiştir.

2013-2014 dönemini kapsayan Eylem Planının uygulama süresinin dolmasını müteakip *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2016-2019)* iki ayrı doküman şeklinde yayımlanmıştır. Eylem Planı bölümü, hizmete özel gizlilik derecesinde olduğundan kamuyla paylaşılmamıştır. Ulusal siber güvenlik konusu, amaç ve eylemler bakımından bu strateji dokümanında beş ana başlık altında ele alınmıştır. Bu başlıklar aşağıdaki şekilde sıralanmıştır¹¹⁰.

- Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması
- Siber Suçlarla Mücadele
- Farkındalık ve İnsan Kaynağı Geliştirme
- Siber Güvenlik Ekosisteminin Geliştirilmesi
- Siber Güvenliğin Millî Güvenliğe Entegrasyonu

Eylem planına ilişkin olarak, hangi eylemlerin tamamlandığına, hangilerinde eksiklik bulunduğu dair kamuoyuna bilgilendirme yapılmamıştır.

Siber Güvenlik Strateji dokümanları serisinde son olarak, 2020 ila 2023 yıllarını kapsayan *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)* 29 Aralık 2020 tarihinde

¹⁰⁹ Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2013-2014)

¹¹⁰ Ulusal Siber Güvenlik Stratejisi (2016-2019)

yayımlanmıştır. Doküman, toplam 12 bölümden oluşmakta olup, eylem maddeleri ve eylem tabloları bölümleri hizmete özel gizlilik dereceli olduğundan kamuoyuna açıklanmamıştır.

Dokümanda; 8 stratejik amaç, bu amaçlara ulaşmak için gerçekleştirilmesi planlanan 40 eylem maddesi ve eylem maddelerinin ifası için 75 uygulama adımı bulunduğu belirtilmiştir. Dokümanda yer verilen 8 stratejik amaçtan İleri seviye tehditlerle mücadele kapsamında tanımlanan *Organik Siber Güvenlik Ağı* konsepti ve kaynağı ve hedefi yurt içi olan veri trafiğinin yurt içinde kalması hedefi akılda kalıcı değişiklikler olarak göze çarpmıştır.

Her üç strateji belgesi ve aradan geçen zaman göz önüne alınarak genel bir değerlendirme yapmak gerekirse; Türkiye'nin siber güvenlik eylem planlarının küresel anlamda kabul görmüş pek çok kritere uyum sağladığı ancak özellikle süreklilik, bütçe tahsisi, hedeflerin takibi, insan kaynağının geliştirilmesi ve siber caydırıcılık konularında eksikliklerin olduğu görülmektedir.¹¹¹

Siber Güvenlik Strateji Belgesi ve Uygulama Planı (2024-2028) ise 09 Eylül 2024 tarihli Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

3.6.2. Kural ve Kurumlar

Türkiye'de ulusal siber güvenlik çalışmalarına milat olarak gösterilebilecek 2008 yılından bugüne kadar geçen 15 yıllık zaman zarfında gerek ilgili mevzuatta gerekse teşkilatlanmada önemli gelişmeler yaşanmıştır. Bütün bu gelişmeler arasında başlıcaları şu şekilde sıralanabilir¹¹².

- Bilgisayar Olayları Müdahale Ekibi (TR-BOME)'nin 2006 yılında kurulması
- 2007 yılında 5651 İnternet'te işlenen Suçlarla ilgili kanunun yayımlanması.
- 2008 yılında ilk ulusal siber tatbikatın icrası.
- 2009 yılında çıkarılan 5902 sayılı kanun ile Türkiye'de afet hâllerindeki acil durum yönetimi yetkisinin AFAD'a verilmesi ve aynı kanuna göre afetlerin, teknolojik ve doğal afetler olarak ikiye ayrılması.

¹¹¹ Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi, Hüseyin ÇAKIR, Sündüs ARINMIŞ UZUN, 2021,

¹¹² Duygu Fidancıoğlu, <https://medium.com/cyber-alliance/turkiyenin-siber-guvenlik-tarihi>, 11/09/2023

- 2010 yılında yayınlanan Millî Güvenlik Kurulu Bildirisi'nde siber tehdidin global düzeyde ulaştığı boyut ve bu tehdidin ulusal güvenliğe etkilerinin ele alınması.
- Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonunu sağlamak üzere 2012 yılında Siber Güvenlik Kurulunun oluşturulması.
- 2012 yılında yayınlanan Bakanlar Kurulu kararı ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na başta ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak olmak üzere siber güvenlik alanında görev ve yetkiler verilmesi.
- TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü'nün 2012 yılında kurulması.
- Türk Silahlı Kuvvetleri Siber Savunma Komutanlığı'nın 2012 yılında kurulması.
- BTK bünyesinde 27 Mayıs 2013 tarihinde Ulusal Siber Olaylara Müdahale Merkezinin (USOM) oluşturulması.
- Emniyet Genel Müdürlüğü bünyesinde 2011 yılında kurulmuş olan Bilişim Suçlarıyla Mücadele Daire Başkanlığı'nın 2013 yılında Siber Suçlarla Mücadele Daire Başkanlığına dönüştürülmesi.
- 2013, 2016 ve 2020 yıllarında yayınlanan Ulusal Siber Güvenlik Strateji ve Eylem Planı belgeleri.
- Sektörel Siber Olaylara Müdahale Ekipleri'nin (Sektörel SOME) ve kurumlar bünyesinde de Kurumsal SOME'lerin 2013 yılında kurulması.
- 2014 yılında yayımlanan 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi'nin yayınlanması.

- BTK tarafından 2014 yılında yayımlanan Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği.
- Kamu kurumları arasındaki veri trafiğinin daha güvenli yapılabilmesi amacıyla İnternete kapalı kamuya özel sanal bir ağ olan Kamu Sanal Ağı (KamuNet)’in 2015 yılında kurulması.
- 2016 yılında çıkarılan 6757 sayılı Kanun ile Bilgi Teknolojileri ve İletişim Kurumu’na; “Siber saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alma” yetkisinin verilmesi.
- 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 2016 yılında yayımlanması.
- 2018 yılında yayınlanan 703 sayılı Kanun Hükmünde Kararname ile Siber Güvenlik Kurulu mülga edilerek görev ve yetkilerinin Cumhurbaşkanınca belirlenen kurul veya merciye devredilmesi.
- Bilgi ve İletişim Güvenliğine ilişkin 2019/12 sayılı Cumhurbaşkanlığı Genelgesi.
- Bilgi ve İletişim Güvenliği Rehberi’nin 2020’de yayınlanması.
- 2020 yılında oluşturulan Siber Güvenlik ve İletişim Altyapısı Çalışma Grubu tarafından “bir siber güvenlik çatı mevzuatının oluşturulması” önerisi.
- 2020’de yürürlüğe giren Siber Güvenlik Elemanı (Seviye 5) ulusal meslek standardı.
- Bilgi ve İletişim Güvenliği Denetim Rehberi’nin 2021’de yayınlanması.
- Siber güvenlik alanında yerli sektörün gelişmesini sağlamak amacıyla “Yerli Siber Koordinasyon Grubu”nun 2021 yılında kurulması,

- Bilgi ve İletişim Güvenliğinin Sağlanması Hakkında Yönetmelik Taslağı'nın hazırlanarak 2022 yılında onaya gönderilmesi.
- Mesleki Yeterlilik Kurumu tarafından 2022 yılı içerisinde Etik Hacker (Seviye 5) meslek standardı yayımlanması.
- Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından Ulusal Siber Güvenlik Çalıştayı yapılması,
- Ulusal Siber Güvenlik Yönetişimi Mevzuat Taslağı hazırlıklarına 2023 yılında başlanması.
- EPDK tarafından 2023 yılında yayınlanan Siber Güvenlik Yetkinlik Modeli.

Cumhurbaşkanlığı Hükûmet Sistemine geçiş ile birlikte politika yapılışı sürecine ilişkin birtakım değişiklikler meydana gelmiş, politika belirleme yetkisi Cumhurbaşkanına, politika oluşturma ve geliştirme görevi Politika Kurullarına tevdi edilmiş, söz konusu politikaların uygulanması yetkisi ise Bakanlıklara verilmiştir.

1 sayılı Cumhurbaşkanlığı Kararnamesi ile Dijital Dönüşüm Ofisi'ne "Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek" görevi atanmış, bununla birlikte Ofisin kuruluş teşkilatında yer alan Siber Güvenlik Daire Başkanlığı'na; kamu kurumları ve kritik altyapılar, sahadaki uygulamaları takip, ekosistemi ve iş birliklerini geliştirmek, yerli ve millî siber güvenlik ürünlerinin geliştirilmesi ve yaygınlaştırılması, kritik teknoloji ve bilgi varlıkları ve bilgi güvenliği yönetim sistemi ana başlıklarında görevler tevdi edilmiştir.

Yine aynı Kararname ile Sanayi ve Teknoloji Bakanlığı uhdesinde Millî Teknoloji Genel Müdürlüğü kurulmuş, bahse konu teşkilata, bilgi güvenliği düzeyinin yükseltilmesi, yerli ve millî ürünlerin üretilmesi ve kullanımının yaygınlaştırılması, siber güvenlik ekosisteminin geliştirilmesi başlıklarında bazı görevler verilmiştir.

9 Temmuz 2018 tarihinden itibaren uygulanmaya başlanan Cumhurbaşkanlığı Hükûmet Sisteminin 1 sayılı Cumhurbaşkanlığı Kararnamesi ile Cumhurbaşkanına bağlı çalışan Güvenlik

ve Dış Politikalar Kurulu’na “Siber güvenlik ile ilgili politika ve strateji önerileri geliştirmek” görevi verilmiştir.

On Birinci Kalkınma Planının (2019-2023) “İyi Yönetişim” başlığı altındaki hükme dayanarak Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı’na; siber güvenliğe yönelik düzenlemelerin ve teknik altyapının güçlendirilmesi ile güçlü bir koordinasyon yapısının oluşturulması, hazırlanacak rehberlerle bu konuda kamu kurumlarına yol gösterilmesi, Ulusal Siber Güvenlik Stratejisi’nin güncellenmesi çalışmalarının koordinasyonu, kamu kurumlarında bilgi güvenliği yönetim sistemi kurulması ve denetlenmesine yönelik usul ve esasların belirlenmesi ve kamuda siber güvenliğin koordinasyonunun tek çatı altında toplanarak etkinliğinin artırılması gibi önemli sorumluluklar verilmiştir.

Ayrıca, yukarıda sıralı liste dâhilinde bahsi geçen Yerli Siber Koordinasyon Grubu tarafından hâlihazırda ikinci safha çalışmaları yürütülen çalışmalarda bugüne kadar; “Siber Güvenlik Taksonomisi” geliştirilmiş, Kamuda Siber Güvenlik Ürünlerinin Kullanımının Yaygınlaştırılması hususunda çalıştay yapılmış, Kamu Bilişim Alımları Yönetmeliği yayımlanmış, öncelikli siber güvenlik alanları belirlenmiş ve yerli siber güvenlik sektörü için destek/teşvik mekanizmalarının mevcut durum analizi gerçekleştirilmiştir.

Bu kapsamda Türkiye’nin topyekûn bir siber saldırıyla karşı karşıya kalması ve bunun bir afet seviyesine ulaşması hâlindeki olası kriz sürecinin AFAD tarafından koordine edileceği hususu, ilgili kanunla düzenlenmiştir¹¹³. Ancak bu kriz yönetiminin nasıl yapılacağı, hangi kurumsal yapılanmalar ve süreçler dâhilinde sürdürüleceği konusu net olarak ortaya konmamıştır.

2018 yılında kaldırılan Siber Güvenlik Kuruluna tevdi edilmiş olan yetki, görev ve sorumluluklara dair, Kurul’un mülgası sonrası kısmi atamalar mevcut olsa da tamamı bugüne kadar herhangi bir kuruma veya merciye devredilmemiştir.

Sunulan bilgilerden anlaşıldığı üzere, Türkiye’de siber güvenlik alanında mevzuat oluşturma ve bunu kurumsallaştırma anlamında özellikle son on yıl zarfında önemli adımlar atılmış, gelişmeler yaşanmıştır.

¹¹³ 5902 Sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun, 17/06/2009

Oluşturulan kurumlar tarafından siber güvenliğe ilişkin strateji ve politikalar belirlenmiş, yol haritası ve eylemler tanımlanmıştır. Kurum ve kurallarda önemli mesafe alınmışsa da hâlihazırda eksik bulunan veya aksayan, güncelliğini yitirmiş veya fazlalık olan hususlar tespit edilerek ilerleyen bölümlerde tartışılmıştır.

Türkiye’de siber güvenlik yönetişiminde, merkezi bir otorite bulunmamakla birlikte, siber güvenlik konusundaki ana görev ve sorumlulukların yerine getirilmesinde görevlendirilen; Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı (DDO), Sanayi ve Teknoloji Bakanlığı ve Ulaştırma ve Altyapı Bakanlığı başta olmak üzere çok sayıda kurum ve kuruluş bulunduğu görülmektedir.

3.6.3. Uygulamalar

Türkiye'nin siber güvenlik alanındaki gelişimi, yerli ve millî teknolojilerin geliştirilmesi, uluslararası rekabet gücü yüksek üretim ve siber güvenlik sahasında küresel ve millî atılım hedefleri doğrultusunda ilerlemektedir. Ayrıca, kamu kurumlarında siber güvenlik ürünlerinin kullanımının yaygınlaştırılması, siber güvenlik mevzuatı, yerli siber güvenlik sektörü için destek/teşvik mekanizmalarının mevcut durum analizi gibi konularda çalışmalar yürütülmektedir.

Siber Tatbikatlar

Siber güvenlik alanındaki tedbirler ve uygulamalar, icra edilen ulusal ve uluslararası tatbikatlarla değerlendirmeye tabi tutulmaktadır. Bu anlamda ilk siber güvenlik tatbikatı: TR-BOME koordinatörlüğünde 20–21 Kasım 2008 tarihlerinde 8 kurumun katılımı ile yapılmıştır. Tatbikatta kurumların dış kaynaklı bir siber saldırıya maruz kalmaları durumunda TR-BOME ile iş birliği süreçlerinin kontrol edilmesi amaçlanmıştır.

Ulusal ve uluslararası seviyede siber güvenlik tatbikatlarının gerçekleştirilmesine yönelik faaliyetler sürdürülmektedir. Ulaştırma ve Altyapı Bakanlığı koordinasyonunda kamu kurum ve kuruluşlarımızda nitelik ve yetkinliklerin artırılması ve güncel durumun gözlemlenmesi amacıyla 2011 yılından bu yana 7 ulusal ve 2 uluslararası siber güvenlik tatbikatı düzenlenmiştir.

Ulaştırma ve Altyapı Bakanlığı ile BTK iş birliği ve ITU ile Karşılıklı İlerleme İçin Siber Güvenlik İttifakı’nın (CAMP) katkılarıyla düzenlenen Uluslararası Siber Kalkan 2019 tatbikatı 19-20 Aralık 2019 tarihinde Ankara’da gerçekleştirilmiştir. Tatbikatta 17 farklı ülkeden 90’a yakın

katılımcıya ev sahipliği yapılmış olup, USOM bünyesinde geliştirilen teknik altyapı ve senaryolar ile katılımcılara bir yandan uygulamalı siber güvenlik tecrübesi yaşatılırken bir yandan da olası siber saldırılarda atılması gereken adımlar konusunda bilgi paylaşımında bulunulmuştur. Bununla birlikte NATO, AGİT gibi uluslararası kuruluşların düzenlediği tatbikatlara da ayrıca katılım sağlanmaktadır.

Ayrıca, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) kapsamında ise başta kritik altyapılar olmak üzere ülkemizin siber ortamdaki varlıklarının korunması ve SOME'lerin siber olay hazırlık seviyesinin artırılması amacıyla 12-13 Ekim 2021 tarihlerinde Ulaştırma ve Altyapı Bakanlığı ve BTK iş birliği ile 36 kamu kurum ve kuruluşumuzdan 135 katılımcının iştirakiyle Siber Kalkan 2021 tatbikatı düzenlenmiştir. Ayrıca; 11-12 Ekim 2022 tarihlerinde Ulaştırma ve Altyapı Bakanlığı ve BTK iş birliği ile 50 kamu kurum ve kuruluşumuzun iştirakiyle Siber Kalkan 2022 tatbikatı düzenlenmiştir. İlave olarak Ulaştırma ve Altyapı Bakanlığı ve BTK iş birliğiyle, 20-21 Ekim 2022 tarihinde finans sektöründe bulunan 40 kuruluşun katılımıyla Finans Sektörü Ulusal Siber Kalkan 2022 Tatbikatı gerçekleştirilmiştir.

