T.C.
GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

AVRUPA BİRLİĞİ ÜLKELERİ İLE TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİLERİ VE EYLEM PLANLARININ İNCELENMESİ

SÜNDÜS ARINMIŞ UZUN

ADLİ BİLİŞİM ANA BİLİM DALI

ŞUBAT 2022


GAZİ ÜNİVERSİTESİ
Gazi
1926

AVRUPA BİRLİĞİ ÜLKELERİ İLE TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİLERİ VE EYLEM PLANLARININ İNCELENMESİ

Sündüs ARINMIŞ UZUN

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

ŞUBAT 2022

Sündüs ARINMIŞ UZUN tarafından hazırlanan "AVRUPA BİRLİĞİ ÜLKELERİ İLE TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİLERİ VE EYLEM PLANLARININ İNCELENMESİ" adlı tez çalışması aşağıdaki jüri tarafından OY ÇOKLUĞU ile Gazi Üniversitesi ADLİ BİLİŞİM ANA BİLİM DALI Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Hüseyin ÇAKIR
Bilgisayar ve Öğretim Teknolojisi Eğitimi, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Başkan: Prof. Dr. Şeref SAĞIROĞLU
Bilgisayar Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylamıyorum.

……...

Üye: Prof. Dr. Olgun DEĞİRMENCİ
Hukuk, TOBB -Ekonomi ve Teknoloji Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

……...

Tez Savunma Tarihi: 10/02/2022

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..…….

Prof. Dr. Aslıhan TÜFEKCİ
Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Sündüs ARINMIŞ UZUN
10/02/2022

AVRUPA BİRLİĞİ ÜLKELERİ İLE TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİLERİ VE EYLEM PLANLARININ İNCELENMESİ

(Yüksek Lisans Tezi)

Sündüs ARINMIŞ UZUN
GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

ŞUBAT 2022

ÖZET

Bu çalışma, tehlike, korku veya risklere karşı kişinin kendini özgür hissetme olarak tanımlanan güvenlik kavramı içinde değerlendirilen siber güvenlik olgusunun incelenmesine odaklanmıştır. Kişi veya kurumların bilgileri, iletişim verileri ile varlıklarının korunmasının amaçlandığı siber güvenliğin geliştirilmesi, yaygınlaştırılması ve toplumsal farkındalığın yükseltilmesi için ülkeler eylem planları hazırlamaktadır. Eylem planlarının kapsamı, hayata geçirilmesi ve sonuçlarının analiz edilmesi ülkelerin siber güvenlik düzeylerinin yükseltilmesini sağlamaktadır. Söz konusu olgulara dayanılarak çalışmanın amacı, incelenen ülkelerin eylem planlarının analiz edilerek elde edilen sonuçlarla Türkiye'nin siber güvenlik eylem planına yönelik önerilen geliştirmektir. Çalışmanın amacına ulaşılması için Türkiye'nin, Avrupa Birliği'ne üye ülkelerin ve İngiltere'nin siber güvenlik eylem planlarının incelenmiş, belirlenen on bir kriter kapsamında tüm eylem planları kıyaslanmış ve elde edilen bulgular kullanılarak Türkiye'nin gelecek eylem planının geliştirilmesi için konu başlıkları ile içerikler oluşturulmuştur. Bu amaca ulaşılması nitel araştırma modellerinden olan doküman inceleme yönteminden yararlanılmış olup literatür taraması yapılmış, eylem planları analiz edilmiş ve mevzuat değerlendirilmiştir. Çalışma kapsamında, öncelikle güvenlik, ulusal güvenlik ve siber güvenlik kavramları incelenmiştir. Daha sonra Türkiye'nin siber güvenliğin koordinasyonu ve planlaması kapsamında yaptığı çalışmalar ile 2013-2014, 2016-2019 ve 2020-2023 dönemlerini kapsayan eylem planları detaylı olarak ele alınmıştır. Avrupa Birliği'ne üye ülkeler ile İngiltere'nin siber güvenlik alanındaki çalışmaları ve eylem planları derinlemesine analiz edilerek on bir başlıkta Türkiye'nin ve örnek alınan diğer ülkelerin stratejileri ve eylem planları kıyaslanmıştır. Bu kıyaslama sonunda Türkiye'nin pek çok kritere uyum sağladığı ancak özellikle eylem planlarının sürekliliği, insan kaynağının geliştirilmesi ve siber caydırıcılık konularında eksikliklerin olduğu tespit edilmiştir. Son olarak kıyaslama sonucunda elde edilen veriler kullanılarak Türkiye için hazırlanacak yeni eylem planına öneriler hazırlanmıştır.

Bilim Kodu	:	92401
Anahtar Kelimeler	:	Güvenlik, siber güvenlik, siber güvenlik eylem planı, Avrupa Birliği'nin siber güvenlik stratejisi.
Sayfa Adedi	:	277
Danışman	:	Doç. Dr. Hüseyin ÇAKIR

EXAMINATION OF CYBER SECURITY STRATEGIES AND ACTION PLANS OF EUROPEAN UNION COUNTRIES AND TURKEY

(M. Sc. Thesis)