Olay Müdahale

Bilahare, Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur. 2013 yılında kurulan Ulusal Siber Olaylara Müdahale Merkezi (USOM), BTK bünyesinde faaliyet göstermekte olup ülkemizde siber güvenlik olaylarına müdahalede ulusal koordinasyonu sağlamakta ve uluslararası temas noktası olarak görev yapmaktadır. Kritik altyapı sektörlerinin kendi sektörel SOME'leri mevcut olup bunlar sektöre özgü düzenleme ve denetleme faaliyetlerini yürütmektedirler. Kurumsal SOME, Sektörel SOME'ler ve USOM, ulusal siber güvenlik olaylarına müdahalenin ana icracısı konumundadır. Bugün hâlihazırda, USOM koordinasyonunda görev yapan 14 Sektörel ve 2.100'ün üzerinde Kurumsal SOME siber vatanın korunmasına yönelik çalışmalar yürütmektedir.

USOM siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetleri yapmakta, kritik sektörlerle yönelik siber saldırıların önlenmesinde ulusal ve uluslararası koordinasyonu sağlamaktadır. Tehdit istihbaratına yönelik konular da USOM aracılığı ile duyurulmaktadır.

Siber suç kapsamındaki soruşturma, inceleme ve takip, kolluk kuvvetleri vasıtasıyla İçişleri Bakanlığı uhdesindeki EGM ve Jandarma Siber Suçlarla Mücadele Daire Başkanlıkları yetki ve sorumluluğunda yürütülmektedir. Bu kapsamda; suç içerikli paylaşım yapan kullanıcının tespiti, adli bilişim incelemelerinin gerçekleştirilmesi, zararlı yazılım ve adli delil incelemesi gibi faaliyetlerin yanı sıra uluslararası siber suçlarla mücadele organizasyonları ile de çalışılmaktadır.

Yerli ve Millî Teknolojiler

Siber güvenlik ürünlerinin ulusal çapta kullanımına dair tutulan bir envanter olmadığından kullanım oranları bilinmemekle birlikte, üretici ve satıcı rakamlarından yabancı ürünlerin ülke genelinde yaygınlığının ve piyasa hâkimiyetinin yüksek olduğu görülmektedir. Bu kapsamda yerli ürünler için potansiyel pazar payı bir fırsat, sert rekabet ortamı da zorluk olarak görülebilir. Bu zorlukların aşılması ve yerli ürünlerin yaygınlaşması için devlet teşvik, destek ve düzenlemeleri bir ön koşul olmaktadır.

Konuya ilişkin olarak, yerli ürün kullanımı hususu 2011 yılında yayınlanan Cumhurbaşkanlığı genelgesi ile ilk kez güçlü bir şekilde telaffuz edilmiştir. Bilahare 10’uncu Kalkınma Planı’nda, müstakil bir program olarak, yaklaşık 20 eylem maddesinden oluşan “Kamu Alımları Yoluyla Teknoloji Geliştirme ve Yerli Üretim Programı” ile devam etmiştir. Orta vadeli programlar, Ulusal Siber Güvenlik Stratejisi, 11’inci Kalkınma Planı, Ekonomi Reformları Eylem Planı gibi birçok üst strateji ve politika belgesinde gündeme getirilmiş bir husus olmuştur. Millî Teknoloji Hamlesinin gerçekleştirilmesine yönelik olarak belirlenen kritik teknolojilerin başında ise siber güvenlik yer almakta, siber güvenlikte yerli teknolojilerin geliştirilmesi konusu millî güvenlik meselesi olarak ele alınmaktadır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)’ün 8 stratejik amacından biri de “Yerli ve Millî Teknolojilerin Geliştirilmesi ve Desteklenmesi” olarak belirlenmiştir. Bu kapsamda yerli ve millî siber güvenlik çözümlerinin sayısının artırılması ve kullanımının yaygınlaşması, siber güvenlik ekosistemimizin büyümesi ve gelişmesi için kamu-akademi-özel sektör arasındaki iş birliklerinin geliştirilmesi ve daha üst seviyeye çıkarılması, yerli ürün ve hizmetleri uluslararası pazarda rekabet edebilecek seviyelere çıkarmak adına siber güvenlik ve performans bakımından yeterliliklerinin test edilmesi ve ürünlerin sertifikasyonu için gerekli ulusal mekanizmanın kurulması gibi hedeflere eylem planında yer verilmiştir.

Türkiye’de özel sektörde siber güvenlik ürün ve hizmetleri sağlayan birçok firma faaliyet göstermektedir. Bunlar arasında; savunma sanayi firmalarından Aselsan, Havelsan ve STM ile birlikte yönetilir güvenlik servisleri sunan ISP’ler (Turkcell, Türk Telekom, Vodafone, Türksat), yerli üreticilerden Picus, Labris, Beam, IcsFusion, Loddos, Cyberwise, Dataflowx, Difose, Turktrust; yabancı ürünlerin distribütörlüğünü yapan firmalar ve siber güvenlik entegratörü olarak çalışan firmalar bulunmaktadır. Dünyada ilkleri başarma anlamında; Picus, ağ siber test sistemi; Labris Harpp on-prem AI DDoS yatıştırma sistemi; Difose, adli inceleme sistemi sayılabilir.

Hâlihazırda doğrudan siber güvenlik sektöründe çalışan firma envanteri mevcut değildir. Siber güvenlik sektörüne ilişkin faaliyetler Sanayi ve Teknoloji Bakanlığı envanterlerinde “bilişim teknolojileri” altında yer almakta ve müstakil olarak tutulmamaktadır. Bu kapsamda müracaat edilebilecek bilgi kaynaklarından biri Türkiye Siber Güvenlik Kümelenmesi Ürün, Firma, Eğitim ve Hizmet Kataloğu olarak görülebilir.

Konuya ilişkin olarak bilgi ve iletişim teknolojileri alanında faaliyet gösteren yerli ve millî firmaların yurt dışı pazarlarda etkinliğini artırmak için DEİK ve Dijital Dönüşüm Ofisi Başkanlığı 2022 yılı Haziran ayı içerisinde Dijital Teknolojiler iş konseyini hayata geçirmiştir. Siber güvenlik, yapay zekâ, oyun, bulut bilişim yıkıcı teknolojiler odağında belirlenen alt komitelerde küresel pazara açılma ve bu pazarlarda güçlenme hedefiyle çalışmalar gerçekleştirilecektir.

Türkiye'nin siber güvenlikte yerli teknoloji geliştirme alanındaki durumu olumlu bir seyir izlemektedir. Ülke, yerli ve millî siber güvenlik ürünlerinin geliştirilmesi ve kullanımının yaygınlaştırılması konusunda önemli adımlar atmaktadır. Dijital Dönüşüm Ofisi Başkanlığı, yerli siber güvenlik teknolojilerinin güçlendirilmesi amacıyla çalışmalar yürütmekte ve ulusal siber güvenlik ekosisteminin güçlendirilmesi için teşvik sistemini ve kamu alımlarını bütünleştirmeye yönelik bir sistematik geliştirme çalışmalarına başlamıştır. Ülke, yerli siber güvenlik ürünlerinin dünya pazarına açılması için uluslararası iş birliklerini artırmakta ve ürünlerin dünya çapında rekabet edebilirliğini sağlamak için çalışmalar yürütmektedir. Bu çerçevede, Türkiye'nin siber güvenlikte yerli teknoloji geliştirme alanındaki durumu, ulusal güvenlik politikaları ve stratejileri doğrultusunda olumlu bir yönde ilerlemektedir.

Türkiye'de yerli ve millî siber güvenlik teknolojilerinin geliştirilmesi için çeşitli kuruluşlar ve projeler faaliyet göstermektedir. Dijital Dönüşüm Ofisi Başkanlığı, bu alanda önemli bir rol

oynamaktadır. Özellikle 1 Numaralı Cumhurbaşkanlığı Kararnamesi kapsamında, yerli siber güvenlik teknolojilerinin geliştirilmesi ve kullanımının kamuda yaygınlaştırılması için çalışmalar yürütmektedir. Ayrıca, Millî Teknoloji Genel Müdürlüğü, siber güvenlik alanında yerli ve millî ürünlerin üretilmesi, kullanımının yaygınlaştırılması, veri merkezi ve veri işleme altyapısının güçlendirilmesi ve siber güvenlik ekosisteminin geliştirilmesine katkı sağlamak amacıyla görevlendirilmiştir.

3.6.4. Denetim, Gözetim ve Onay

Denetim, Test ve Sertifikasyon

Ülkemizde siber güvenlikte standardizasyon ve sertifikasyon konusunda çeşitli çalışmalar yürütülmektedir. TSE (Türk Standartları Enstitüsü) tarafından TS 13638 standardı ve ISO 15408 standartlarına uygun sertifikasyon hizmetleri sunulmaktadır. Ayrıca, ISO/IEC 27000 serisi güvenlik standartları Türkçeye uyumlaştırılarak yayımlanmaktadır. Türkiye Siber Güvenlik Kümelenmesi koordinasyonunda TRTest tarafından yürütülen Test ve Sertifikasyon Projesi kapsamında Siber Güvenlik Ürünleri Test ve Uygunluk Kriterleri uygulanmaktadır.

Ulusal siber güvenliği sağlamak üzere geliştirilen rehber, genelge vb. standartlar bu alana değer katmakta, uyum ve denetim çalışmalarının özet sonuçları Dijital Dönüşüm Ofisi ile paylaşılarak özellikle kamu ve kritik altyapıların güvenlik seviyesi hakkında daha net bir fikir edinilmektedir.

Siber güvenlik alanında sertifikasyona yönelik olarak; TSE tarafından sağlanan TS 13638 standardı (Bilgi Teknolojileri - Güvenlik Teknikleri - Sızma Testi Yapan Personel ve Firmalar İçin Şartlar) ve ISO 15408 standardı kapsamında çeşitli kurum ve firmalar tarafından “Ortak Kriterler Değerlendirme Laboratuvarları” ile donanım temelli ataklar, yazılım temelli ataklar ve kripto konularında sertifikasyon hizmeti sunulmaktadır.

İstanbul Üniversitesi-Cerrahpaşa bünyesinde de IoT cihazlarının fonksiyonel ve güvenlik yeterliliklerinin testi için “ISTEC-Nesnelerin İnterneti Ekosistemi Güvenlik Test ve Değerlendirme Merkezi” kurulmuş ve çalışmalara başlamıştır.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Türk Standartları Enstitüsü koordinasyonunda bulut bilişim ve denetim hizmetlerine ilişkin standart çerçevesi oluşturulma çalışmaları başlamıştır.

Tatbikatlar

Siber güvenlik tatbikatları tehditlere karşı alınan tedbirlerin etkinliğini ve bu tedbirleri işleten iş gücünün yetkinliğini ölçmek için kullanılan ana araçlardan biridir. Türkiye’de, Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu tarafından “Ulusal Siber Kalkan” tatbikatları gerçekleştirilmektedir. Başta kritik altyapılar olmak üzere ülkemizin siber ortamdaki varlıklarının korunması ve SOME’lerin siber olay hazırlık seviyesinin artırılmasını amaçlayan bu tatbikatlar 2022 yılı içinde finans sektörü için ayrıca da yapılmıştır. Enerji sektörü düzenleyicisi EPDK da kendi sektörü için benzer tatbikatları gerçekleştirmektedir.

Ülkemizde yürütülen siber güvenlik çalışmaları kapsamında uluslararası iş birlikleri yapılmaktadır. Siber güvenlik alanında görev yapan insan kaynağının yetkinliğinin artırılması, siber olaylara hazırlık seviyelerinin yükseltilmesi ve paydaşlar arasında iş birliğinin geliştirilmesi amacıyla sektörel, ulusal ve uluslararası siber güvenlik tatbikatları gerçekleştirilmektedir. Hem kurum ve kuruluşlarımızda hem de ulusal seviyedeki siber olaylara hazırlık seviyelerinin ve olay müdahale kabiliyetlerinin artırılması için atılan önemli adımlar kapsamında 2011’den bu yana Ulaştırma ve Altyapı Bakanlığı koordinasyonunda yedi ulusal ve iki uluslararası siber güvenlik tatbikatı gerçekleştirilmiş bulunmaktadır.

Uluslararası Siber Kalkan 2019 tatbikatı, UAB ve BTK koordinasyonunda 19-20 Aralık 2019 tarihinde ITU ile Karşılıklı İlerleme İçin Siber Güvenlik İttifakı’nın katkılarıyla Ankara’da gerçekleştirilmiştir. Tatbikatta 17 farklı ülkeden 90’a yakın katılımcıya ev sahipliği yapılmıştır.

NATO Kilitli Kalkan (Locked Shields), NATO Siber Koalisyon (Cyber Coalition) ve NATO Kriz Yönetim Tatbikatı gibi çeşitli uluslararası siber güvenlik tatbikatlarına da katılım ve katkı sağlanması sürdürülmektedir.

NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (NATO CCD COE) tarafından yıllık olarak yapılan Kilitli Kalkan (*Locked Shields*) tatbikatlarına Türkiye’de farklı kurumlardan siber güvenlik uzmanları ile takım oluşturularak katılım sağlanmaktadır. Dünyanın en geniş katılımlı ve birçok otoriteye göre en karmaşık ve ileri teknolojilerine sahip siber savunma tatbikatı olarak kabul edilmektedir. Bu kapsamda, USOM tarafından söz konusu tatbikatlara düzenli olarak katılım sağlanmakta olup son olarak 22-26 Nisan 2024 tarihlerinde NATO Siber Savunma Mükemmeliyet

Merkezi (Estonya/Talin) tarafından koordine edilen Kilitli Kalkan-2024 (Locked Shields-2024) Tatbikatı'na katılım sağlanmıştır.

Söz konusu faaliyetlerin yanı sıra; Uluslararası Telekomünikasyon Birliği (ITU) tarafından Birleşik Arap Emirlikleri/Dubai'de gerçekleştirilen Küresel Siber Tatbikat (*Global CyberDrill*) ve NATO Destek ve Tedarik Ajansı (NSPA) tarafından icra edilen Lojistiği Desteklemek Amacıyla Kritik Altyapı için Siber Dayanıklılık Tatbikatı da 2024 yılı içerisinde USOM tarafından iştirak edilen diğer uluslararası iş birliği çalışmaları arasında yer almaktadır.

Siber Koalisyon (*Cyber Coalition*) siber savunma tatbikatı, NATO tarafından yıllık olarak organize edilmektedir. Üç gün süren etkinliğe, NATO üyesi ve ittifak ülkelerinden katılım sağlanmaktadır. Türkiye aktif olarak bu tatbikatlara katılmaktadır.

Güneydoğu Avrupa ülkelerinde ve Türkiye'de siber suçlardan gelir elde edilmesi ile mücadele amacıyla Avrupa Konseyi ve Avrupa Birliği tarafından yürütülen IPROCEEDS projesi kapsamında uluslararası siber güvenlik tatbikatının altyapısı ve senaryoları USOM tarafından hazırlanıp icrası gerçekleştirilmiştir. Söz konusu tatbikatlar Yunanistan, Romanya, Türkiye ve Mauritius'ta gerçekleştirilmiştir.

Yerli ve Millî Ürünler

Yerli siber güvenlik ürünlerinin kendi kategorilerinde birbirlerine göre seviyesini tespit etmek üzere yapılan seviyelendirmeye ve fonksiyonel uygunluğa yönelik çalışmalar gerçekleştirilmektedir. Diğer yandan, yabancı muadillerine nazaran seviye tespiti, yazılımsal ve donanımsal olarak güvenlik düzeylerinin belirlenmesi ve ürünleşme sürecinin tespitine yönelik bir test mekanizması aktif değildir.

Sonuç olarak, muhtelif mevzuatın yanı sıra, Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Bilgi ve İletişim Güvenliği Rehberi, Bilgi ve İletişim Güvenliği Denetim Rehberi gibi belgelerle siber güvenlik alanında standartlar belirlenmiş ve denetim mekanizmaları oluşturulmuştur. Bununla birlikte uluslararası sertifikasyon ve standartların sektör tarafından bilinmesi ve çalışılması da önem arz etmektedir.

3.6.5. İş Birliği ve Koordinasyon

Türkiye'nin siber güvenlik alanına müstakilen memur edilmiş bir makam bulunmamakla birlikte, ulusal siber güvenlik ekosistemi; içerisinde kamu kurumları, teknolojiyi üreten, geliştiren, entegre eden siber güvenlik sektörü, üniversiteler, sivil toplum kuruluşları, bireyler, politika geliştiriciler, standart belirleyiciler, düzenleyiciler ve daha fazlasını barındıran geniş bir ağdan oluşmaktadır.

SSB tarafından kurulan Türkiye Siber Güvenlik Kümelenmesi son yıllarda bu ağdaki paydaşlar arasındaki etkileşim ve iletişimin ana aktörü konumuna gelmiştir. Kısaca ifadesiyle 'Küme', 2017 yılında Savunma Sanayii Başkanlığı öncülüğünde ve ilgili tüm kamu kurum/kuruluşları, özel sektör ve akademi temsilcilerinin katkılarıyla temelleri atılan, siber güvenlik alanında teknoloji üreten ve dünya ile rekabet edebilen Türkiye ana hedefi doğrultusunda siber güvenlik yapılanmasının geliştirilmesi amacıyla kurulan bir platformdur.

Platform, DDO ve SSB arasında 1 Şubat 2021 tarihinde imzalanan protokol kapsamında iki kurum tarafından müştereken yürütülmektedir. Türkiye Siber Güvenlik Kümelenmesi yerli ve millî siber güvenlik teknoloji üreticilerini ve hizmet sağlayıcılarını toplayan ve etkileşim sağlayan bir proje olarak kurgulanmıştır. 255 üye firması bulunan Türkiye Siber Güvenlik Kümelenmesi tarafından "pazara erişim, inovasyon, yeteneğe erişim, teknolojik üstünlük ve etkileşim" olmak üzere beş ana başlıkta faaliyetler yürütülmektedir.

Siber güvenlik ekosisteminin güçlendirilmesinde etkileşim ve iletişimin önemi büyüktür. Bugün bu etkileşim ve iletişim ortamının oluşturulmasında sivil toplum kuruluşlarının da payı yüksektir. Türkiye'de siber güvenlik ile ilgili faaliyetleri bulunan ve aralarında Türkiye Bilişim Derneği, Bilişim Teknolojileri ve Siber Güvenlik Derneği, Boğaziçi Siber Güvenlik Merkezi, Bilgi Güvenliği Derneği gibi birçok kuruluş bulunmaktadır. Dernekler, yayınladıkları raporlar ve yaptıkları etkinliklerle Türkiye'nin siber güvenlik farkındalığını artırmaktadırlar.

Buna ilave olarak üniversitelerin siber güvenlik kulüpleri ile ortak faaliyetler yürütülmekte, BTK başta olmak üzere kamu ve özel sektör paydaşları tarafından gençlere alanda bilgi ve beceri kazandırabilmek için yaygın faaliyetler icra edilmektedir. Bunlardan ilk akla gelenleri

Teknofest’ler, Siber Güvenlik Yarışmaları, Hackathonlar, Capture the Flag, BootCamps olarak sıralanabilir.

Bütün bu kurum, kuruluş, organize edilen faaliyetler ve ilgili projeler yoluyla, yerli ve millî siber güvenlik teknolojilerinin geliştirilmesi ve ulusal siber güvenlik ekosisteminin güçlendirilmesi amaçlanmakta, ekosistemin güçlenmesi sayesinde yaygınlaşan yerli ürünlerin ekonomiye ve güvenliğe doğrudan katkı sağlaması hedeflenmektedir.

3.6.6. Topyekûn Farkındalık

Dijital dünyada daha dayanıklı vatandaş için siber güvenlik alanında toplumsal farkındalığın oluşturulması ve nitelikli insan kaynağı yetiştirilmesi büyük önem taşımakta, bu maksada ulaşmak için önemli çalışmalar yürütülmekte ve eğitim müfredatlarının geliştirilmesi üzerine odaklanılmaktadır.

Bu konuda, en küçükten başlayarak toplumun tüm kesimlerinin siber güvenlik olgusunun içerisine bilgili bir şekilde çekilmesi ve topyekûn bir farkındalık kazanılması önemlidir. Bu farkındalığın oluşmasında eğitim, şüphesiz yaşamsal bir rol oynamaktadır.

Türkiye’de siber güvenliğe yönelik eğitimler incelendiğinde, konunun ilk ve ortaöğretimin genel müfredatında olmadığı görülmektedir. Bu sebeple ilk ve ortaöğretim seviyesinde siber güvenliğe yönelik müfredatın geliştirilmesi ve öğretilmesi hususu gelişime açıktır.

Bu kapsamda Türkiye’de siber güvenliğe özel eğitim veren kurumlardan en önde geleni, 2020 yılında açılışı gerçekleştirilen ve Siber Güvenlik Lisesi olarak da bilinen Pendik Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi’dir. Sızma testi, adli bilişim, yapay zekâ ve siber tatbikat laboratuvarları bulunan okulda eğitim görececek öğrencilere Teknopark İstanbul başta olmak üzere siber güvenlik faaliyeti yürüten firmalarda geniş staj imkânı sunulmaktadır.

Lisans, yüksek lisans ve doktora seviyesinde de siber güvenlik ve bilgi güvenliği alanlarına yönelik akademik programlar mevcuttur. 2023 yılı itibarıyla yaklaşık 30’un üzerinde üniversitede yüksek lisans programı bulunmaktadır. Lisans alanında siber güvenlik mühendisliği programı bir, adli bilişim mühendisliği programı bir olmak üzere hâlihazırda iki üniversitede bu eğitimler verilmektedir.

Bazı üniversitelerin bünyesinde siber güvenlik alanında doğrudan çalışmalar yapan veya diğer bilişim teknolojileri ile birlikte siber güvenlik alanına da hizmet eden Uygulama ve Araştırma Merkezleri yer almaktadır. 2023 yılı itibarıyla mevzuatı yayımlanmış bu şekilde 20 merkez bulunmaktadır.

2023 yılı itibarıyla siber güvenlik ve bilgi güvenliği alanlarında kapasite geliştirmeye yönelik olarak 27 üniversitede “Bilişim Güvenliği Teknolojisi” adı ile “yüksekokul” seviyesinde öğretim programı uygulanmaktadır.

Okullarda verilen siber güvenlik müfredatının her okula göre uygulama usulü, ders içeriği farklılık göstermektedir. Temel bilgi güvenliği ve siber güvenliği müfredatının belirlenerek standartlaşmasına, siber güvenlik eğitim ve öğretiminin ilk ve ortaöğretimden yükseköğretim düzeyine kadar tüm seviyelerde bütüncül bir bakış açısı ile ele alınmasına ihtiyaç vardır.

Ankara, Ege, Gebze Teknik ve İstanbul Teknik üniversiteleri bünyesinde Siber Güvenlik Meslek Yüksekokulları 2023 yılı güz döneminde eğitim öğretime açılmıştır. Teknoparkların içinde bulunan siber güvenlik meslek yüksekokullarında, öğrencilere siber güvenliğin temellerinin yanı sıra güvenlik teknolojileri, ağ güvenliği, sızma testleri ve veri analizi gibi konularda da eğitim verilmektedir.¹¹⁴¹¹⁵

Siber güvenlik alanında nitelikli iş gücü gelişimine yönelik faaliyetler kamu, STK ve özel sektör ve akademi eliyle de gerçekleştirilmekte olup, bu çalışmalardan bazıları aşağıda sıralanmıştır.

TÜBİTAK Sanayi Doktora Programı, BTK Akademi, Türkiye Siber Güvenlik Kümelenmesi Siber Kariyer Eğitim Programı, 1 Milyon İstihdam Projesi ile gerçekleştirilen siber güvenlik eğitimleri ile kritik sektörlerde faaliyet gösteren siber güvenlik uzmanlarının yetenekleri artırılarak kurum ve kuruluşlarımızın siber olaylara hazırlık kapasitesi geliştirilmektedir.

Siber güvenlik alanında pratik ve uygulama yetkinliğinin artırılması, siber olaylara hazırlık seviyesi ve müdahale kabiliyetinin artırılması amacıyla; DDO, Siber Küme, BTK (USOM) gibi

¹¹⁴ Yükseköğretim Kurulu, 16/05/2023. <https://www.yok.gov.tr/Sayfalar/Haberler/2023/siber-saldirilara-karsi-uzman-yetistirmek-icin-4-yeni-myo-aciliyor.aspx>,

¹¹⁵ Duygu Fidancıoğlu, 02/09/2023. <https://medium.com/cyber-alliance/turkiyede-siber-guvenlik-ve-bilgi-guvenligi-egitimi>

paydaşlar tarafından, farklı siber güvenlik alanlarına hitap eden konsept yarışmalar düzenlenmektedir.

Siber Yıldız yarışmasının bir sonraki aşaması olan ve genç yeteneklerimizin profesyonelleşme yolunda ilerlemesine olanak vererek, ülkemizin ihtiyacı olan siber güvenlik uzmanlarının yetiştirilmesine yönelik FETİH Siber Talimhane projesi ile uygulamalı siber güvenlik eğitim laboratuvarı altyapısı çalışmaları USOM bünyesinde tamamlanmıştır.

Yaklaşık 2.3 milyon üyesi bulunan BTK Akademi üzerinden sunulan çevrim içi siber güvenlik eğitimlerine 2024 yılı Haziran ayı sonu itibarıyla 32 farklı başlıktaki eğitimlere 570.275 kişi katılım sağlamıştır. Siber güvenliğin farklı alanlarında birçok eğitim BTK Akademi ve USOM iş birliği ile gerçekleştirilmektedir.

Üniversite bilgi işlem sorumlularına siber güvenlik farkındalığını artırmak amacıyla temel siber güvenlik farkındalığı konularını içeren bir eğitim programı hazırlanıp ilgili personellere BTK/USOM bünyesinde eğitimler verilmiştir. Siber farkındalığın artması ile birlikte, üniversiteler genelinde siber olayların tespit ve engellenme oranlarında artış görülerek, maddi ve manevi kayıpların önüne geçilmesi amaçlanmıştır.

USOM ve BTK Akademi iş birliği ile ülke genelindeki tüm SOME personellerine siber güvenlik bilgilerinin ve olgunluk seviyelerinin yükseltilmesi amacıyla "SOME Online Eğitim Serisi" hazırlanıp hizmete sunulmuştur. Eğitimler çeşitli içerik ve seviyelerde toplam 172 dakika olup 8 bölüm, 76 video ve 40 adet etkileşimli sorudan oluşmaktadır. SOME Eğitime BTK Akademi Online Eğitim Platformu üzerinden ulaşılabilir.

Gençlik ve Spor Bakanlığı, BTK Akademi ve USOM iş birliğinde öğrencilerine yönelik uygulamalı siber güvenlik eğitimleri düzenlenmiştir. Siber Tehdit Avcılığı 25 öğrenci, Gaziantep Siber Güvenlik Atölyesi 25 öğrenci, Sinop İli Kali Linux Sızma Testi Eğitimi 25 öğrenci, Siber Tehdit Avcılığı ve Olay Müdahale Atölyesi 25 öğrenci, Sızma Testi ve Olay Müdahale Süreçleri 25 öğrenci, Geleceğin Hackerları 20 lise öğrencisi, İstanbul Rami Siber Talimhane 30 öğrenci, Çanakkale Siber Güvenlik Atölyesi 25 öğrenci ve Hacktrick Etkinliği ile 400 öğrenciye BTK'da yüz yüze eğitim ile toplamda 650 öğrenciye yönelik siber güvenlik eğitimleri gerçekleştirilmiştir.

İnternetin güvenli ve bilinçli kullanımı konusunda ise BTK tarafından “Güvenli İnternet Merkezi”, “Güvenli İnternet Bilgi Destek Hattı” ve “Güvenli Web” İnternet sayfası kurulmuştur. Öte yandan; Aile ve Sosyal Hizmetler Bakanlığı, Millî Eğitim Bakanlığı, Sağlık Bakanlığı, Gençlik ve Spor Bakanlığı ve Erişim Sağlayıcılar Birliği ile geçtiğimiz süreçte güvenli İnternet kullanımına ilişkin çeşitli konularda protokol imzalanarak öğrenci, öğretmen ve velilerle birlikte eğitimcilere yönelik eğitimler, seminerler düzenlenmiştir. Ayrıca; ülke çapında çocukların ve gençlerin yeni teknolojilerle doğrudan etkileşimlerini sağlayarak, teknolojinin, İnternetin doğru kullanılmasını ve bu konuda bilinçlenmelerini sağlamak amacıyla hizmet veren gezici Güvenli İnternet Tırı ile 2018 yılından beri 200 okul ziyaret edilerek 80 binden fazla öğrenciye ulaşılmıştır. Güvenli İnternet Tırı ile okullarda tanıtım etkinlikleri gerçekleştirilmeye devam edilmektedir.

Bilgi Teknolojileri ve İletişim Kurumu tarafından bilinçli ve güvenli İnternet kullanımı konusunda farkındalık oluşturmak amacıyla her yıl düzenlenen 'Güvenli İnternet Günü' etkinliği ile; ortaokul ve lise öğrencileri ile katılımcılara, güvenli ve bilinçli İnternet kullanımı, İnternet yardım merkezi, İnternet destek hattı, siber zorbalık, siber saldırı, ebeveyn ve çocuklar için doğru İnternet kullanımı gibi konularda bilgilendirmeler gerçekleştirilmektedir. Ayrıca öğrenciler Güvenli İnternet Atölyeleri’ni ziyaret ederek, İnternetin bilinçli ve güvenli kullanımına yönelik düzenlenen eğitim ve yarışmalara da katılım sağlayabilmektedir.

2023 yılında yayın hayatına başlayan Bilgi Teknolojileri ve İletişim Dergisi (BTK Dergi), Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yayımlanan hakemli ve akademik dergidir. Dergide, Türkçe ve İngilizce olmak üzere; makale, çeviri, kitap tanıtımı ve araştırma raporları yayımlanmaktadır. Dergide; Yeni Medya ve İletişim, Siber Güvenlik, Haberleşme Teknolojileri, Yapay Zekâ, Bilgi Toplumu, Bilişim Hukuku, Nesnelerin İnterneti, Büyük Veri, Dijital Mahremiyet, Blok Zinciri Teknolojisi, Dijitalleşme ve Toplum konularındaki çalışmalara yer verilmektedir.

Millî Eğitim Bakanlığı tarafından EBA platformu üzerinden farkındalık içeriğinin yanı sıra, DDO ile iş birliği içerisinde ülke çapındaki farkındalık projesi Siber Zekâ Bilgi Yarışması düzenlenmektedir.

Emniyet Genel Müdürlüğü tarafından toplumsal siber güvenlik farkındalığının artırılması amacıyla SİBERAY projesi yürütülmektedir.

Yine DDO eşgüdümünde ve TRT ile birlikte İnternetin güvenli kullanımı, sanal zorbalık, İnternet bağımlılığı, dijital okuryazarlık, yapay zekâ, nesnelerin İnterneti, dijitalleşmenin hayata yansımaları, millî teknolojiler ve ortalama gibi konu başlıklarından oluşan 10 bölümlük “Dijital Tayfa” dizisi hazırlanmış ve yayımlanmıştır.

Diğer pek çok girişimin yanında, siber güvenlik alanında eğitim ve farkındalığın artırılması bağlamında Kalkınma Ajansı koordine ve desteğinde yürütülen Siber Vatan Programı ve Boğaziçi Üniversitesi Siber Güvenlik Merkezi (BÜSİBER) sayılabilir. Siber Vatan Programında Siber Güvenlik, Yazılım, Yapay Zekâ, Blok Zincir ve Mobil Uygulama ve Oyun Geliştirme gibi alanlarda tekno-girişimciliğin geliştirilmesi amacıyla çeşitli modüllerden oluşan program ve projeler kurgulanmakta, BÜSİBER ile de akademik bir bakış açısıyla siber güvenliğin gerektirdiği uzmanlık ve odaklanmayı sağlamak hedeflenmektedir.

Yukarıda da ifade edildiği üzere Türkiye’de ulusal siber güvenlik kapasitesinin inşası, siber güvenlik farkındalığının artırılması ve nitelikli siber güvenlik iş gücünün tesis edilmesi için önemli sayıda proje ve faaliyet yürütülmektedir.

Sektör ihtiyaçlarının belirlenerek, okullarda bu ihtiyaca uygun sayı ve nitelikte iş gücü sağlanması, mezunların kamu ve özel sektörde istihdamını artıracak iş birliği modellerinin geliştirilmesi, okullarda siber güvenlik eğitimi verme yeteneklerinin artırılması, tüm bu kapasite geliştirme çalışmalarının da bütüncül bir bakış açısı ile ulusal bir strateji ve politikanın parçası olarak yürütülmesi şüphesiz gerekliliktir.

Diğer taraftan, hâlihazırda siber güvenlik ve bilgi güvenliği alanında çok sayıda eğitim etkinliği bulunmakla birlikte, bu eğitilenlerin sektörde istihdamına ilişkin kapsamlı bir araştırma ve/veya veri bulunmamaktadır. Eğitim kalitesi, eğitmen ve öğrencilerin gelişimi, mezunların sektöre kazandırılması konusunda denetleme ve izleme mekanizmalarının aktif olarak çalıştırılması önemli görülen bir husustur.

Bu konuda ayrıca, siber güvenlik başlığının toplumun odak ilgi noktalarından biri hâline getirilmesine yönelik tüm kesimleri hedefleyen inisiyatiflerin de sayıca artırılması gerektiği hususu göze çarpmaktadır.

3.6.7. Uluslararası İş birliği

Türkiye'nin ulusal siber güvenlik yönetişimi ve organizasyonu konusunda ulusal ve uluslararası alanda attığı adımlar ve yaptığı ilgili düzenlemeler, ülke dışında da kabul görmekte ve Türkiye'nin siber güvenlik endekslerinde görece üst sıralarda yer almasını sağlamaktadır.