Sündüs ARINMIŞ UZUN
GAZİ UNIVERSITY
INFORMATICS INSTITUTE

February 2022

ABSTRACT

This thesis is focused on analysing the cyber security phenomenon which is depicted and concerned in terms of security concept that people describe this concept as feeling freedom against threats, fear and risks. In order to improve and spread cyber security awareness by protecting individuals' and institutions' communication information, countries are preparing course of actions. In order to analyse the consequences and make the extent of action plans to be realized, it is done through the improving the rate of cyber security levels in countries. The aim of this paper is to improve Turkey's cyber security action plan with the help of analysing different countries' course of actions .To reach its goal, action plans of Turkey, European Union countries and United Kingdom are investigated by comparing their action plans depending on the pre-defined eleven criteria. The results are used to enhance Turkey's future action plan that constitutes the headings and contents of this paper. In favour of achieving the aim, one of the qualitative methods which is document review is conducted. Literature review, inspection of action plans is also utilized and regulations are evaluated. In the scope of work, firstly, security, national security and cyber security notions are examined. Then, Turkey's actions regarding to the cyber security coordination and planning are addressed. Moreover, the action plans including 2013-2014, 2016-2019 and 2020-2023 periods are evaluated in detail. The action plans of countries in European Union and United Kingdom's are addressed profoundly, Turkey's and the other countries strategies and action plans are compared using the eleven criteria. As a result of this comparison, it can be said that Turkey complies with most of the criteria. Yet, the continuity of actions plans, improving human sources and cyber deterrence are considered as the factors that Turkey is insufficient. Lastly, the results of the comparisons are used in place of providing suggestions for new action plan.

Science Code	:	92401
Key Words	:	Security, cyber security, cyber security action plan, cyber security strategies of the European Union.
Page Number	:	277
Supervisor	:	Assoc. Prof. Hüseyin ÇAKIR

TEŞEKKÜR

Uzun ve zorlu bir sürecin meyvesi olan tezimin yazılma sürecinde ve tamamlanmasında bana desteğini hiçbir zaman esirgemeyen ve her türlü desteği tam zamanında veren eşim Hakan UZUN'a, kendisine ayıracağım en değerli vakitlerden çalarak hazırladığım çalışmamdaki küçük destekçim biricik oğluma teşekkürlerimi bir borç bilirim. Sadece başarımda değil başarısızlıklarımda da yanımda olan ve bana inanmaktan hiç vazgeçmeyen kıymetli anne ve babama şükranlarımı sunarım. Çalışmamı gerek konusunun belirlenmesinde gerekse yazım sürecinde fikirleriyle güçlendiren ve desteklerini hiçbir zaman esirgemeyen hocam Doç. Dr. Hüseyin ÇAKIR'a ve desteklerinden dolayı çalışma arkadaşım Simge KOÇTAŞ'a sonsuz teşekkürlerimi sunarım. Bu destekler sayesinde çalışmam akademik ve bilimsel değerlere bağlı bir şekilde sonuçlanabilmiştir.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

ABD	Amerika Birleşik Devletleri
ACD	Active cyber defense/ Aktif siber savunma mekanizması
AET	Avrupa Ekonomik İşbirliği Örgütü
AGİT	Türkiye ve Avrupa Güvenlik ve İşbirliği Teşkilatı
AI	Artificial intelligence/ Yapay zeka
AKÇT	Avrupa Kömür ve Çelik Topluluğu
APT	Advanced persistent threat/ Gelişmiş sürekli tehdit
AR	Augmented reality/ Artırılmış gerçeklik
Ar-Ge	Araştırma ve geliştirme
BİT	Bilgi İletişim Teknolojileri
BM	Birleşmiş Milletler
BSI	Enformasyon Üyeliğinden Sorumlu Federal Ofis/ Bundesamt für Sicherheit in der Informationstechnik
BT	Bilgi teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı
CDPC	Avrupa Suç Sorunları Komitesi
CERT	Computer emergency response team/ Siber olaylara müdahale ekibi
CIA	Merkezî İstihbarat Teşkilatı/ Central Intelligence Agency
CII	Critical information infrastructure/ Kritik bilgi altyapısı
CIIP	Critical information infrastructure protection/ Kritik bilgi altyapısı koruma
CISO	Chief information security officer/ Baş bilgi güvenliği görevlisi
ECJRC	Avrupa Komisyonu Ortak Araştırma Merkezi
ENISA	Avrupa Ağ ve Bilgi Güvenliği Ajansı
EURATOM	Avrupa Atom Enerjisi Topluluğu
Fintech	Finansal teknoloji
Iot	Internet of things/ Nesnelerin interneti
IPv6	Internet protokolü sürüm 6
IRGC	İslam Devrim Muhafızları Birlikleri
KHK	Kanun Hükmünde Kararname

Kısaltmalar	Açıklamalar
NATO	Kuzey Atlantik Antlaşması Örgütü
NCIIPC	National Critical Information Infrastructure/ Ulusal Kritik Bilgi Altyapısı Koruma Merkezi
NCSC	National cyber security centre/ Ulusal siber güvenlik merkezi
NPDO	National Pre-Departure Orientation/ Pasif Savunma Teşkilatı
OECD	Organisation for Economic Co-operation and Development/ Ekonomik Kalkınma ve İşbirliği Örgütü
PKI	Public key infrastructure/ Kamu anahtar altyapısı
SOME	Siber olaylara müdahale ekipleri
STK	Sivil toplum kuruluşu
TBMM	Türkiye Büyük Millet Meclisi
USOM	Ulusal Siber Olaylara Müdahale Merkezi
VR	Virtual realty/Sanal gerçeklik

1. GİRİŞ

Günümüz dünyasında bilgi kaynaklarının güvenliği ve korunması hiç olmadığı kadar önem kazanmıştır. Globalleşen ve dijitalleşen dünyada sürekli olan yeni tehditlerin ortaya çıkması kendisini en çok siber alanda göstermektedir. Kişisel verilerden altyapılara kadar çeşitlenen dijital hizmetler zararlı yazılımların, kötü amaçlı korsanların veya organize devlet birimlerinin hedefi haline gelmiştir. Sağlık verileri, eğitim verileri, altyapı tesisleri vb. pek çok faktör ülkeler tarafından sürekli olarak korunmak ve sağlam sistemler içinde kullanılmak zorundadır.