Uluslararası platformlarda bilgi paylaşımı ve etkin iş birliği kapsamında UAB ve BTK tarafından; BM, AB, NATO, AGİT, G20, OECD, Türk Devletleri Teşkilatı, Ekonomik İş birliği Teşkilatı gibi uluslararası organizasyonların politika ve strateji belirleyici faaliyetlerine katkı ve katılım sağlanmaktadır.

Türkiye, Uluslararası Telekomünikasyon Birliği (ITU) tarafından en son 2020 yılında yayımlanan "Global Siber Güvenlik Endeksi"ne göre dünya genelinde 200'e yakın ülke içinde 11. sırada, Avrupa ülkeleri arasında ise 6. sırada yer alarak bu alanda belirli bir olgunluğa erişmiş olduğunu göstermiştir.

Her alanda olduğu gibi siber güvenlik alanında da dünyada belirlenmiş standartlara uyum sağlama yönünde gayret gösterilmesi, hatta bu standartların oluşturulmasına ve geliştirilmesine doğrudan katkı sunularak etkin rol oynanması önemlidir. Bu sayede ülkemiz ilgili alanda belirli gelişmişlik düzeyine gelmekte ve söz sahibi olmaktadır.

Siber saldırılara müdahalede bilgi paylaşımı açısından ulusal ve uluslararası istihbarat kaynakları ile iş birlikleri yapılması teknik bir gerekliliğin ötesinde siber savunma yapısını güçlendirmek için zorunlu koşullardan biridir. Bu amaçla USOM uluslararası siber olaylara müdahale organizasyonlarına (*Trusted Introducer*, FIRST, NATO-MISP, OIC-CERT) üye olmuş durumdadır.

Bununla birlikte USOM; siber tehdit istihbaratı edinimi, üretimi ve paylaşımı noktasında ulusal ve uluslararası paydaşlarıyla koordinasyon sağlanmasında önemli görevler üstlenmektedir. İnternet aktörleri, uluslararası kuruluşlar, adli makamlar, araştırma merkezleri, üniversiteler ve özel sektör kuruluşları ile birlikte hareket ederken aynı zamanda uluslararası alanda ülkemizin temas noktası olma görevini de yerine getirmektedir. Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST), Güvenilir Tanıtıcı (TI), Karşılıklı İlerleme için Siber Güvenlik İttifakı (CAMP), Uluslararası Telekomünikasyon Birliği (ITU), OIC-CERT ve NATO bünyesindeki Zararlı Yazılım

Bilgi Paylaşım Platformu (MISP) gibi uluslararası kuruluşların ve organizasyonların yanı sıra birçok ülkenin ulusal siber olaylara müdahale ekibiyle de çift yönlü olarak bilgi paylaşımı içerisinde bulunmaktadır.

USOM'un faaliyet ve iş birlikleri haricinde de diğer kurum ve kuruluşlar tarafından yapılan uluslararası siber tatbikatlara iştirak, konunun diğer bir önemli boyutunu oluşturmaktadır. Bu konuda katılım sağlanan tatbikatlar yukarıda evvelce sıralanmıştır.

Türkiye'de siber güvenlik alanında ulusal düzeyde yapılan çalışmalar kapsamında, ulusal siber güvenlik kapasitesinin inşası ve siber güvenlik farkındalığının artırılması ve bu yolla ülkemizin ihtiyaç duyduğu nitelikli siber güvenlik iş gücünün tesis edilmesine yönelik birçok proje ve faaliyet yürütülmüş ve yürütülmeye devam etmektedir. Bu çalışmalar, siber güvenlik alanında toplumsal farkındalığın oluşturulması, nitelikli insan kaynağı yetiştirilmesi ve ulusal siber güvenlik yönetişiminin güçlendirilmesi için önemli bir temel oluşturmaktadır.

4. Türkiye’de Atılması Gereken Orta ve Uzun Vadeli Adımlar

Şura kapsamındaki çalışmalar sonucunda önümüzdeki dönemde yapılması gerekenlere ışık tutacak bazı ipuçlarının ortaya çıktığı söylenebilir. Büyük krizlerin ve deprem başta olmak üzere doğal afetlerin merkezinde bulunan ülkemiz için yeni çağın kuvvet çarpanı olarak dijital dünyada egemen olmak bir zorunluluktur.

Öncelikli olarak; kriz, gerginlik ve çatışma ortamlarında gerekli dijital becerilerin edinilmesi gerektiği açıktır. Bu prensiple, görev kritik sistemlerden ve kritik altyapılardan başlamak üzere dijital egemenlik kapasitesinin ve ülke verisinin değere dönüştürülmesi için yerleştirme çabalarının kısa vadede ivedilikle artırılması önem arz etmektedir.

Kritik altyapıların dayanıklılığının sağlanması için hem yerel hem de ulusal düzeyde paydaşlar arasındaki koordinasyon esastır. Bu koordinasyon, zorlukların ve zayıf noktaların etkili bir şekilde ele alınması için hem kamu hem de özel kurumları içermelidir. Kritik altyapılarda koordinasyonu ve dayanıklılığı artırmaya yönelik kısa ve orta vadede üzerine eğilinmesi gerekli bazı önemli hususlar şu şekilde sıralanabilir.

- Ülkemizin fiber, mobil ve uydu altyapılarının, iletişim ağlarının kritik bileşenleri olarak kabul edilmesi, korunması ve dayanıklılığına öncelik verilmesi.
- Potansiyel afetleri simüle etmek ve müdahale planlarının ve prosedürlerinin etkinliğini test etmek için gerçekçi Afet Simülasyon ve Tatbikatların yapılması.
- Kritik altyapıları siber saldırılar ve fiziksel sabotaj dâhil olmak üzere çeşitli tehditlere karşı korumak için hem dijital hem de fiziksel güvenlik endişelerinin ele alınması.
- Karşılıklı bağımlılıkları ve güvenlik açıklarını daha iyi anlamak için altyapıların (ör. BT, OT) sınıflandırılarak bir envanterinin çıkarılması ve birbirleriyle olan ilişkilerinin haritalandırılması.
- Bağlantı bant genişliğini ve dayanıklılığını artırmak için yüksek hızlı yeni nesil elektronik haberleşme altyapılarının (fiber optik ağlar, 4,5G ve ötesi mobil haberleşme altyapıları gibi) karasal altyapıların geliştirilmesine, genişletilmesine ve çeşitlendirilmesine dönük yatırımların daha da artırılması.

- Kritik altyapıların olgunluğunu ve güvenliğini artırmak için denetim ve sızma testi gereklilikleri gibi mevzuat ve düzenlemeleri yürürlüğe koymak suretiyle altyapı yönetimini geliştirmek için dijital ikizler gibi teknolojilerden yararlanılması.

Bilginin gizliliği ve bütünlüğü kapsamında şifreleme ve kriptoloji teknolojileri, veri güvenliği açısından vazgeçilmez bir unsur olarak kabul edilmektedir. Bu alandaki gelişmelerin desteklenmesi ve Türkiye'nin küresel ortamda rekabetçi kalmasının sağlanması büyük önem taşımaktadır. Askerî sistemlerde belirli ilerlemeler sağlanırken, şifreleme ve kriptoloji teknolojilerinin sivil uygulamalarda eksiklikleri bulunmaktadır. Bu açığı kapatmak ve her iki sektördeki yetenekleri güçlendirmek için çaba gösterilmelidir.

Diğer birçok alanda olduğu gibi bu alanda da yetişmiş personelin daha iyi şartlarda çalışma isteğiyle sık sık kurum değiştirmesi, dahası ülkeyi terk ederek yurt dışına göç etmesi, insan kaynağı eksikliği yaratması yönüyle ciddi bir sorun alanıdır.

Nitelikli personeli elde tutmak için gerekli politikalar üretmek kadar, daha az personel ile işi devam ettirebilmenin yolları da aranabilir. Bunun için iş tanımlarının sadeleştirilmesi, görev birleştirmeleri, uzman havuzları oluşturulması ve özellikle kamuda uzaktan çalışmanın yaygınlaştırılması gibi alternatifler değerlendirilebilir. Örnek vermek gerekirse, her kurumun kendi siber operasyon merkezini (SOC) kurarak işletmesi gerekli olmayabilir, doğru kaynağı doğru yere yönlendirmek suretiyle süreç daha verimli işletilebilir.

Yeni nesil teknolojik gelişmelerin veri güvenliği ve siber tehditler üzerindeki etkileri oldukça kapsamlıdır. Özellikle yapay zekâ, blokzincir, IoT cihazları ve kuantum gibi teknolojiler, siber tehditlerin ölçeğini ve karmaşıklığını artırmaktadır. Bu teknolojiler, siber saldırı sathını da genişletmekte ve yöntemleri çeşitlendirmektedir. Yapay zekâ destekli saldırıları daha karmaşık hâle getirirken, IoT cihaz sayısının artması daha yüksek hacimli saldırılara yol açabilmektedir. Kuantum teknolojileri ise siber olayların öngörülebilirliğini, şiddetini ve ölçeğini karmaşıklaktadır.

Bu teknolojilerin kullanımıyla ilgili potansiyel faydalar arasında ise daha hızlı ve doğru saldırı tespiti, 7/24 koruma, yüksek miktarda verinin hızlı işlenmesi, insan hatalarının azaltılması ve otomasyonun sağlanması gibi avantajlar sıralanabilir. Bu anlamda yapay zekâ kullanımının

gelecekte önemli bir rol oynaması beklenmektedir. Potansiyel kullanım alanları, anomali tespiti ve kural bazlı uygulamaların yerini alabilir ve müdahale için bilgi ve belgelerin yaygınlaştırılmasını sağlayabilir.

Ancak, bu teknolojilerin kullanımıyla beraber ciddi sınamalar da ortaya çıkmaktadır. Özellikle yapay zekâ eğitiminde veri setlerinin zehirlenmesi, yapay zekâ destekli saldırıların karmaşıklığı, IoT cihazlarının tehdit oluşturması gibi riskler bulunmaktadır.

Bu nedenle, yeni nesil dijital teknolojilerin siber tehditler üzerindeki etkileri dikkatle incelenmeli ve bu teknolojilerin kullanımıyla ilgili potansiyel faydaların yanı sıra riskler de göz önünde bulundurularak gerekli güvenlik önlemleri alınmalıdır. Eğitim ile teknik bilgi ve becerilerle donatılmış nitelikli insan kaynağının yeni nesil siber olaylara müdahale etme ve dahası alanda operatif ve taktik etki bırakma konusunda fark yaratan bir kuvvet çarpanı olacağı hususu akıldan çıkarılmamalıdır.

Siber güvenlik ekiplerinin otomasyon ve yapay zekâyı kullanması, siber olaylara müdahale süreçlerini daha hızlı ve etkin hâle getirmekte kaynakların verimli kullanılmasını sağlamaktadır. Otomasyon, tekrarlayan görevler ve süreçteki insan hatalarını azaltırken, yapay zekâ ise daha karmaşık ve gelişmiş saldırıları tespit ve analiz konularında önemli rol oynamaktadır. Bu noktada dijital vatanın korunması ve dayanıklılığının sağlanması için siber olayların düzgün monitör edilmesi, ağda, sunucularda ve son kullanıcılarda meydana gelen tüm olayların görünürlüğünün sağlanması kritik önem taşımaktadır.

İki ucu keskin bir kılıç gibi olan söz konusu teknolojilerin ahlaki değerler çerçevesinde, dikkatli ve sorgulayıcı bir bakış açısıyla kullanılması gerekmektedir. Potansiyel faydaları ve riskleri göz önünde bulundurarak, siber güvenlik ekiplerinin bu teknolojilere yönelik sürekli olarak güncel kalacak şekilde eğitilmeleri önemlidir.

Siber güvenlik alanındaki gelişmeler, siber tehditlerin doğasını ve karmaşıklığını değiştirmekte ve bu durum, siber güvenlik ekiplerinin müdahale kapasitesini artırmak için yeni stratejilere ihtiyaç duymalarına neden olmaktadır. Sıklıkla ifade edildiği üzere gelişmekte olan yapay zekâ, blokzincir vb. teknolojilerle yeni saldırı yüzeyleri ve yöntemleri geliştirilmiştir. Bununla eş zamanlı olarak, insan kaynağının gelişimi ve dönüşümü ile süreçlerin bu gelişmelere

ayak uyduracak şekilde dinamik uyumu sayesinde siber olaylara tespit ve müdahale de daha bütünleşik ve hızlı evrilmelidir. Bu evrimin yerli ve millî teknolojilerle yapılması ve dijital bağımsızlık hedefinde bir kaldıraç olarak kullanılması hedeflenmelidir.

Yeni ortaya çıkan ve gelişmekte olan teknolojilerle birlikte siber güvenlik konusundaki yükün önemli bir kısmı sıradan vatandaşın omuzlarına yüklenecektir. Örnek vermek gerekirse, gelinen noktada, yapay zekâ sayesinde çok daha gerçekçi ve ikna edici derin sahtecilik (deep fake) yoluyla dolandırıcılığın kolaylaştığı ve bu saldırı yönteminin yaygınlaşacağı söylenebilir.

Her bir sosyal medya platformunun, dijital iletişim için kullanılan her bir temas noktasının sosyal mühendislik saldırıları için birer laboratuvara ve hatta oyun alanına dönüşeceği açıktır. Böylesi bir tehditle etkin mücadelenin sadece SOME'ler tarafından olay müdahale merkezlerinde yapılabileceği iddiası iyimser bir yaklaşım olacaktır. Dolayısıyla sıradan kullanıcının bilgi güvenliği farkındalığının artırılarak teyakkuz hâlinin üst düzeye çıkarılması, şüphe kaslarının güçlendirilmesi ve mücadele için gerekli araç gerecin kendisine sağlanması önem arz etmektedir.

Bireyin veya toplumun zararlı bilgilere ve dezenformasyona karşı direnç gösterme yeteneği, eleştirel düşünme, bilgi güvenliği ve medya okuryazarlığı gibi becerilerin üzerine inşa edilir. Bu yetenekler, dijital dünyada karşılaşılan bilgi kirliliği ve manipülasyonla başa çıkmak için önemlidir. Yüksek dijital bağışıklık, insan bağışıklığında olduğu gibi, tehdit unsurlarıyla savaşma yeteneği ile öne çıkmaktadır. Yapay zekâ ve otomasyon, gelecekte bu bağışıklığın sağlanması için önemli unsurlar olacaktır. Bu teknolojiler, büyük veri analizi ve algılama sistemleri gibi araçlarla zararlı içeriği tanımlamak ve etkili bir şekilde mücadele etmek için kullanılabilir.

İnsan faktörü bu noktada kritik öneme sahiptir; çünkü bireylerin bilinçli bir şekilde bilgiye yaklaşması ve eleştirel düşünme becerilerini kullanarak bilgiyi değerlendirmesi, dijital dünyada güvenliğin sağlanmasında temel bir rol oynamaktadır. Bu nedenle, yapay zekâ ve otomasyon gibi teknolojiler, insanların bilgi güvenliği ve dezenformasyona karşı dirençli olmalarını desteklemek için yardımcı araçlar olarak da kullanılmalıdır.

Dijital bağışıklık, modern dünyanın karmaşık ve sürekli evrilen bir gerçeği hâline gelmiştir. Bu bağlamda, maruz kalınan etkenlerle etkin bir şekilde savaşmak temel bir gerekliliktir. Süreçlerin

titizlikle tanımlanması ve yürütülmesi, kurumların ve bireylerin dijital varlıklarını korumak için önemli bir adımdır.

Diğer yandan, ulusal ve uluslararası düzeyde iş birliği ve bilgi paylaşımı, tehditlerle başa çıkmak için daha güçlü ve koordineli bir yaklaşım sağlar. Varlıkların sınıflandırılması ve zafiyetlerin tespiti, dijital altyapının güvenliğini sağlamak için gereklidir. Sistemlerin sürekli olarak izlenmesi ve geliştirilmesi, tehditlerin hızla değişen doğasına uyum sağlamak açısından önem taşımaktadır. Bununla birlikte, dijital bağışıklığı tam anlamıyla sağlamak için insan faktörüne de yatırım yapılmalıdır. Bilinçli ve eğitimli personel, dijital tehditlere karşı daha dirençli bir organizasyon oluşturmanın anahtarıdır.

Dijital çağın gerekliliklerine uyum sağlamak için teknolojinin yerinde ve doğru kullanılması da kritik öneme sahiptir. Yedekleme ve kurtarma süreçleri ile felaket kurtarma planları, olası risklere karşı hazırlıklı olmanın önemli bir parçasıdır.

Dijital bağışıklığın sürdürülebilirliği; sürekli izleme, analiz ve güncellemeye bağlıdır. Siber tehditlerin izlenmesi, tespiti ve önlenmesi süreci ise karmaşık ve dinamik bir yaklaşım gerektirmektedir. Teknolojideki her türlü ilerlemeye rağmen bu alanda insan sezgisine, öngörü ve sağduyusuna duyulan ihtiyaç azalmayacaktır. Bu nedenle alınacak her türlü teknik ve idari siber güvenlik önlemi, güçlü bir insan kaynağı ve sürekli eğitimle mutlaka desteklenmelidir.

Dijital bağışıklığı güçlendirmek için tespit ve önleme stratejileri hayati öneme sahiptir. Bu stratejiler, olayların hızlı bir şekilde tespiti ve uygun yanıtların verilmesini sağlayarak olası zararları minimize etmeyi amaçlar. Otomasyon ve yapay zekâ gibi teknolojiler, tehditleri hızla tanımlayıp karşı önlemler almayı kolaylaştırarak bu süreci daha etkin hâle getirebilir. Aynı şekilde, yedekleme ve kurtarma süreçleri, olası veri kayıplarına karşı önleyici bir önlem olarak önemli bir rol oynar ve dijital varlıkların güvenliğini sağlamaya yardımcı olur.

Yasal ve teknolojik tedbirlerin alınması, dijital güvenliğin sağlanması için vazgeçilmezdir ve bu çerçevede, organizasyon yapılarının oluşturulması ve olgunlaştırılması tehditlere karşı daha dirençli bir yapı oluşturmak için gereklidir. Ulusal ve uluslararası düzeyde bilgi paylaşımının sağlanması için iş birliğinin geliştirilmesi, dijital tehditlerle mücadelede daha etkili bir yaklaşımı teşvik ederken hem proaktif hem de reaktif tedbirlerin alınması, tehditlere karşı sürekli bir çaba

gösterilmesini sağlar. Bu stratejilerin etkin bir şekilde uygulanması, dijital bağışıklığın güçlendirilmesine yardımcı olacaktır.

Yeni nesil dijital teknolojilerin, siber olayların doğası ve karmaşıklığı üzerindeki etkisi oldukça derinlemesine incelenmelidir. Bu teknolojiler, siber tehditlerin ölçeğini ve karmaşıklığını önemli ölçüde değiştirmiştir. Özellikle kuantum ve blokzincir teknolojileri ve yapay zekânın eğitilmesi, sunduğu fırsatlar ve modellerdeki riskler gibi alanlarda ortaya çıkan eğilimler, siber tehditlerin çok daha karmaşık ve öngörülemez hâle gelmesine katkıda bulunmaktadır.

Yapay zekânın yanlış verilerle eğitilerek zehirlenmesi ve IoT cihazlarının ilerleyen süreçte potansiyel tehdit oluşturması gibi faktörler, siber saldırıların artan bir şekilde karmaşık hâle gelmesine yol açmaktadır. Bu bağlamda, yapay zekânın savunma yeteneklerimize entegre edilmesi ve yapay zekâ destekli araçların kullanılması, siber güvenlik alanında önemli bir stratejik ölçek olarak öne çıkmaktadır.

Saldırı yüzeyinin artması, teknoloji çeşitliliğinin genişlemesi ve sertifikasyon ile akreditasyonun önem kazanması gibi faktörler de ayrıca dikkate alınmalıdır. Özellikle IoT cihazlarının sayısının logaritmik artışı, farklı saldırı vektörlerinin ortaya çıkmasına neden olabilir ve bu da savunmayı daha zorlaştırabilir.

Yapay zekâ, kuantum hesaplama ve otomasyon gibi alanlardaki gelişmelerin, siber olayların öngörülebilirliğini, şiddetini ve ölçeğini de karmaşıklaştırması, savunma stratejilerinin daha dinamik ve çok katmanlı bir yaklaşımla hazırlanması ve sürekli güncel tutulması gerektiği anlamına gelmektedir.

Siber olaylara müdahalede ulusal ve uluslararası iş birliğinin önemi, dijitalleşmenin son derece arttığı günümüz dünyasında daha da belirginleşmektedir. Türkiye'nin bu iş birliklerinde etkin bir rol oynaması ve hedefler belirlemesi önem taşımaktadır. Öncelikle, siber güvenlik ekosistemindeki birçok paydaşın katılımını gerektiren bu yapıda kamu, özel sektör, akademi, askerî kurumlar ve sivil toplum kuruluşları arasında canlı bir iş birliği ve tecrübe paylaşımı artırılarak sürdürülmelidir. Bu etkileşim ortamı, özellikle SOME'ler arasında çok daha etkin bir şekilde kullanılabilir.

Siber güvenlik, multidisipliner bir alan olduğundan, tek bir kurumun çabasıyla başarılamayacak kadar karmaşıklık içermektedir. Bu nedenle, ulusal seviyede birçok kurumun bir araya gelmesi ve iş birliği içinde hareket etmesi tercih değil, bir mecburiyet olarak görülmelidir. Siber olayların öncesi, olay anı ve sonrasında yapılması gerekenlerin bilinmesi ve uygulanması, alınan derslerin kaydedilmesi, tecrübe paylaşımı ve geri besleme hususları büyük önem taşımaktadır. Tehdit istihbaratı paylaşımı da siber olaylara müdahale açısından en kritik unsurdur.

Uluslararası iş birliği ise siber güvenlik anlayışının şekillendirilmesi, ulusal politikalarımızın empozesi ve bilgi alışverişinin artırılması açısından önemli bir diplomatik araçtır. Bu konuda, uluslararası seviyede iş birliği anlaşmaları ve ortak platformlar oluşturulmaktadır. Kamu kurumlarının iletişimini artırmak ve kurumlar arası iş birliğini güçlendirmek kadar küresel ağlarla irtibatla ve uyumlu olmak da önemlidir. Türkiye'nin ulusal düzeyde USOM gibi yapıları güçlendirmesi ve uluslararası düzeyde benzer organizasyonlarla ortaklıklarını geliştirmesi gerekmektedir. Bu şekilde, koordineli bir şekilde hareket ederek sadece uygulayan değil, aynı zamanda yön veren bir pozisyonda olunabilir.

Sonuç olarak, siber güvenlik alanındaki gelişmelerin takip edilmesi, ulusal ve uluslararası iş birliklerinin güçlendirilmesi, otomasyon ve yapay zekâ gibi yeni teknolojilerin dikkatlice kullanılması ve siber güvenlik ekiplerinin sürekli eğitilmesi, Türkiye'nin siber güvenlik alanındaki müdahale kapasitesini artırmak için atılması gereken adımlar arasında yer almaktadır.

Özetle, değişen ve gelişen teknolojiler ile beraber evrilen siber olaylara müdahale ve önleyici eylemler için de yenilikçi yaklaşımlar sergilenmesi bir mecburiyet olarak görülmektedir. Bu yaklaşımların millî bilinç ve disiplinle ele alınması ayrıca önemlidir. Derlenmiş diğer öneriler ise şu şekilde sıralanabilir:

- Yapay Zekâ, Blokzincir, Bulut Bilişim, IoT cihazları ve Kuantum teknolojileri gibi yeni teknolojilerin siber tehditlerin ölçeğini ve karmaşıklığını artırdığı göz önünde bulundurularak, siber güvenlik önlemlerinin bu gelişmelere ayak uyduracak şekilde geliştirilmesi gerekmektedir.
- Yerli ve bağımsız teknolojilere verilen destek artırılmalı ve vatandaşın bilgi güvenliği farkındalığının yükseltilmesi için çalışmalar yapılmalıdır.

- Dijital vatanın korunması ve dayanıklılığının sağlanması için siber olayların sürekli monitör edilmesi, ağda, sunucularda ve son kullanıcılarda meydana gelen tüm olayların analizi kritik önem taşımaktadır.
- Değişen teknolojiler ile beraber evrilen siber olaylara müdahale ve önleyici aksiyonlar için yenilikçi yaklaşımlar sergilenmeli ve bu yaklaşımların millî bir bilinç ve disiplinle ele alınması önemlidir.
- Dijital bağışıklığın temel gerekleri olan maruz kalma ve etkenlerle baş etme yeteneğinin güçlendirilmesi için proaktif ve reaktif tedbirler alınmalı, bireylerin ve toplumun zararlı bilgilere ve dezenformasyona karşı direnç gösterme yetenekleri artırılmalıdır.
- Siber güvenlik ekiplerinin otomasyon ve yapay zekâ kullanımının rolü göz önünde bulundurularak, bu teknolojilerin potansiyel faydaları ve riskleri değerlendirilmeli ve dikkatlice kullanılmalıdır.
- Ulusal ve uluslararası iş birliğinin önemi vurgulanmalı ve kurumlar arası iş birliği güçlendirilmelidir. Türkiye'nin uluslararası politikalara yön veren bir konumda olması ve uluslararası iş birliklerinde aktif rol alması hedeflenmelidir.

Bu bağlamda, uzun tartışmalar ve kapsamlı mülahazalar sonucunda ortaya çıkan görüş, değerlendirme, tespit ve önerilerin detaylı ve nispeten ham sürümüne Ek-4'ten ulaşılabilir. Bu kapsamda ayrıca, somut birkaç çözüm teklifi, nasıl ve niçin sorularına da belirli oranda cevap verebilecek şekilde aşağıda sunulmuştur. Aşağıda bir düzine kadarına değinilen konular, aslında büyük oranda Şura çalışmaları sırasında berraklaşan ve tamamı Ek-1'de sunulan anket sorularındaki eylem maddelerinden türemiştir.

4. 1. Post Kuantum Kriptografi

Post-kuantum kriptografi veya kuantum sonrası şifreleme, mevcut kriptografik algoritmaların, kuantum bilgisayarların gelişimi ile kırılabilir hâle gelme riskine karşı bir yanıt olarak gereklidir. Gelişmiş ülkelerin de strateji belgelerinde öncelikli olarak yer verdikleri bu konuda, kuantum bilgisayarlar, *Shor Algoritması* gibi tekniklerle RSA, ECC gibi yaygın

kriptografik yöntemleri etkisiz hâle getirebilir. Bu durum, veri güvenliği ve gizliliği konusunda ciddi riskler oluşturabilecektir.

Kuantum sonrasına hazırlıksız yakalanıldığı ve uygun geçiş yapılmadığı takdirde, gelecekte mevcut kriptografik sistemlerin kuantum bilgisayarlar tarafından muhtemelen kırılmasıyla birlikte, kişisel verilerin mahremiyeti ve kurumsal bilgilerin gizliliği tehlikeye girecek, finansal sistemler, e-ticaret işlemleri ve ülke ekonomisi savunmasız hâle gelecek, görev kritik devlet kurumları başta olmak üzere stratejik varlıkların bekası tehlikeye düşebilecek, en hafif yönüyle itibar kaybı yaşanacaktır. Bu anlamda post-kuantum kriptografi konusunda eyleme geçmek, gelecekteki siber tehditlere karşı dayanıklı bir güvenlik altyapısı kurmak için hayati önem taşımaktadır.

Kuantum sonrasına yeterli hazırlık ve uygun geçiş sağlandığında ise; yeni yapıya karşı dayanıklı bir güvenlik altyapısı oluşturulmuş, ülke verisinin gizliliği ve bütünlüğü korunmuş, vatandaşın güven ve aidiyeti artmış, ülke itibarı güçlenmiş, mevcut ve gelecekteki siber tehditlere karşı proaktif bir yaklaşım sergilenmiş, istihbari, siyasi ve ekonomik olarak önemli bir kaldıraç edinilmiş olacaktır.

Son derece ileri teknolojileri barındıran bu alanda gelişim sağlamak için ciddi gayret ve kaynak gereksinimi bulunmaktadır. Münferit olarak tek bir kurum veya şirketin üstesinden gelmesi zor görünen söz konusu araştırma ve geliştirme alanında, koordinatör bir kurum (Örn. TÜBİTAK) belirlenerek, ilgili bakanlıklar, üniversiteler, şirketler ve uluslararası ortaklıkların katkı ve katılımıyla ilerlenmesi hedeflenmelidir.

Çalışmalarda; mevcut kriptografik algoritmaların ve kriptoloji altyapısının detaylı analizi, paydaşların eğitim ve ortak faaliyetler yoluyla konuya angaje edilmesi, alandaki son gelişmelerin takibi, izlenmesi ve uyumlandırma planlamaları, kuantum sonrası algoritmaların araştırılarak uygun olanların belirlenmesi, kavramsal doğrulaması yapılan algoritmaların pilot projelerde uygulanarak denenmesi, tam geçiş sürecinin planlanması gibi aşamalar öngörülebilir.

Faaliyetlerin icra edileceği fiziksel altyapının hazırlanması, post-kuantum destekleyen kriptografik kütüphanelerin oluşturulması, algoritmaların sına ve güvenlik ölçümleri için simülasyon ve test araçlarının belirlenmesi ile eğitim materyallerinin oluşturulması ilk akla gelen faaliyet alanlarıdır.

Emek yoğun ve akıl teri gerektiren çalışmalarda üst düzey nitelikli personel gerekliliği açıktır. Alanında uzman ve temayüz etmiş teorik fizikçiler, kuantum fizikçileri, atom altı/parçacık fiziği araştırmacıları, nükleer fizik uzmanları, bilgi sistemleri ve bilgi güvenliği uzmanları, elektrik elektronik mühendisleri, kriptografik araştırmacılar, kuantum bilgi sayımı (computing) uzmanları, matematikçiler, inatçı, kararlı ve sebat etmesini bilen bir üst yönetim ve iş birliği ile ortak üretimi önceleyen bir çalışma ekibi ön gerekliliktir.

4. 2. Biyo-ilhamlı Dijital Bağışıklık

Biyo-ilhamlı dijital bağışıklık, doğadan ilham alınarak dijital sistemlerin güvenliğini ve dayanıklılığını artırmayı amaçlayan bir yaklaşımdır. Bu yöntem, biyolojik organizmaların bağışıklık sistemlerinden esinlenerek, dijital ortamda benzer savunma mekanizmaları oluşturmayı hedefler. Siber tehditlerin hızla evrildiği günümüzde, geleneksel güvenlik yöntemleri yetersiz kalmakta ve dijital sistemlerde daha dinamik ve adaptif bir savunma yapısına ihtiyaç duyulmaktadır. Bu alandaki çalışmalar, dijital güvenlikte yeni bir dönemin başlangıcını temsil etmektedir.

Biyo-ilhamlı dijital bağışıklık yeteneğinin edinilmediği durumda; daha sofistike ve hedefe yönelik artan siber saldırılar karşısında yetersiz kalınabilir, hassas verilerin korunmasındaki yetersizlikler nedeniyle veri ihlalleri yaşanabilir, bu hem bireysel hem de kurumsal düzeyde büyük kayıplara yol açabilir, kritik sistemlerdeki aksaklıklar operasyonel kesintilere neden olabilir ve iş sürekliliği riske girebilir, güvenlik ihlalleri sonrasında oluşacak zararlar ve onarım maliyetleri, büyük finansal yükler getirebilir. Dahası, alanda azalan iş gücü ve artan saldırılar karşısında çaresiz kalınabilir.

Biyo-ilhamlı dijital bağışıklık sistemi geliştirilerek bu teknolojiye sahip olunduğu takdirde ise; adaptif ve proaktif gelişmiş savunma mekanizmaları ile siber tehditlere karşı daha güçlü bir koruma sağlanır, tehditlerin hızla tespit ve bertaraf edilmesi, zarar oluşmadan önce müdahale edilmesini sağlar, hassas verilerin korunması ve gizliliğinin sağlanması ile güvenilirlik artar, kritik sistemlerin kesintisiz çalışması büyük oranda garanti altına alınarak, operasyonel verimlilik artar.

Bahse konu yeteneğin kazanılmasında, adından da anlaşılacağı gibi biyolojik sistemlere detaylı hâkimiyet kadar bu sistemlerin dijital ortama bağışıklık boyutuyla nasıl uyarlanabileceğine

dair bilgi ve birikim gerekir. Bu yönüyle ağırlıklı olarak disiplinler arası bir yaklaşım gereklidir. Siber tehditlerin sürekli evrildiği göz önünde bulundurularak, dijital bağımsızlık sistemlerinin de sürekli güncellenmesi ve adaptif hâle getirilmesi önemlidir. Mevcut güvenlik sistemleri ile entegrasyonun sorunsuz olması ve uyumun sağlanması gerekliliğinin yanı sıra çalışanların ve diğer paydaşların bu yeni sistem hakkında eğitilmesi ve bilinçlendirilmesi önemlidir.

Bu alanda olası bir çalışmanın aşamalarını sıralamak gerekirse bunlar; mevcut sistemlerin analiz edilmesi ve dijital bağımsızlık sistemine geçiş için planlama yapılması, uygun çözümlerin araştırılarak geliştirilmesi, geliştirilen çözümlerin pilot projelerde test edilmesi ve performans değerlendirmelerinin yapılması, başarılı pilot projeler sonrasında, sistemin genel kullanıma verilmesi ve entegrasyonun sağlanması, sistemlerin sürekli izlenmesi, tehditlerin analiz edilmesi ve alınan geri beslemeler doğrultusunda gerekli güncellemelerin yapılması olarak sıralanabilir.

Çözümün hayata geçirilmesi ve geliştirilmesinde; tasarım, simülasyon ve modelleme araçları, siber tehdit istihbarat imkân ve gereçleri ile ürün güvenlik analiz ve testleri için uygun yeteneklerin ilk etapta edinilmesi gerektiği ifade edilebilir.