Siber dünya içinde saldırılar, terörizm, casusluk, suç işleme veya zorbalık gibi durumlar sürekli artmakta devletleri, kişileri ve kurumları devamlı olarak teyakkuz halinde bırakmaktadır. Nesnelerin interneti, endüstri 4.0 vb. kavramlar ile bağlantılı dünyanın sınırları giderek belirsizleşmekte ve yeni mücadele alanları ortaya çıkmaktadır. Siber güvenlik bir aktörün zafiyeti ile çökebilmekte veya bir aktöre yapılan saldırı diğer aktörleri savunmasız bırakabilmektedir.

Ülkelerin sosyal, siyasal, ekonomik ve kültürel yapılarının güvenliği 21. yüzyılda boyut değiştirerek sanal bir yapıya bürünmüştür. İletişim ağlarının güvenli olması sadece gizlilik açısından değil aynı zamanda hayatın akışı, ekonomik hayatın sürekliliği ve siyasal sistemlerin işlerliği için de son derece önemlidir. Doğal afet zamanında iletişim hatlarının yoğunluktan çökmesi gibi olaylar toplumsal karmaşa ve siyasal buhranlara neden olabilmektedir. Bu açıdan hem güvenlik hem süreklilik siber güvenliğin doğrudan bir yansımasıdır.

Hayatın her alanında kullanılan bilgisayar teknolojileri insan işlerini kolaylaştırmakta, otomatikleştirmekte ve en önemlisi sürdürülebilir bir yapıya sokmaktadır. Kullanılan her türlü uygulamaların güvenilir olması, stabil çalışması ve her an ulaşılabilir olması siber güvenliğin bir yansımasıdır. Özellikle Türkiye'deki gibi e-devlet uygulamalarının güvenliği ve ulaşılabilirliği daha fazla önem kazanmıştır. Vatandaşların hassas verilerinin tutulduğu büyük sistemlerden çalışanların kişisel verilerinin depolandığı tüm yapılara kadar siber güvenliğin önemi her geçen gün artmaktadır.

Bilgilerin güvenilir olması özellikle son on yılda önemini artıran bir alana dönüşmüştür. Sosyal medya tarafından yayılan yanlış veya manipülatif bilgiler toplumsal huzursuzluklara neden olabilmekte, siyasal sistemlere zarar verebilmekte ve toplulukları yönlendirebilmektedir. Bu açıdan önlem alınması, yanlış bilgilerin yayılmasının engellenmesi ve toplumsal düzenin korunması hususu da siber güvenliğin bir yansıması olarak son yıllarda öne çıkmaktadır.

Siber güvenlik alanı dağınık ve çok farklı alanları kapsayan bir yapıdadır. Bu açıdan karmaşıktır ve yönetilmesi oldukça zordur. Tek bir kişinin veya uzmanın eline bırakılmayacak kadar önemli olan bu alanın bir merkezi olmalı, merkeze bağlı alt birimleri oluşturulmalı ve her bir birimin yetki, görev ve sorumluluklarının tespit edilmesi gerekmektedir. Ülkemizde daha çok bilgi işlem birimlerine teslim edilen bu alanın yeni yeni önem kazanarak bağımsız birimlere büründüğü görülmektedir. Buna rağmen gelişmenin hızlanması ve sistematik yapıların güçlü bir şekilde kurulması beklenmektedir.

Yaşanan birçok olayda görüldüğü üzere bir sistem ne kadar güvenilir tasarlanırsa tasarlansın saldırıya uğrama veya zarar görme olasılığı her zaman için vardır. Böyle durumlarda önemli olan saldırı sonrası toparlanmanın hızlı olması, bilgilerin güvenilir bir şekilde kurtarılması ve çalışmaların aksamadan sürekliliğinin korunmasıdır.

Siber güvenlik temelinde son kullanıcıya bağımlıdır. Son kullanıcının en ufak bir hatası sağlam yapılandırılmış bir sistemi kolaylıkla zafiyete uğratabilir veya ne kadar otomatik olursa olsun bir sistemin insan faktörüne karşı son derece hassas ve savunmasız olduğu ifade edilmektedir. Bu açıdan son kullanıcıların siber saldırılara karşı eğitimli olması, siber saldırı türlerini bilmesi, olası risk faktörleri hakkında hassas olması büyük önem kazanmıştır. Çalışmada detaylı olarak inceleneceği üzere her bir ülkenin stratejisi ve eylem planında son kullanıcının eğitilmesine özel önem verilmiş ve birçok faaliyet oluşturulmuştur. Özellikle devlet organlarında son kullanıcı eğitimlerine özel önem verilmeye başlanıldığı söylenebilir.

Yukarıda açıklanan tehdit ve olumsuzluklarla mücadele etmek için tüm aktörlerin işbirliğine ihtiyaç duyulmaktadır. Bu işbirliği aktörlerin kendilerini geliştirmelerine ve güncel gelişmeleri takip etmeleriyle sıkı sıkıya ilişkilidir. Kamu kurumları, özel sektör, üniversiteler, bireyler ve sivil toplum kuruluşları ile birlikte tüm aktörleri içine alan ortak stratejilere ulaşmak amacıyla hazırlanan eylem planları gerek hazırlık gerek korunma