Paydaş gruplar genel başlıklar altında sıralanacak olursa; yeterli sayıda ve nitelikte araştırma ve geliştirme ekibi, bilişim ve güvenlik uzmanları, yazılımcılar, adli bilişimciler, bilgisayar korsanları ve biyolojik sistemler konusunda uzman danışman ve araştırmacılar ön plana çıkan aktörlerdir.

4. 3. Yapay Zekâ (YZ) Destekli Otonom Siber Müdahale

Bu yaklaşım, giderek artan ve daha karmaşık hâle gelen siber saldırılara karşı hızlı ve etkili çözümler sunmak için gelecekteki en etkili yol olarak görülmektedir. Geleneksel güvenlik sistemleri, büyük hacimli ve çok çeşitli siber tehditlerle başa çıkmakta zorlanırken, YZ teknolojileri, bu tehditleri hızlı bir şekilde tespit edip yanıt verebilme yeteneğine sahiptir. Bu sayede, siber güvenlik ekiplerinin yükü hafifletilir ve kritik olaylara daha stratejik müdahaleler sağlanabilir. Siber olaylara yapay zekâ destekli otonom müdahale, modern siber tehditlere karşı etkin ve hızlı çözümler sunarak, dijital güvenlikte yeni bir dönemin kapısını aralamaktadır. Bu alanda yapılacak yatırımlar ve geliştirmeler, siber güvenlikte önemli kazanımlar elde edilmesini sağlayacaktır.

YZ destekli otonom müdahale yeteneğinin kazanılmaması ve uygulanmaması durumunda; siber olaylara manuel müdahale süreçleri daha uzun sürebilir ve bu durum geç müdahale nedeniyle saldırının etkilerini artırabilir, zamanında tespit ve müdahale edilemeyen saldırılar, ciddi veri kayıplarına ve ihlallerine yol açabilir, kritik sistemlerin saldırıya uğraması durumunda, iş süreçlerinde aksaklıklar ve kesintiler yaşanabilir, güvenlik ihlallerinin tespiti ve onarımı, uzun vadede daha yüksek maliyetler oluşturabilir.

Söz konusu sistemlerden yararlanmak suretiyle; YZ algoritmaları, tehditleri gerçek zamanlı olarak tespit edip hızlı müdahale sağlayabilir, otomatik süreçler sayesinde, zaten sayıca azalmış durumda olan siber güvenlik ekiplerinin manuel iş yükü azalır ve stratejik kararlar almaya odaklanabilirler, karmaşık ve gelişmiş siber saldırılara karşı daha etkin bir koruma sağlanır, kritik sistemlerin kesintisiz çalışması sağlanarak operasyonel verimlilik artırılır ve uzun vadede siber saldırılara karşı daha etkili ve ekonomik çözümler elde edilir.

Siber olaylara YZ destekli otomatikleştirilmiş müdahale yeteneğinin kazanılmasında; YZ algoritmalarının eğitimi için yüksek kaliteli ve yeterli miktarda veri sağlanmalıdır. Ayrıca, geliştirilen YZ modellerinin güvenilir ve doğru sonuçlar verdiğinden emin olunması, işin önemli bir boyutudur. Bu nedenle, oluşturulan sistemler sürekli izlenmeli ve yeni tehditlere karşı güncellenmelidir. Mevcut güvenlik altyapısıyla uyumlu ve entegre çalışacak çözümler tercih edilmeli, ilgili paydaşlara gerekli eğitimler yeteri kadar verilmelidir.

Çalışma ekibinde, yukarıdaki maddede sıralı aktörlere ilave olarak yapay zekâ uzmanları ile veri bilimciler de dâhil edilmelidir.

4. 4. Siber Seferberlik

Küreselleşen dünyada devletler, sürekli olarak siber tehditlerle karşı karşıya kalmakta ve bu tehditler, ulusal güvenlik, ekonomi ve toplum üzerinde büyük riskler yaratmaktadır. Siber seferberlik organizasyonu, ülkenin sahip olduğu her türlü dijital imkân ve yeteneğin, tehlike gördüğü hasma yönlendirilmesi maksadıyla yapılan teşkilatlanma ve gerekli diğer hazırlıkların tamamı olarak ifade edilebilir.

Bu kapsamda mevcut bulunan fiziki bilişim altyapısı, işlemci gücü, hafıza ve diğer donanımların yanı sıra, bu yapının üzerinde koşan her türlü yazılım ile bunları kullanan insanların

bilgi ve birikimini de kapsamaktadır. Ülke sınırları içerisindeki hatta kimi sempatican ve gönöl coğrafyası mensupları da dâhil edildiğinde ülke sınırlarını da aşan bu birikim ve kabiliyet, iyi organize edildiğinde etkisi öngörülemez bir kuvvet çarpanı olarak yarar sağlayabilir.

DDoS saldırılarından, hedef odaklı gelişkin ve süreklilik arz eden nokta siber saldırılara kadar geniş bir yelpazede inisiyatif almayı kolaylaştırıcı bir etken olacağı düşünülen bahse konu yetenek kazanıldığında, kendisine yöneltilen saldırıları defetmede de ciddi avantaj sağlayacaktır.

Organizasyon için, ülkemiz genelinde yeni nesil yüksek hızlı haberleşme altyapılarının (fiber, 4,5G ve ötesi) yaygınlaştırılması ve İnternet erişimi bant genişliğinin artırılması, mevzuatta ihtiyaç duyulacak güncellemelerin yapılması, envanterin sürekli güncel tutulması hususları, kritik adımlar olarak tanımlanabilir.

Müstakilen bu göreve memur edilmiş merkezi bir otorite ve koordinatör makama ihtiyaç duyulan yapıda; güvenlikten sorumlu ilgili kurumlar, özel sektör ve akademik camia arasında etkin bir iş birliği ve en önemlisi yükümlü vatandaşlar ve gönüllüler ile yakın koordinasyon şarttır.

Siber seferberlik planının hazırlanması ve ihtiyaç analizinin yapılması, tüm paydaşların eğitilmesi için gerekli programlarının düzenlenmesi, mevcut yetenek envanteri ile birlikte ilişki ve bağımlılık haritalama, potansiyel risklerin analizi ve yönetim stratejilerinin geliştirilmesi, kullanılacak teknolojik araç ve gereç seçimi, bunların test ve değerlendirmesi ile iletişim ve koordinasyon platformlarının hayata geçirilmesi belli başlı aşamalar olarak sıralanabilir.

Hükümet ve düzenleyici kurumlar, kritik altyapı operatörleri, teknoloji ve güvenlik şirketleri, akademik kurumlar, sivil toplum kuruluşları ve vatandaşlar konuya ilişkin ana aktörlerdir.

4. 5. Ulusal Siber Görev Gücü

Ulusal çapta siber saldırıların sayısı ve karmaşıklığı artmaktadır. Enerji, su, sağlık, finans ve güvenlik gibi kritik altyapıların korunması için merkezi bir müdahale ve koordine yeteneği gereklidir. Bu kapsamda görevli, farklı kurumlar arasındaki koordinasyon eksikliklerini gidermek ve gerektiğinde maruz kaldıkları siber saldırılara zamanında müdahale etmek amacıyla merkezi bir görev gücüne ihtiyaç vardır.

Bu yapı kurulmadığı takdirde, kritik altyapı ve hizmetlerde büyük kesintiler ve zararlar yaşanabilir, büyük ölçekli siber saldırılar ekonomiye ciddi zararlar verebilir, farklı kurumlar arasındaki bilgi ve iş birliği eksikliği, güvenlik açıklarının büyümesine neden olabilir.

Aksi durumdaki iyi senaryoda ise ulusal güvenlik ve kritik altyapıların korunması sağlanır, siber saldırılardan kaynaklanan ekonomik zararlar minimize edilir, farklı kurumlar arasında etkin iş birliği ve koordinasyon tesis edilir.

Benzetmek gerekirse Polis Özel Harekât veya Özel Kuvvetler Komutanlığı benzeri elit, yetkin, yetenekli, kurumlara vakıf, yatay ve dikey koordine içerisinde, her olaya değil, belirli kritik olaylara müdahale etmesi gereken bu yeteneğin hayata geçirilmesi ve sürdürülmesinde; kamu ve özel sektör arasında güçlü iş birliği ve koordinasyon sağlanması, görev gücünün çalışmalarında gizlilik ve güvenliğin en üst düzeyde tutulması ve ilgili paydaşların sürekli olarak eğitilmesine dikkat edilmelidir.

Gerekli yasal ve düzenleyici çerçevenin oluşturulması, görev gücünün amaçları, hedefleri ve stratejilerinin belirlenmesi, yetenekli insan kaynağı, teknolojik altyapı ve finansal kaynakların sağlanması ile operasyonel plan ve süreçlerin oluşturulması önemli kilometre taşları olarak tanımlanabilir.

4. 6. Temel Bilişim Servislerinin Vatandaşa Bedelsiz Sunulması

Yerli ve millî temel bilişim hizmetleri (işletim sistemi, elektronik posta, veri depolama alanı, anti-viral ürünler, güvenlik duvarı, üretken yapay zekâ vb.) vatandaşla ücretsiz sunulmalıdır.

Vatandaşlarımız tarafından hâlihazırda kullanılan gündelik bilgi sistem temel servislerinin hemen tamamı yabancı menşelidir. Bunlara örnek vermek gerekirse, ağırlıklı olarak; işletim sistemi (Windows) ve ofis uygulamaları (Office) olarak Microsoft, İnternet tarayıcı, e-posta (Gmail) ve arama motoru (Chrome) olarak Google, sosyal medya (Facebook) ve anlık haberleşme (Whatsapp) olarak Meta, belirli bir kesim tarafından kullanılan Apple ve ürünleri, bulut depolama hizmetleri olarak hemen hepsi ve son dönemde de Chat GPT üretken yapay zekâ ve türevleri sıralanabilir. Sıralı bu örneklerle Çin menşeli TikTok ve Rus arama motoru Yandex ve diğer bazı yabancı güvenlik ürünleri eklenebilir.

Bu durum, vatandaşa ait ülke verisinin toplamda yaklaşık çeyrek yüzyıldır yurt dışında, ağırlıklı olarak da ABD’de, işlendiği ve depolandığını göstermekte, hem istihbari hem de ekonomik değer olarak bir zafiyet ve sömürüye işaret etmektedir.

Bu anlamda kendi bilişim hizmetlerini sunma ihtiyacı, hem millî güvenlik hem de ekonomik bağımsızlık açısından büyük önem taşımaktadır. Yabancı bilişim hizmetlerine olan bağımlılık, verilerin güvenliği ve gizliliği konusunda ciddi riskler oluşturmakta, ayrıca, yerli çözümler, ülkenin teknolojik altyapısının ve yazılım endüstrisinin gelişmesine katkı sağlayarak ekonomik büyümeyi teşvik edebilmektedir.

Her Türk vatandaşına, doğumundan ölümüne kadar kullanacağı bu temel servislerin ücretsiz sağlanması ile söz konusu zafiyetin önüne geçilmesi ve vatandaştaki aidiyet ve güven duygusunun artırılması sağlanabilir.

Bu kapsamda vatandaşa@eposta.tr uzantılı bir e-posta adresi verilebilir. Bu adresin kullanılması Kayıtlı Elektronik Posta (KEP) benzeri asgari olarak devlet işlerinde zorunlu tutulabilir. Tebligat, yazışma vb. söz konusu adres üzerinden yapılabilir. Buna ilave olarak her kademedeki öğrenciye MEB tarafından da@k12.edu.tr uzantılı e-posta adresi ilaveten verilmelidir.

Konu hakkında ayrıca, yerli işletim sistemi ve ofis yazılım paketi açık kaynak olarak kullanıma sunulabilir. Bu yazılımları kullananlara bazı teşvik ve ayrıcalıklar sunulabilir. Bahse konu hizmetler, bulut depolama alanı (örneğin vatandaş başına 100 GB) ile desteklenebilir ve tamamı buluttan da sağlanabilir.

Sosyal medya ve anlık mesajlaşma uygulamalarına ikna ve geçiş sürecinde görece daha fazla zorluk yaşanabilir. Ancak iyi bir çalışmayla bu alan da canlandırılabilir ve cazip kılınabilir.

Siber güvenlik ürünleri ile yapay zekâ konusu ise vatandaşa sunulması gerekli hizmetlerden diğerleri olacaktır. Bu sayede toplumun konuya ilgi ve aşinalığı ile birlikte genel güvenlik durumu da artırılabilecek, daha kaliteli ve verimli çıktıları olabilecektir.

E-posta, veri depolama alanı ve siber güvenlik ürünleri (özellikle mobil platformlar için) hemen verilebilecekken, yerli işletim sistemi, yerli ofis yazılımları ve üretken yapay zekânın 2030 yılına kadar, yerli sosyal medya platformu ve anlık mesajlaşma uygulamasının ise iyi bir planlama

ve benimsetme kampanyasıyla birlikte 2030 sonrasında hayata geçirilebilmesinin mümkün olduğu değerlendirilmektedir.

Çalışmalarda kullanım alışkanlıklarını iyi analiz etmek ve kullanıcı deneyimini öncelikli olarak ele almak stratejik önemdedir. Bu süreçte dikkatli planlama, kullanıcı odaklı yaklaşım ve güçlü bir iş birliği ağı oluşturmak kritik önem taşımaktadır. Başarılı bir geçiş süreci, ülkenin uluslararası alanda rekabet edebilirliğini artıracak ve vatandaşlarına güvenli, bağımsız bilişim hizmetleri sunulmasını sağlayacaktır.

4. 7. Müşterek Siber İstihbarat ve Tecrübe Paylaşım Platformu

Siber tehditlerin giderek daha karmaşık ve yaygın hâle gelmesi, tek başına hareket eden kurumların bu tehditlerle başa çıkmasını zorlaştırmaktadır. Müşterek siber istihbarat ve tecrübe paylaşım platformu, kurumların ve paydaşların siber tehditlere karşı ortak bir savunma mekanizması oluşturmasını sağlar. Bu platform, tehdit bilgilerini, saldırı tekniklerini ve en iyi uygulamaları paylaşarak, tüm katılımcıların güvenlik durumunu iyileştirir ve saldırılara karşı daha dirençli hâle getirir.

Müşterek bir siber istihbarat ve tecrübe paylaşım platformunun olmaması durumunda; tehditlerin geç tespit edilmesi daha büyük zararlar doğurabilir, zira aynı saldırı yöntemleri farklı kurumlarda tekrar tekrar başarılı olabilir. Çok açıktır ki paylaşılmayan bilgiler nedeniyle kurumlar, benzer güvenlik açıklarını kapatmada başarısızlık yaşayabilir. Kurumlar arasındaki iş birliği ve koordinasyon eksikliği, topyekûn bir zafiyet yaratarak siber güvenliği zayıflatabilir. Ayrıca tek başına yapıldığında siber savunma maliyetleri daha yüksek olabilir ve kaynak israfına yol açabilir.

Söz konusu platform, kurulacak bir müşterek siber güvenlik mükemmeliyet merkezinin çatısı altında da yer alabilir. Platform sayesinde; güvenlik açıkları, tehdit ve saldırılar erken tespit edilerek önleyici tedbirler alınabilir, ortak bilgi ve tecrübelerle, daha etkili savunma stratejileri geliştirilebilir. Yapı, ulusal çapta olabileceği gibi sektörel bazlı da kurgulanabilir. Yapılacak tecrübe paylaşımları ile benzer güvenlik açıklarının hızla kapatılması sağlanır. Kurumlar arasında iş birliği, ortak anlayış ve koordinasyon artarken karşılıklı güven gelişir. Bütün bu faydalara ek olarak ortak savunma çözümleri, maliyetlerin paylaşılmasını ve azaltılmasını sağlar.

Adı geçen platformun oluşturulmasında dikkat edilmesi gerekli ilke ve prensipler şu şekilde sıralanabilir. Platformun paydaşı her kurum ve kuruluş, yaptığı katkı oranında ortamdan yararlanmalıdır. Her kurum ve kuruluşun kendi ölçeği nispetinde yaptığı paylaşım kadar platformdan yararlanabilmesine izin veren bir yapı tasarlanması, paylaşım kültürünü harekete geçirerek bu anlamda teşvik edici bir rol oynayacaktır. Platformun yararları görüldükçe ve duyuldukça, hem paydaşların sayısı hem de onların platforma nitelikli katkısı artacaktır.

Paylaşılan bilgilerin gizliliği ve güvenliğinin korunması hususu yasal çerçevede teminat altına alınmalıdır. Anonimleştirerek paylaşılan bilgilerin doğruluğu ve güvenilirliği sağlanmalı, alınan dersler kütüphanesinin oluşturulması maksadıyla tüm paydaşların aktif katılımı ve iş birliği teşvik edilmelidir. Platform sürekli güncellenmeli ve yeni tehditlere karşı adaptif ve proaktif olmalıdır.

Müşterek siber istihbarat ve tecrübe paylaşım platformu, siber güvenlikte kolektif bir yaklaşım benimseyerek, kurumların ve paydaşların tehditlere karşı daha dayanıklı ve dirençli hâle gelmesini sağlayacaktır.

4. 8. Yerli Siber Güvenlik Ürünlerinin Önündeki Psikolojik Bariyerin Kaldırılması

Hâlihazırda, yerli siber güvenlik ürünlerine karşı belirli oranda bir güven eksikliği ve yabancı ürünlerin daha güvenilir, maliyet etkin ve idamesi mümkün olduğuna dair bir algı mevcuttur. Mevcut bu algının somut veya soyut, haklı veya haksız gerekçeleri bulunsa da genel durumun bu şekilde olduğu yaygın olarak kabul görmektedir.

Bu noktada, yerli ürünlerin yeterince teşvik edilmediği ve kaynaklarının sınırlı olduğu noktasında tespit ve önermelerin yanı sıra, kullanıcı cephesinde de aynı ürünün yabancı muadiline nazaran daha yetersiz ancak daha maliyetli olduğu ve satış sonrası yeterli destek imkânları bulunmadığına dair iddialar mevcuttur. Tüm bunlara ilave olarak, sadece yeterli bilgi ve ilgi eksikliğinden kaynaklanan ve mesnetsiz ön yargılarla desteklenen bir de psikolojik bariyer, yanlış ve yanlış bir olumsuz algı bulunmaktadır.

Söz konusu psikolojik bariyer nedeniyle ilgili sektör yeterince gelişmemekte ve arzu edilen noktaya ulaşamamakta, yerli ürünler olgunlaşmadığı durumda yabancı muadili tercih edilmekte ve kısır döngü böylece sürüp gitmektedir. Bu kısır döngünün en sevimsiz sonucu ise

ekonomik kayıplar, teknolojik geri kalmışlığın kemikleşmeye başlaması ve nitelikli beyinlerin göç suretiyle yitirilmesidir.

Bu husus böyle devam ettiği takdirde yabancı ürünlere olan bağımlılık artmaya devam edecek, yerli ürünlerin gelişimi ve benimsenmesi engellenecektir. Ekonomik kayıpların yanında millî güvenlik riskleri de bu olumsuz tablo dahilindedir.

Bu kısır döngünün bir şekilde kırılması gereklidir ve kırıldığı durumda yerli ürünlere olan güven artar, kullanıcılar yerli ürünleri tercih eder. Kendi teknolojimize dayalı güvenlik çözümleri millî güvenliği güçlendirir, ekonomik büyüme sağlar.

Bu bariyerin aşılabilmesi için ihtiyaç duyulan saha çalışmalarının ve yapılacak diğer araştırma sonuçları saklı kalmak kaydıyla önerilebilecek bir dizi somut önlem şu şekilde sıralanabilir.

Yerli ürünlerin güvenliği ve etkinliği konusunda şeffaf olunmalı, kullanıcıların güveni kazanılmalıdır. Yerli ürünlerin kalitesi ve performansı yüksek tutulmalı, uluslararası standartlara uygun olmalıdır. Kullanıcılara yerli ürünlerin avantajları ve güvenilirliği hakkında sürekli eğitim ve bilgilendirme yapılmalı, temas sürdürülmelidir. Buna ilave olarak, yıllara sâri açık kaynak veya yerli güvenlik ürünlerine kademeli olarak geçiş ana planı oluşturulmalı ve bu husus yeterli mevzuatla da desteklenmeli, kamu tedariklerinde bu husus bilhassa gözetilmelidir.

4. 9. Dezenformasyona Karşı Otomasyon

Günümüzde İnternet ortamında hızla yayılan yanlış, yanlış, yanıltıcı ve yönlendirici bilgilerin varlığı, toplumları ciddi şekilde etkilemektedir. Bu tür dezenformasyon içerikleri, vatandaşların doğru bilgiye ulaşmasını engelleyerek manipülasyonlara zemin hazırlamaktadır.

Dezenformasyon adı verilen yanıltıcı bilgilerin kasıtlı olarak yayılması, toplumsal huzursuzluk, güvensizlik ve yanlış kararlar alınmasına sebep olmaktadır. Öyle ki kriz, afet ve gerginlik durumlarında kitleleri kışkırtmak ve yöneltmek, sosyal medya ve dijital platformların da hızla yaygınlaşmasıyla daha kolay hâle gelmiştir.

Toplumu koruma ve doğru bilgilendirme amacıyla dezenformasyon karşısında bilginin doğruluğunu, güncelliğini ve tarafsızlığını gösteren bir otomasyon sistemi, bireylerin doğru bilgiye ulaşmasını sağlamak suretiyle, kamu düzeni ve güvenliğini artırabilir.

Böylesi bir sistemin tasarımında öncelikli olarak şu ilkelere uymak gerekir. Kullanıcı bilgileri ve doğrulama süreçlerinin gizliliği ve güvenliği korunmalıdır. Doğrulama sürecinde tarafsızlık ve objektiflik ilkesine uyulmalıdır. Sistem kullanıcı dostu ve herkesçe erişilebilir olmalı, asgari dijital okuryazarlık bilgisiyle kullanılabilmelidir. Dezenformasyon taktik ve tekniklerine karşı sistem sürekli güncellenmelidir.

Sistem geliştirme aşamaları ise; toplumun bilgi doğrulama ihtiyacının analizi ve planlanması, dezenformasyonun tespiti için gerekli verilerin toplanması ve işlenmesi, bilgi doğrulama algoritmalarının geliştirilmesi, modellenmesi ve testi, pilot uygulamalar ve geri bildirimlerin alınması, genel kullanım için devreye alınması ve mevcut dijital platformlarla entegrasyonunun sağlanması olarak sıralanabilir.

Tahayyül edilen otomasyon sisteminin kullanıcı arayüzü, kullanıcıların bilgi doğrulama sürecini kolay ve etkili bir şekilde gerçekleştirebilmeleri için tasarlanmalı, sade, anlaşılır ve kullanıcı dostu olmalıdır. Bilgi doğrulama hizmetine hızlı erişim sağlayacak bir etkileşim yöntemi kullanılmalıdır. Arayüz, mobil cihazlarda da sorunsuz çalışacak şekilde tasarlanmalıdır.

Bilgi doğrulama modülünün de asgari olarak şu tür birtakım özelliklere sahip olması beklenmelidir. Örneğin; kullanıcıların belirli bir bilgi veya haberin doğruluğunu arayabilecekleri bir arama çubuğu bulunmalı, karşılaştıkları metin veya görseli sisteme yükleyerek doğruluğunu kontrol edebilmeli, şüpheli buldukları bir web sitesi linkini girerek o site içeriğinin doğruluğunu kontrol edebilmelidir. Bunlara ek olarak, kullanıcıların doğrulama işlemi sırasında veya sonrasında anlık bildirimler alması ve yanlış bilgi tespit edildiğinde kullanıcılara uyarı mesajları iletilmesi gibi özellikler de düşünülebilir.

Sistemin etkin ve sağlıklı işleyebilmesi için, ilgili düzenleyici kurumlar, konvansiyonel medya kuruluşları, sosyal medya yetkilileri, akademik kurumlar ve araştırmacılar, sivil toplum kuruluşları ve teknoloji şirketleri gibi paydaşların ortak anlayış, iş birliği ve koordine içerisinde olmaları gerekmektedir.

4. 10. Ulusal Sosyal Mühendislik Tatbikatları

Sosyal Mühendislik Tatbikatları genellikle kurum çalışanlarının veya sıradan vatandaşın sosyal mühendislik saldırılarına karşı tepkisini ve savunma kapasitesini test etmek ve geliştirmek amacıyla yapılan bir dizi faaliyet manzumesidir.

Bilindiği üzere sosyal mühendislik, bireyleri gizli bilgilerini ifşa etmeye veya güvenliği tehlikeye atan eylemleri gerçekleştirmeye yönlendirmeye ikna sürecini içerir. Sosyal mühendislik tatbikatları da benzer yöntemlerle ancak zarar vermeden farkındalık yaratma motivasyonu ile icra edilir.

Bu tatbikatların ana amacı, güvenlik protokollerindeki zayıflıkları belirlemek ve bireyleri sosyal mühendislik saldırılarını daha iyi tanımaları ve bunlara nasıl yanıt verecekleri konusunda eğitmek ve bilgilendirmektir. Daha özelde ise; vatandaşlara sahte oltalama e-postaları göndererek, bu tür dolandırıcılık girişimlerine düşüp düşmediklerini ve bu tür girişimleri nasıl tanıyacaklarını öğretmek, bireylerin, sahte bir bahane altında hassas bilgileri sağlama konusunda kandırılıp kandırılmayacağını test etmek, belirli tesislere izinsiz giriş yapmayı deneyerek fiziksel güvenlik önlemlerini test etmek, kişinin, bir otorite figürü veya güvenilir bir şahıs gibi davranan biri tarafından kandırılıp kandırılmayacağını değerlendirmek gibi amaçlarla icra edilebilir. Mevcut toplumsal dayanıklılık seviyesini ölçmeye, ulusal güvenlik ve siber savunma yeteneklerini geliştirmeye ve toplumsal dijital dayanıklılığı artırmaya yardımcı olur, bir başlangıç noktası teşkil eder.

85 milyon nüfuslu bir ülkede ulusal çapta bir sosyal mühendislik farkındalık tatbikatı yapmak oldukça karmaşık ve büyük bir girişimdir, ancak mümkündür. ‘Siber Güvenlik Haftası’, ‘Dijital Dayanıklılık Farkındalık Günü’ gibi faaliyetlerle de aynı takvim dâhilinde birlikte yürütülebilir. Böyle bir tatbikatın başarılı olabilmesi için dikkat edilmesi gereken birkaç önemli nokta bulunmaktadır.

● Merkezi bir otorite veya kuruluşun bu tatbikatı planlaması ve yönetmesi gerekmektedir. Bu, devlet kurumları, siber güvenlik ajansları veya büyük güvenlik firmaları tarafından gerçekleştirilebilir.

- Yerel yönetimler, kamu kurumları, özel sektör ve özellikle servis sağlayıcılar ile iş birliği yapılmalıdır. Bu hususun gözetilmesi tatbikatın geniş bir alanda etkili olmasını sağlar.

- Tatbikat öncesinde halkı bilgilendirmek için medya kampanyaları düzenlenebilir. Bu kampanyalar, sosyal mühendislik saldırıları hakkında bilgi verir ve tatbikatın amacını açıklar.

- Okullar, üniversiteler, iş yerleri ve kamu kurumları aracılığıyla eğitim programları düzenlenebilir. Bu programlar, sosyal mühendislik saldırılarına karşı nasıl koruma sağlanacağını öğretir.

- Ortalama simülasyonları ve halkın tatbikat sırasında karşılaştığı şüpheli durumları bildirebileceği bir web portalını kapsayan bir teknik altyapı gereklidir.

4. 11. Ulusal Siber Güvenlik Makamı

Ulusal siber güvenlik otoritesi/makamı, ülkenin siber güvenlik stratejilerini belirleyen, uygulayan, koordine eden ve denetleyen merkezi bir devlet kurumudur. Hâlihazırda, yetki ve sorumluluklarıyla konudan doğrudan ve müstakilen sorumlu bir devlet organının bulunmamasının eksikliği hissedilmektedir. Kurulacak böyle bir otoriteden, ulusal siber güvenliği sağlamak amacıyla politika geliştirme, uygulama, izleme ve denetleme gibi çeşitli görevlerin eş güdüm ve orkestrasyonunu yerine getirmesi beklenmektedir.

Gelişmiş ülkeler, hatta gelişmekte olan ülkeler de incelendiğinde siber güvenlik konularından doğrudan sorumlu, çok aktörlü ve çok paydaşlı faaliyetlerin merkezinde bulunan, koordine, eylemleri izleme, denetim ve kontrol görevlerini yerine getiren bir devlet kurumunun varlığına rastlanmaktadır. Bu tür bir kurumun bulunmadığı durumda sıklıkla, bir görevin birden fazla sorumlusu varken, bazı görevlerin sahipliği konusunda belirsizlikler yaşanabilmekte, yönetişimde aksaklık ve eksikliklere rastlanmaktadır.

Bu kapsamda merkezi bir otoritenin oluşturulmasıyla ulusal düzeyde dijital dayanıklılığın artırılması, geliştirilmesi ve güçlü koruma yolunda mesafe alınacağı ve kamu içerisinde ve kamu-özel sektör arasında daha etkin iş birliği ve koordinasyon sağlanacağı, siber olaylara karşı hızlı ve etkili müdahale kapasitesi edinileceği değerlendirilmektedir.

Bu noktada hatırlatılması gereken ve geçmiş tecrübelerden de görüldüğü üzere organizasyon yapısında değişikliğe gitmek ve yeni kurumlar oluşturmak tek başına yeterli olmamaktadır. Bu girişimi destekler biçimde herkesin katılımını teşvik eden kapsayıcı ve bütüncül politikalar geliştirilmeli, faaliyetler şeffaf ve hesap verebilir bir şekilde yürütülmeli, bahse konu otoritenin kurumsal altyapısının oluşturulması ve kapasitesinin geliştirilmesi temin edilmeli ve en önemlisi strateji ve eylem planlarının sahadaki karşılığı yakından takip edilmeli, değerlendirilmeli ve denetlenmelidir.

5. Genel Değerlendirme

Dijital egemenlik ve dijital dayanıklılık, 2030 yılı ve sonrasındaki on yıllara dair stratejik planlamalar için önemli bir başlık olarak görülmektedir. Bu bağlamda, hızla gelişen ve evrilen teknoloji dünyası, ulusal düzeyde bu iki kavramın sağlam bir şekilde yapılandırılmasını gerektirmektedir. Belirlenen teknolojiler ışığında, dijital dayanıklılık ve dijital egemenliğe dair genel değerlendirmeler aşağıda sunulmuştur.

Öncelikle, 5G ve 6G teknolojileri, iletişim altyapısının temelini oluşturacağından bu altyapıların güvenli hizmet verecek şekilde kurulması ve yaygınlaştırılması, ulusal egemenlik için kritiktir. 5G teknolojisinin sunacağı geniş bant genişliği ve düşük gecikme sürelerine erişilebilmesi IoT cihazlarının yaygınlaşmasını hızlandırırken, 6G'nin sunması beklenen daha yüksek hız ve güvenilirlik, endüstriyel otomasyon ve otonom sistemler için yeni kapılar açacaktır. Bu teknolojilerin güvenli bir şekilde entegre edilmesi, siber tehditlere karşı dayanıklılığın sağlanması ve artırılmasına temel teşkil edecektir.

Kuantum hesaplama ve kriptografi, geleceğin dijital güvenliğinin temel taşları arasında yer almaktadır. Kuantum hesaplama, mevcut kriptografik yöntemleri kırabilecek potansiyel güce sahip olduğu için, kuantum kriptografi ve kuantum anahtar dağıtımı gibi yeni güvenlik protokollerinin geliştirilmesi gerekecektir. Bu alanlardaki yenilikler, ulusal güvenliğin korunmasında kilit rol oynayacaktır.

Kablosuz güç beslemeli IoT cihazları, endüstriyel uygulamalardan sağlık sektörüne kadar geniş bir yelpazede kullanım alanı bulacaktır. Bu cihazların; enerji verimliliği ve güvenliği, dijital ekosistemin sürdürülebilirliği ve güvenirliliği açısından önem taşıdığı gibi yeterince alınmamış güvenlik önlemleri sebebiyle öngörülemez zararlar ve kaotik durumlara sebebiyet verebilecektir.

Beyin-bilgisayar arayüzü (BCI) teknolojileri, insan-makine etkileşiminde devrim yaratacak potansiyele sahiptir. Bu teknolojiler, özellikle sağlık ve savunma sektörlerinde yenilikçi uygulamalara kapı aralayacaktır. Diğer yandan, bilhassa insansı robotların teknolojik gelişimiyle kesiştiği noktada bu tür sistemlerin güvenliği ve etik kullanım kuralları, dijital egemenlik kapsamında ele alınması gereken önemli konu başlıkları arasında yer almalıdır.

Bu bağlamda duyuşal İnternet, veri iletiminde yeni bir boyut kazandırarak, daha zengin ve etkileşimli kullanıcı deneyimleri sunacaktır. Bu teknolojinin entegrasyonu, dijital dayanıklılık stratejilerinin bir parçası olarak değerlendirilmeli ve veri güvenliği önceliklendirilmelidir.