gerekse mücadele için son derece önem kazanmıştır. Bunun için ülkeler stratejiler belirlemekte, eylem planları oluşturmakta, uzman ekipler kurmakta, hedefler belirlemekte ve hedeflerin takibini yapmaktadır. Küreselleşme ile birlikte ülkelerin birbirlerine yakınlaşması sistemin dışında kalamama ve sisteme uyum sağlama ile sonuçlanmıştır. Ülkemizde dünyadaki gelişmeleri takip ederek Siber Güvenlik Kurulu oluşturmuş ve 2013-2014, 2016-2019 ve 2020-2023 dönemlerini kapsayan oldukça detaylı stratejiler oluşturulmuş ve bu stratejilere nasıl ulaşılacağının açıklandığı eylem planları hazırlamıştır. 2020-2023 dönemini kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020 yılı sonunda açıklanmış olup siber güvenlik stratejisi kamuoyuna açıklanmasına rağmen eylem planı gizli tutulmuştur. Ancak eylem planı stratejilere ulaşmak için atılması gereken adımları açıkladığı ve doğrudan stratejilere bağlı olduğu için ülkenin genel siber güvenlik politikasını temsil ettiği değerlendirilmiştir.

Siber Güvenlik Kurulu'nun görev ve yetkilerinin belirlenmesi son derece isabetli olmuş, ancak 703 sayılı KHK ile yapısının yeni sisteme geçişi sağlanmamıştır. Bu durum büyük bir yetki karmaşasına neden olmuş ve bir nevi stratejinin ve eylem planlarının sahipsiz kalmasına neden olmuştur. Daha sonra yapılan düzenlemeler ise konuyu tam olarak çözmemiş ve çok başlılık devam etmiştir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'ne bağlı olarak kurulan Siber Güvenlik Dairesi Başkanlığı ile doğrudan Dijital Dönüşüm Ofisi siber güvenlik alanındaki politika belirleme, bilgi güvenliğini sağlama, denetim yapısını kurma ve genel olarak alanın gelişmesine katkı sağlamaktadır.

Problem durumu

Siber güvenlik kavramı güvenlik kavramın tamamlayıcı bir öğesidir. Bir ülkenin güvenliğinin sağlanması için bilgi ve iletişim teknolojilerinin, kritik altyapıların, yedekleme sistemlerinin vb. siber güvenlik değişkenlerinin de güvenliğinin garanti edilmesiyle mümkündür. Bu garantinin verilebilmesi için ülkeler belirli bir dönemi kapsayan planlar hazırlar ve yatırım yaparak hedeflerini gerçekleştirmek için faaliyet yürütür. Çalışmanın problemi, oluşturulması hedeflenen siber güvenlik stratejilerinin ve eylem planlarının nasıl olması gerektiği, başarı için atılması gereken adımlar ve maliyetlendirme gibi unsurların ne olması gerektiğinin ortaya koyulması durumudur. Problemin dayanağı ülkelerin sürekli olarak siber saldırılara uğraması, siber saldırılar sonrası kurumların zarar görmesi ve söz konusu tehdidin giderek büyümesidir (Hürriyet, 2021a; Sabah, 2021, Hürriyet, 2021b;

Threatmap, 2021). Daha önce siber güvenlik strateji ve eylem planlarının incelenmesi konusunda araştırmalar yapılmasına rağmen kıyaslama veya strateji ve eylem planlarında hangi unsurların yer alması gerektiği hususuna yeteri kadar ağırlık verilmemiştir. Bu çalışma ile İngiltere ve AB ülkelerinin eylem planları ve stratejilerinin tamamı incelenecek, hangi hedeflerin yer aldığı analiz edilecek ve güçlü bir siber güvenlik eylem planının nasıl olması gerektiği tartışılacaktır.

Araştırmanın amacı

Araştırmanın amacı, problem durumunda tanımlanan unsurların açıklamasının yapılması, Türkiye'nin, siber güvenlik stratejisi ve eylem planlarının değerlendirilmesi, AB ülkeleri ve İngiltere'nin siber güvenlik stratejisi ve eylem planlarının detaylı bir şekilde analiz edilmesi, ülkelerin siber güvenlik stratejilerinin ve eylem planlarının uzman görüşlerine dayanılarak belirlenen on bir ortak kriterlere göre kıyaslanması ve Türkiye'nin gelecek siber güvenlik eylem planına yönelik uygulanabilir öneriler geliştirilmesidir. Türkiye için öneriler geliştirilmesi çalışmanın özel amacı olup bu amacı ulaşmak için incelenen stratejilerin ve eylem planlarının kıyaslanması sonucunda elde edilen bulgulardan yararlanılmıştır. Çalışmanın alt amaçları aşağıdaki gibi belirlenmiştir:

- Türkiye ile incelenen ülkelerin stratejileri ve eylem planları sürekli midir?
- Türkiye ile incelenen ülkeler kritik altyapı güvenliği için yatırım yapıyor mu?
- Türkiye ile incelenen ülkelerde siber güvenlik alanında Ar-Ge çalışmaları yürütülüyor mu?
- Türkiye ile incelenen ülkelerde altyapının gelişen teknolojiye adapte ediliyor mu?
- Türkiye ile incelenen ülkelerde gelişen teknolojide liderlik yapma hedefi var mı?
- Türkiye ile incelenen ülkeler siber uzayda güçlü ittifak kurma amacına sahip midir?
- Türkiye ile incelenen ülkeler siber güvenlik insan kaynağının geliştirilmesi yatırım yapıyor mu?
- Türkiye ile incelenen ülkelerde kamu düzeyinde eğitim sağlanması hedefine sahip midir?
- Türkiye ile incelenen ülkeler devlet, iş dünyası ve sivil toplum arasında ortaklık kurmaya çalışıyor mu?
- Türkiye ile incelenen ülkeler siber saldırılara karşı yasal önlemlerin geliştirilmesi için çalışmalar yürütüyor mu?

- Türkiye ile incelenen ülkelerde siber caydırıcılığın oluşturulması hedefine sahip midir?

Çalışmanın son alt amaç ise Türkiye'nin güçlü ve kapsamlı bir siber güvenlik stratejisi ve eylem planı hazırlaması için yapılması gerekenlerin belirlenmesidir. Bu alt amaca inceleme sonunda elde edilen bulgulardan yararlanılarak ulaşılması hedeflenmiştir.

Araştırmanın önemi

Türkiye geçmişte 2013-2014 ve 2016-2019 dönemlerini kapsayan stratejileri ve eylem planları hazırlamıştır. Daha sonra 2020 yılının sonunda 2020-2023 dönemini kapsayacak stratejisi ve eylem planı (kamuoyuna açıklanmamıştır) yürürlüğe koyulmuştur. Ancak strateji ve eylem planlarının sürekliliği ve kurumsal yapının oluşturulması açısından sorunlar yaşanmaktadır. Bu çalışma ile İngiltere ve AB ülkeleri stratejileri ve eylem planlarının incelenmesi sonucunda elde edilen bulgular kullanılarak strateji ve eylem planlarının sürekliliği, kurumsal yapının kurulması ve güçlü bir strateji ve eylem planı için içeriğin nasıl olması gerektiği ortaya koyulmaya çalışılmıştır. Stratejiler ve eylem planları önceden belirlenen hedeflere ulaşılması için takip edilecek adımların belirlendiği belgeler olduğundan siber güvenlik alanında bütüncül bir politika yürüten İngiltere ve AB ülkeleri ve incelenmiştir. Çalışmanın önemi ulusal güvenlik ve özelde ulusal siber güvenlik eylem planının başarısının dayanaklarının oluşturulmasıdır. Böylece Türkiye'nin siber güvenlik düzeyinin yükselmesi, saldırılara karşı caydırıcılığının yüksek olması, siber güvenlik alanında lider ülke konumuna ulaşması ve bilişim alanında gelişme sağlaması mümkün olabilir.

Varsayımlar

Siber güvenlik alanı neredeyse tüm dünya ülkelerinin dışında kalmasının mümkün olmadığı kadar küresel, kullanılan teknolojiler açısından benzer özelliklere sahip ve en önemlisi gelişmeye açık yeni mücadele alanı olmasından dolayı ülke amaç veya hedefleri yakınsamaktadır. Söz konusu gerekçelerden dolayı çalışma içinde AB ve İngiltere'nin siber güvenlik politikalarının diğer ülkeler ile benzer olduğu varsayılmıştır. Bunun yanı sıra Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization/NATO) veya Avrupa Güvenlik ve İşbirliği Teşkilatı (The Organization for Security and Co-operation in

Europe/ AGİT) gibi örgütler kendi yapıların siber güvenlik alanına özel önem vermektedir. AB ülkeleri, İngiltere ve Türkiye'nin söz konusu örgütlere üye olması ile üye ülkeler arasındaki işbirliği stratejilerin ve eylem planlarının da benzeşmesine katkı sağlamaktadır. Seçilen ülkelerin siber güvenlik alanındaki amaçlarının açık, erişilebilir ve karşılaştırılabilir olması örneklemin bir diğer gerekçesidir. Dünyadan izole ülkelerin dahi benzer hedeflere hareket ettiği ve diğer ülkelerle mücadele ettiği varsayılmakta olup siber güvenlik alanında yaşanan gelişmeler bu varsayımı güçlendirmektedir. Yapılan incelemeler ve değerlendirmeler neticesinde siber güvenlik stratejisi ve eylem planı açıklayan diğer dünya ülkeleri benzer amaç ve hedeflere sahiptir. Siber güvenlik alanında doküman açıklamayan kapalı rejimlere sahip ülkelerin ise uygulamaları, liderlerinin açıklamaları ve ülke içindeki gelişmeler incelenmiş olup aynı şekilde bu küresel alanda yer almaya çalıştığı gözlemlenmiştir. İngiltere ve AB ülkelerinin eylem planlarıyla stratejilerinin bu açıdan diğer dünya ülkeleriyle benzer olduğu varsayılmıştır. Böylece siber güvenlik alanında çalışan uzmanların görüşlerinden yararlanılarak elde edilen on bir kıyaslama kriterinin başarı değerlendirmesi yeterli olduğu varsayımı üzerinde durulmuştur. Strateji ve eylem planı kavramlarının iç içe geçmesinden ve strateji kavramının eylem planı kavramını kapsamasından dolayı incelenen ülke dokümanlarındaki hedef ve hedeflere ulaşılması için yapılması gerekenlerinin genel olarak ülke politikalarını açıkladığı varsayılmıştır. Ayrıca çalışmanın bir diğer varsayımı incelenen strateji ile eylem planı dokümanlarından elde edilen veriler ile Türkiye'nin gelecek eylem planına yönelik geliştirilen önerilerin tam olarak yeterli olduğudur.

Sınırlılıklar

Çalışmanın varsayımları genel olarak çalışmanın sınırlılıklarıdır. Bu açıdan incelenen ülkelerin AB'ye üye ülkeler ve İngiltere sınırlı tutulması çıkarımların bu bağlantıda yapılması çalışmanın temel sınırlılığı olarak değerlendirilebilir. Diğer yandan uzman görüşlerinden elde edilen değerlendirme kriterlerinin başarılı bir siber güvenlik stratejisi ve eylem planı belgesi için yeterli olduğunun öne sürülmesi çalışmanın diğer bir sınırlılığıdır. Strateji ve eylem planlarının ülkelerin tüm siber güvenlik politikasını kapsadığı hususu çalışmanın bir diğer sınırlılığıdır. Bazı ülkelerin sadece stratejilerine ulaşılırken bazı ülkeler eylem planlarını da (gizlilik dolayısıyla Türkiye dahil birçok ülke eylem planlarını kamuoyuyla paylaşmamıştır) kamuoyuyla paylaşmıştır. Bu açıdan stratejilerin daha kapsayıcı olmasından dolayı çalışmanın son sınırlılığı stratejilerin eylem planlarını

yansıttığıdır. Çalışma içindeki terim ve kavramlar ayrı bir başlık altında açıklanacağı için tanımlar kısmı bu bölümde ele alınmamıştır.