Üretken ve genel yapay zekânın, dijital dönüşüm süreçlerinde kritik roller üstleneceği bugünden açıkça görölmektedir. Bu teknolojilerin doğru ve güvenli bir şekilde kullanımı, verimlilik artışı ve yenilikçi çözümler sunarken, aynı zamanda olası yapay zekâ tehditlerine karşı koruma sağlamalıdır. Siber güvenlik alanında yapay zekâ defansif alanda olduğu kadar ofansif alanda da yer bulacaktır. Defansif alanda özellikle veri odaklı işleme gerektiren, bunu insan sayesinde yapan fonksiyonların yapay zekâ ile yapılır hâle gelmesi kaçınılmazdır. Örneğin Siber Olay Yönetimi fonksiyonlarındaki insan gücünde yüzeysel analizden ziyade ileri analizler için gereksinim olacak şekilde bir dönüşüm olacaktır. Bununla beraber daha önce davranışsal analiz olarak tanımlanan yöntemlerin de çok daha yüksek başarımlara ulaşacağını söylemek mümkündür. Ofansif tehdit araçlarının dönüşümü de bu süreçte gerçekleşecektir. İnsana daha az ihtiyaç olacak şekilde insansız siber tehdit araçları keşif aşamasından itibaren siber saldırı süreçlerini dönüştürecek ve dijital dayanıklılığa risk oluşturacaktır.

Küçük modüler reaktörler (SMR) ve yeni nesil batarya teknolojileri, enerji güvenliği, sürdürülebilirlik ve dijital dayanıklılık açısından kritik imkânlar sunabilecektir. Bu teknolojilerin geliştirilmesi ve yaygınlaştırılmasının, baz istasyonları ve diğer dijital yayım ve aktarım altyapısının daha kesintisiz ve güvenilir bir şekilde çalışmasını destekleyeceği beklenebilir.

Blok zincir teknolojileri, veri güvenliği ve şeffaflık konularında sunduğu avantajların yanı sıra, dağıtık, ademi merkezi ve anonim yapısıyla ulusal dijital egemenlik stratejilerinde zorlaştırıcı anlamda önemli bir rol oynayacaktır. Blok zincir tabanlı çözümlerin, özellikle finansal hizmetler ve tedarik zinciri yönetiminde yeni standartlar belirlemesi beklenebilir.

Terabayt İnternet ve çoklu bulut teknolojileri, veri yönetimi ve depolama çözümlerinde yeni bir çağ açacak, bu yeni çağda uzay ve alt uzay iletişim, uzay veri merkezleri, kuantum algılayıcılar, kuantum görüntüleme ve kuantum iletişim gibi ileri teknoloji uygulamaları, öngörülmesi güç birtakım dijital imkânlar ve yeni açmazlar sunabilecektir. Bu teknolojilerin

entegrasyonu, ulusal güvenlik ve ekonomik kalkınma için yeni fırsatlar yaratacağı gibi, geride kalma durumunda dijital dünyada varlığınız tehlikeye girebilecektir.

Türkiye’deki duruma genel olarak bakıldığında ise çalışılması gerekli, özetle üç ana faaliyet alanı bulunduğu görülecektir. Bu kapsamdaki temel gerekler;

- Ülke siber güvenlik organizasyon yapısının gözden geçirilerek güçlendirilmesi ve yeni bir bakış açısıyla siber güvenlik teşkilatlanma, uygun yönetim sistemleri ve modellerinin geliştirilmesi,
- Yetkin insan kaynağının oluşturulması, kapasite ve yeteneklerin geliştirilmesi, elde tutulması ve en önemlisi sürekli geliştirilmesi için yapıların kurgulanması,
- Siber alanda yüksek teknoloji, birikim, araç ve gereçler, uygulamalar için kendi yerli siber güvenlik teknolojilerinin geliştirilerek elde tutulması,

olarak sıralanabilir.

Yukarıda ifade edilen bu hedeflerin, yüzlerce alt kırılımı ve çalışma alanı olduğu açıktır. Bu alanların bir kısmında hâlihazırda yürütülen çalışmalar olduğu gibi belirli bir takvim dâhilinde başlatılması gerekenler de bulunmaktadır. Bunlara bir de her gün yenileri eklenen gelişmiş saldırılar ve tehditler olduğu gibi geliştirilen yeni teknolojilerin getirdiği riskler dâhil edildiğinde ortaya çıkan manzara, bitiş çizgisi olmayan ve tempolu bir şekilde koşulması gereken bir maratona benzetilebilir.

Sonuç olarak, 2030 yılı ve sonrasında dijital dayanıklılık ve egemenlik, ancak gelişen teknolojilerin güvenli ve sürdürülebilir bir şekilde entegre edilmesiyle mümkün olacak, ulusal düzeyde bu teknolojilerin doğru yönetimi ve kullanımı, stratejik hedeflere ulaşmada önemli bir rol oynayacaktır.

Belirlenen hedeflere ulaşmak için inat ve sebatla çalışılması ve istikrarla alınması gereken uzun bir yol bulunmaktadır. Bu yolda atılması gereken adımların belirlenmesi görece kolay bir aşamayken, bu hedeflerin somut gerekçelere dayandırılan önem derecelerinin tayin edilerek

önceliklendirilmesi, detaylandırılması, safhalandırılması, eylem planlarına dönüştürülmesi, eylemlerin sahiplendirilmesi ve dahası gerekli çalışmaların yapılması daha meşakkatli diğer aşamaları oluşturmaktadır.

Özellikle de Dijital Egemenlik ve Dayanıklılık gibi önemli ve kapsamlı bir konuda belirlenen hedeflere ulaşabilmek için sihirli bir değnek, büyülü bir çözüm veya kestirme bir yol olmadığı tespiti bir kez daha bu vesileyle vurgulansa da bunun yolu her zaman yetenek ve kapasite geliştirmek ve bunları da güncel tutmaktır.

EKLER

Ek -1 : Önem ve Önceliklendirme Anketi

Ek -2 : Değerlendirme Formu (Örnek)

Ek -3: Çözüm Öneri Formu (Örnek)

Ek -4: Tespit, Teklif ve Öneriler

KAYNAKÇA

Yazar Adı	Yayının Adı, Yayımcı, Yayın Tarihi, Yeri
Gençkaya Ö.F.	TÜBİTAK, Bilgi ve Toplum Başkanlığı, Popüler Bilim Yayınları, (T.Y.)
Çakır H. et al.	Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi, Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi (JEBPIR), 2021, Şf.353-379
-	Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2013-2014), UDH Bakanlığı, 2013
-	Ulusal Siber Güvenlik Stratejisi (2016-2019), UDH Bakanlığı, 2015
-	5902 Sayılı Afet ve Acil Durum Yönetimi Başkanlığının Teşkilat ve Görevleri Hakkında Kanun, 17/06/2009
AFAD	“2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi”, AFAD, 2014
Piret Pernik et al.	National Cyber Security Organisation: United States, CCD CoE, 2016
Mikk Raud	China and Cyber: Attitudes, Strategies, Organisation, NATO CCD CoE, 2016
Sebastian Cymutta	National Cybersecurity Organisation: Germany, NATO CCD CoE, 2020
Anna-Maria Osula	National Cybersecurity Organisation: United Kingdom, NATO CCD CoE, 2015
UK GOV	UK National Cyber Strategy 2022
Ogawa H. et al.	Cybersecurity Governance in Japan, Int. Journal of Cyber Diplomacy, 2021
Evan A. Feigenbaum	The Korean Way With Data, Carneige Endowment for International Peace, Ağustos 2021
Sungbaek Cho	National Cybersecurity Organisation: Republic of Korea, NATO CCD CoE, 2022,
Ünver G.N.	Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye ve İngiltere Örneği, Livre de Lyon, 2023
Janne Hakal et al.	Russia's Strategy In Cyberspace, NATO SC CoE, 2021
Deborah H.-Couriel	National Cybersecurity Organisation: Israel, NATO CCD CoE, 2017
ENISA	ENISA Threat Landscape 2023 July 2022 to June 2023, ENISA, Ekim 2023
TÜBİTAK	TÜBİTAK 2024-2025 Ar-Ge ve Yenilik Konu Başlıkları, TÜBİTAK, Versiyon: 22.01.2024
AB Komisyonu	EU Commision, Action Plan Against Disinformation, 2018
BTK	Türkiye’de Dijital Dönüşüm ve Dijital Okuryazarlık, BTK, Aralık 2022
OECD	Digital Government Review of Türkiye, OECD, 2023
OECD	21 st Century Readers-Developing Literacy Skills In A Digital World, OECD, 2021
Cem Okyay	Bir Deniz Kuvveti Stratejisinin Temelleri, 03 Haziran 2023, LinkedIn
Atilla Aydın	Dijital Çağda Egemenlik: Şapkayı Önümüze Koyma Vakti Geldi, 19 Mayıs 2018, Medium
Uslu S., Babaoğlu C., Beyribey Y.E.	Dijitalin Yüzyılı, 2023, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi
WEF	Global Innovation Index 2023
MIT	MIT Cyber Defense Index 2022/23

Yazar Adı	Yayının Adı, Yayımcı, Yayın Tarihi, Yeri
USGov	Başkanlık Kritik Altyapı Koruma Komisyonu Raporu (PCCIP), 1997.
USGov	Critical Infrastructure Protection (PDD-63), 1998.
AB	European Programme for Critical Infrastructure Protection (EPCIP), 2004.
AB Komisyonu	The Council of The European Union, 2018
AB	Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, 2009.
ISO	ISO 22301 Standardı Komitesi, (2012). ISO 22301 Toplumsal Güvenlik-İş Sürekliliği Yönetim Sistemi
DDO	On İkinci Kalkınma Planı (2024-2028), 2023.
TDK	Türk Dil Kurumu Sözlüğü, 2022.
Canbek, G., Sağıroğlu, Ş.	Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. Politeknik Dergisi, 9(3), 165-174. (2006).
Tsai, C. W., Lai, C. F., Chao, H. C., & Vasilakos, A. V.	Big Data Analytics: A Survey. Journal of Big Data, 2, 1-32. (2015).
Rao, T. R., Mitra, P., Bhatt, R., & Goswami, A.	The big data system, components, tools, and technologies: a survey. Knowledge and Information Systems, 60, 1165-1245. (2019).
Aktan, E.	Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu. Bilgi Yönetimi, 1(1), 1-22. (2018).
Russom P.	Big Data Analytics. TDWI Best Practices Report, Fourth Quarter, 19(4), 1-34. (2011).
Laney D.	3D data management: controlling data volume, velocity and variety. META Group Research Note 6(70)(2013)
DDO	Veri Merkezleri Raporu
T.C. Str. B.B.lığı	On Birinci Kalkınma Planı (2019-2023). B. (2019).
BTYPK	T.C. Cumhurbaşkanlığı Bilim, Teknoloji ve Yenilik Politikaları Kurulu Siber Güvenlik Teknoloji Yol Haritası, Ekim 2021

İnternet Örün Sayfası (Web) Kaynakları

Bağlantı Yolu	Erişim Zamanı
https://sozluk.gov.tr	23.03.2024
https://ansiklopedi.tubitak.gov.tr/ansiklopedi/yonetisim	26.03.2024
https://genclik.argudenacademy.org/yonetisim-nedir/	26.03.2024
https://medium.com/cyber-alliance/turkiyenin-siber-guvenlik-tarihi 11/09/2023	29.03.2024
https://www.yok.gov.tr/Sayfalar/Haberler/2023/siber-saldirilara-karsi-uzman-yetistirmek-icin-4-yeni-myo-aciliyor.aspx , 16/05/2023	30.03.2024
https://medium.com/cyber-alliance/turkiyede-siber-guvenlik-ve-bilgi-guvenligi-egitimi 02/09/2023	30.03.2024
https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance	01.04.2024
https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance , CISA	01.04.2024
https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cybersicherheitspolitik/cybersicherheitspolitik-node.html#doc18751090bodyText2	02.04.2024
https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum	02.04.2024
https://cyber.gouv.fr/en/french-approach-cyber-0	02.04.2024
https://www.ncsc.gov.uk/collection/risk-management/cyber-security-governance	02.04.2024
https://www.nknews.org/2024/02/south-korea-unveils-new-cyber-strategy-to-counter-north-korean-threats/	03.04.2024
https://ccdcoe.org/library/strategy-and-governance/?search=russia	04.04.2024
https://www.cert.ru/en/about.shtml	04.04.2024
https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics	04.04.2024
https://securitydelta.nl/partners/overview-partners/cyberspark	04.04.2024
https://ir.darktrace.com/pressreleases/2023/4/3/	05.04.2024
https://www.eccu.edu/blog/technology/the-latest-cybersecurity-technologies-and-trends/	04.04.2024
https://www.metacompliance.com/blog/cyber-security-awareness/emerging-technologies-and-their-impact	06.04.2024
https://www.cyberdegrees.org/resources/hot-technologies-cyber-security/	06.04.2024
https://www.linkedin.com/pulse/emerging-cybersecurity-threats-breakthrough-overview-2024-leschik-om47f/	06.04.2024
https://www.usom.gov.tr/hakkimizda	06.04.2024
https://www.usom.gov.tr/arge	06.04.2024
https://tubitak.gov.tr/tr/kurumsal/icerik-politikalar	06.04.2024
https://euvsdisinfo.eu/about/	06.04.2024
https://www.invid-project.eu/	06.04.2024
https://x.com/halilozturkci/status/1762786304431968661	07.04.2024
https://inclusion.ca/research-and-ideas/citizen-resilience-project-2/	07.04.2024
https://www.electronicshub.org/the-average-screen-time-and-usage-by-country/	07.04.2024

Bağlantı Yolu	Erişim Zamanı
https://turkiyevodafonevakfi.org.tr/haberler/global-vodafone-vakfi-ndan-dijital-yetenek-egitimi-arastirmasi	07.04.2024
http://fatihprojesi.meb.gov.tr/	07.04.2024
https://www.siberyildiz.com/	07.04.2024
https://www.fetih.gov.tr/	07.04.2024
https://www.btkakademi.gov.tr/portal/public/hakkimizda	07.04.2024
https://www.siberay.com/hakkimizda	07.04.2024
https://www.dmm.gov.tr/	07.04.2024
https://www.sibervatan.org/kalkinma-ajanslari-sibervatan-programi	07.04.2024
https://siberakademi.bilgem.tubitak.gov.tr/mod/page/view.php?id=10	07.04.2024
https://cybersec.bogazici.edu.tr/tr/hakkimizda	07.04.2024
https://turkiyevodafonevakfi.org.tr/vodafone-vakfinin-7-avrupa-ulkisini-kapsayan-dijital-egitim-girisimine-turkiye-de-katildi/	07.04.2024
https://habitatdernegi.org/dijital-donusum/gelecegin-ekrani/	07.04.2024
https://habitatdernegi.org/kapsayici-ve-surdurulebilir-buyume/dijitalde-hayat-kolay/	07.04.2024
https://www.linkedin.com/pulse/bir-deniz-kuvveti-stratejisinin-temelleri-cem-okyay/?trackingId=up%2FXRw7fQqS47Hrg1g76xQ%3D%3D	07.04.2024
https://medium.com/@sibervatandas/dijital-%C3%A7a%C4%9Fda-egemenlik-%C5%9Fapkey%C4%B1-%C3%B6n%C3%BCm%C3%BCze-koyma-vakti-geldi-1841b815dbfb	07.04.2024
https://cbddo.gov.tr/dijital-tr	07.04.2024
https://dijitalturkiyeplatformu.org/	07.04.2024
https://www.sbb.gov.tr/wp-content/uploads/2022/07/On_Birinci_Kalkinma_Planı-2019-2023.pdf	14.04.2024
https://csrc.nist.gov/projects/post-quantum-cryptography , NIST	27.07.2024
https://gdpr-info.eu/ , General Data Protection Regulation, GDPR	27.07.2024
https://www.itu.int , International Telecommunication Union. (2021). Global Cybersecurity Index	27.07.2024
https://www.un.org , United Nations. (2021). General Assembly Resolutions on Cybersecurity	27.07.2024
https://ec.europa.eu , European Commission. (2021). Digital Markets Act (DMA)	27.07.2024
https://ec.europa.eu , European Commission. (2021). Digital Services Act (DSA)	27.07.2024
https://dodcio.defense.gov/Cyber-Workforce/CWS/	07.09.2024
https://1milyonistihdam.hmb.gov.tr/proje-hakkinda	07.09.2024
https://www.gartner.com/en/information-technology/glossary/cybersecurity-mesh	07.09.2024
https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf	08.09.2024
https://cms-lawnow.com/en/ealerts/2018/11/bulgaria-adopts-new-cyber-security-act	08.09.2024
https://www.cyberwiser.eu/bulgaria-bg	08.09.2024
https://www.coe.int/en/web/cybercrime/parties-observers	08.09.2024

Bağlantı Yolu	Erişim Zamanı
https://www.coe.int/en/web/octopus/-/bulgaria	08.09.2024
https://e-gov.bg/wps/portal/agency-en/about-us	08.09.2024
https://www.govcert.bg/en/	08.09.2024
www.gdbop.bg	08.09.2024
www.cybercrime.bg	08.09.2024
https://www.crc.bg/index.php/bg/rubriki/742/istoriq-na-krs	08.09.2024
www.cdpd.bg/en	08.09.2024
https://www.forbes.com/sites/timbajarin/2022/05/30/the-great-technology-wall-of-china/	08.09.2024