Tanımlar

Çalışma genel olarak güvenlik, siber güvenlik, siber güvenlik stratejisi, strateji ve eylem planı kavramlarına dayanmaktadır. Bu açıdan güvenlik bir toplumun ve özelde kişinin risklere, tehditlere ve korkulara karşı özgür hissetme, emin olma veya endişe duymama anlamında ele alınmıştır. Güvenliğin bir alt dalı olup 2000'li yıllardan sonra büyük gelişme gösteren siber güvenlik kişilere veya kurumlara ait olan bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve bilgileri (bilgisayar dilindeki kullanımıyla verileri) kötü amaçlı saldırılardan korumaktır. Strateji kelimesi genel olarak önceden belirlenen bir hedefe ulaşmak için izlenen adımları veya uygulanan yöntemleri ifade etmektedir. Bu açıdan strateji amaç veya amaçlar bütünü olup eylem planı stratejiye ulaşmak için kullanılacak araç veya araçlardır. Strateji belirlendikten sonra stratejiye ulaşmak için yapılması gerekenlerin ayrıntılı olarak tanımlandığı eylem planı oluşturulmazsa söz konusu amaçlara ulaşılması mümkün değildir. Benzer şekilde üst bir stratejiye sahip olmayan eylem planı zaman kaybıdır. Siber güvenliğin sağlanması hedefiyle oluşturulan eylem planları belirli bir dönem için oluşturulan stratejilere ulaşmak için yapılması gerekenlerin, hedeflerin önceliklerinin, hedeflerin yerine getirilmesinden sorumlu kurumların (veya kişilerin), hedeflerin gerçekleştirilmesinde ihtiyaç duyulan kaynakların ve dönemsel olarak hedeflerin nasıl izleneceğinin belirlendiği belgelerdir.

Bu çalışma ile ülkemizin, AB ülkelerinin ve İngiltere'nin siber güvenlik stratejileri ve eylem planları incelenmiştir. Stratejilerin ve eylem planlarının dayandığı gerekçeler açıklandıktan sonra kıyaslama yapılmıştır. Böylece hem strateji ve eylem planlarındaki farklılıklar ve benzerlikler ortaya çıkmış hem de ülkelerin hangi alanlara daha fazla önem verdiği açıklanmıştır. Siber güvenlik kavram ve uygulamalarının geniş bir alana yayılmasıyla, ülkelerin mevcut teknolojileri, yetişmiş insan gücü gibi pek çok faktör ile öncelikleri ve hedefleri değiştirmiştir. Çalışma ile bu farklılıklar ve öncelikler ele alınarak ülkelerin analizi yapılmıştır. Sonuç olarak bu farklılıklar ve öncelikler doğrultusunda Türkiye'nin gelecekteki stratejisi, eylem planı ve hedeflerine yönelik öneriler geliştirilmiştir.

Çalışmanın ikinci bölümünde, kuramsal çerçeve kapsamında güvenlik ve siber güvenlik kavramları ile söz konusu kavramlarla ilişkili diğer terimler ele alınmış ve çalışmanın ana gövdesi oluşturulmuştur. Üçüncü bölümde, Türkiye Siber Güvenlik Kurulu'nun yetki, görev ve sorumlulukları ele alınmış, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2016-2019 ile 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planları (son iki dönemin eylem planı açıklanmamıştır) detaylı bir şekilde incelenmiştir. Bunun yanı sıra, son güncel gelişmeler neticesinde ülkemizin siber güvenlik politikasının ana çerçevesi çizilmiştir.

Dördüncü bölümde, 28 ülkenin siber güvenlik stratejisi ve eylem planı irdelenmiştir. Ülkelerin en güncel siber güvenlik stratejilerine ve eylem planlarına erişilmiş, detaylı bir şekilde ortaya koyulan hedefler ele alınmıştır. Hedeflere ağırlık verilmesi için giriş veya tanımlara fazla odaklanılmamıştır. Daha çok ülkelerin değerlendirmeleri ile tespitlerine odaklanılmış, daha sonra siber güvenlik stratejileri ve eylem planlarının ana hedefleri ile bu hedeflerine erişmek için atacakları adımlar detaylandırılmıştır. Böylece çalışmanın kapsamının dağılmamasına özen gösterilmiştir.

Beşinci bölümde, araştırmanın yöntemi kapsamında kullanılan model, evren ve örneklem, verilerin toplanması, uygulama ve verilerin çözümlenmesi konuları açıklanmıştır. Altıncı bölümde çalışma kapsamındaki ülkelerin strateji ve eylem planlarında ortak olarak bulunan ve uzman görüşleriyle oluşturulan on bir kriter belirlenmiş ve buna göre ülkelerin stratejileri ve eylem planları kıyaslanmıştır. Bölüm sonunda bir çizelge oluşturularak hem konunun özeti çıkarılmış hem de ülkelerin birbiriyle karşılaştırmanın daha anlaşılır olması sağlanmıştır. Bunun yanı sıra seçilen kriterlerin geneli kapsaması için özen gösterilmiştir. Son olarak bölümün ikinci kısmında Türkiye için gelecek dönemde hazırlanacak eylem planına yönelik öneriler sunulmuştur.

Sonuç ve öneriler başlığı altında ise çalışmanın genel bir özeti yapılmış ve çalışma kapsamında ülkemizde oluşturulacak gelecek strateji ve eylem planlarına yönelik öneriler açıklanmıştır. Ayrıca çalışmanın literatürdeki yeri, katkısı ve önemi kısaca ele alınmıştır.

2. KURAMSAL ÇERÇEVE VE SİBER GÜVENLİK KAVRAMI

Öncelikli olarak kuramsal çerçeve bağlamının oluşturulması için güvenlik ve siber güvenlik kavramları ele alınacak olup siber güvenlik kavramının güvenli bir yapı kurulması arasındaki ilişki incelenecektir. Çalışmanın giriş ve temel kısmı olduğu için bölümün oldukça kısa tutulması amaçlanmıştır.

2.1. Kuramsal Çerçeve

Araştırmanın amacına problem kapsamındaki kavramlar açıklanarak çalışmanın kuramsal yapısının oluşturulması hedeflenmiştir. İlk olarak güvenlik olgusu ve bağlantılı konuları ile siber güvenlik kavramı ve bileşenleri alt başlıklar halinde incelenmiştir. Kısa ve öz bilgilere yer verilerek çalışmanın dayanak noktası olan strateji ve eylem planlarına genel bir hazırlık yapılmıştır.

2.1.1. Güvenlik kavramı

Güvenlik, uluslararası ilişkiler disiplininin çıkışından günümüze dek önemli bir kavram olarak karşımıza çıkmaktadır (Dedeoğlu, 2003: 11-12). Bu çerçevede gerek devletler gerekse pek çok uluslararası örgüt güvenliği temel alan politikalar geliştirmiştir (Terriff, Croft, James ve Morgan, 1999: 2-5).

Güvenlik kavramı farklı dönemlerde farklı şekillerde tanımlanmıştır. Tanımı kişiden kişiye, gruptan gruba, devletten devlete farklı tanımlanan "esası tartışılan" bir kavramdır (Buzan, Wæver ve Wilde, 1998: 21-23).

Güvenlik, yaşam içerisinde tek bir insandan başlayarak toplum ve devlet gibi sosyal örgütlenme biçimlerine kadar genişlemiş bir kavramdır. Abraham Maslow'un insan ihtiyaç hiyerarşileri içerisinde güvenlik ihtiyacı hususu, yeme ve barınmadan sonra ikinci önemli basamak olarak görülmüştür (Aydın, 2008: 308).

Güvenlik, kavram olarak korku, tehlike ve tehditlerden özgür hissetme hali olarak tanımlanmıştır. Bu tanımdan güvenliğin hem fiziksel ve psikolojik boyutu olduğu, hem de subjektif ve objektif tanımlamalara açık olduğu kolayca anlaşılabilir. Özellikle kavram,

psikolojik ve duygusal boyutu bakımından zihinsel süreçleri barındırması ile güvenliğin subjektif tarafına vurgu yapmaktadır (Ak, 2013: 10).

Nitekim subjektif güvenlik durumu, değerlere saldırı korkusunun ön plana çıkarılması ve bu saldırıların olmaması olarak tarif edilmektedir. Eğer subjektif güvenliğe ağırlık verilirse tehdit durumu ile tehdide yönelik tedbir ve önlemlere yapılan vurgu daha çok önem kazanmaktadır. Objektif bir güvenlik tanımında ise kazanılan değerlere karşı sadece tehdidin yokluğu belirtilirken, tedbirler ve önlemler kısmına ağırlık diğeri kadar yoğun olmamaktadır (Page, 2000: 33).

Tarih boyunca güvenliğin fiziksel boyutu üzerine durulmuş, devlet gibi siyasi örgütlenmelerin sınırlarının başka devletlerin saldırıları ve tehditlerinden uzak tutulması anlayışına karşılık geldiği görülmüştür. Bir devletin veya üzerinde yaşayan toplumun kendini güvende hissetmesi; fiziki ve zihni bir boyutla birlikte subjektif bir olgu olmuş, güvensizlik ihtimallerinin ortadan kaldırılması durumuna karşılık gelmiştir. Bu durum, güvensizlik durumlarının tehdit olarak görülmesi olarak da tanımlanmaktadır. Tehdit kavramı ise, gerçek olgu ve olaylara dayanması yanında algı ve tahminler temelinde gerçekleşme ihtimaline göre de şekillenebilmiştir. Güvenlik olgusundan söz edilebilmesi için, güvenliğe ait varlığın korunması ve sürdürülmesine yönelik iç veya dış tehdit algılaması ve tahminlerine gerek duyulduğu açıktır (Dönmez, 2010: 2).

Güvenlik için bireysel düzeyde mevcut olan mantıksal süreçlerin; toplum, devlet gibi örgütlenme biçimlerinde yeniden üretilmesi, farklı düzeylerde güvenlik konusunu meydana getirmiştir. Günümüze kadar toplumsal yaşam alanında kolektif güvenliğe yapılan vurgular, çoğunlukla devletlerin ulusal güvenliği çerçevesinde gerçekleşmiş, devlet temel aktör sayılmıştır (Vogler, 1996: 48).

2.1.2. Ulusal güvenlik

Güvenlik insanlığın gelişimini yönlendiren bir stratejik alandır. Tarihin tüm dönemlerinde güvenliğin sağlanması meselesi güncelliğini korumuş olup, toplumun ekonomik, toplumsal ve aynı zamanda siyasal gelişim düzeylerine orantılı olarak belli bir evrim geçirmiş ve günümüzdeki biçimini almıştır. Güvenlik ve güvenlik örgütlerinin tarihi tüm milletlerin ve devletlerin geçtiği tarihsel gelişim yoluyla sıkı bir bağı bulunduğuna göre bu alanın

öğrenilmesi en önemli işlerdendir. Ulusal güvenlik kavramının kökeni tarihin en derin katlarına kadar uzansa da "ulusal güvenlik" kavramını bir terminolojik ifade olarak ilk kez ABD Başkanı Ruzvelt'in ABD Kongresine göndermiş olduğu 1904 tarihli resmi mektupta geçmektedir. Ancak, bununla birlikte tarihten bellidir ki, güvenliğin sağlanması meselesi sistematik bir görev olarak ilk kez Doğu'da ortaya çıkmıştır. Kuşkusuz ki, insanlığın yaratıldığı günden beri güvenlik meselesi mağara insanından günümüzün çağdaş sivil toplum insanına kadar ve aynıyla kadim kabilelerden devlet yapılanmalarına kadar tüm kesimi ilgilendirmiştir (Qasimov ve Bağırov, 2008, 3-6).

Ulusal güvenliğin geçmişi siber güvenlik kavramının ortaya çıkmasından çok daha önce tanımlanmış ve tartışılmıştır. Ulusal siber güvenlik stratejisinin geliştirilmesine etki eden en önemli gerekçe ulusal varlıkları, ekonomiyi ve toplumsal değerleri güvence altına alma arayışlarıdır. Ulusal güvenlik terimi, II. Dünya Savaşı'ndan sonra öncelikli olarak ABD'de kullanılmaya başlanan askeri temelli bir kavramdır (Kademi, 2014: 7).

Yalın bir ifadeyle söylenirse, ülkenin ve yurttaşların her türlü güvenliğinin sağlanması anlamına gelen ulusal güvenlik kavramı, bu tanımlamadan ötürü basitliği aldatıcı olmamalıdır. Bunun başlıca nedeni ulusal güvenlik kavramının, birçok bilimsel disiplin ile sık ve karmaşık ilişkisinin olması ve uluslararası ilişkiler, siyaset, ekonomi, strateji, hukuk, savaş gibi bilim dallarını içinde barındırmasıdır. Daha net bir tanımlama yapılırsa, ulusal güvenlik; "*Devletin bekasının ve refahının sağlanması, bunlara yönelik tehdit ve risklere karşı gerekli tedbirlerin alınması, ortak kimlik ve değerlerin korunması suretiyle ulusal çıkarların gerçekleştirilmesi halidir*" (Varlık, 2015: 15, 17).

2.1.3. Siber güvenlik kavramının analizi

Siber güvenlik, siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetim yaklaşımları, faaliyetler, eğitim ve teknolojiler bütünü olarak tanımlanabilir (Wired, 2019). Siber güvenlik kavramını ikiye ayırıp tanımlamak gerekmektedir.

Siber kavramı

Siber kelimesi, dil bilimsel açıdan bilgisayar veya bilgisayar ağlarını ilgilendiren ya da içeren kavram veya varlıkları tanımlamak için kullanılan bir kelimedir. Yine literatürde çoğunlukla kullanılan siber uzay (cyber space) kelimesi de birbiriyle bağlantılı donanım, yazılım, sistem ve insanların iletişim veya etkileşimde bulundukları soyut veya somut alanı anlatmak için kullanılmaktadır (Klimburg, 2012). Dil bilimi açısından siber olarak ifade edilen kelime İngilizce'deki anlamı "*cyber*" kelimesine referans gösterilerek "*bilgisayar ağlarına ait olan*", "*internete ait olan*", "*sanal gerçeklik*" manalarında da kullanılmaktadır ve günümüzde bilişim ve iletişim ağlarının oluşturduğu uzayı ifade etmekte olan bir kavram olarak karşımıza çıkmaktadır (Lord, 2011: 76). Sibernetik kelimesi ise siber kelimesinden türeyerek, ilk olarak Norbert Wiener'in "*Sibernetik*" isimli eserinde, "*hayvanlarda ve makinelerde kontrol ve iletişim*" olarak tarif edilmiştir (Wiener, 1965, s. 99).

Bilgisayar kullanımındaki artış, benzeri görülmemiş toplumsal değişimlere yol açarak günlük yaşamda insan hayatı için önemli kolaylıklar sunmaya başlamıştır. İnternetin yaygın olarak kullanılmaya başlanması ile coğrafi sınırlar ortadan kalkmış, insanların her türlü elektronik bilgi hizmetine erişimini mümkün kılan ve "siber dünya" olarak tanımlanan yeni bir dünya oluşmuştur (Gibson ve Erle, 2006: 97). Siber, internete bağlı bilgisayar sistemlerini, iletişim altyapılarını, veri tabanlarını ve bilgi araçlarını barındıran, genellikle ağ (net) olarak bilinen küresel sistem olarak tanımlanabilmektedir (Birleşmiş Milletler, 2019). Bu tanımlardan yola çıkarak günümüzde siber uzayın tek bir uzaydan oluşmadığı, her biri farklı sayısal etkileşim ve iletişim yöntemi sağlayan birbiri ile iç içe geçmiş bir alan olduğu sonucuna ulaşabiliriz. Hızla gelişen ve homojen olmayan küresel bir sistemin varlığından söz edebiliriz (Ak, 2013: 21).

Siber güvenlik kavramı

Siber güvenlik kavramı üzerinde de kavramsal olarak uzlaşı sağlanmamış olmakla birlikte, literatürde bilgi güvenliği (*information security*) ve bilgisayar güvenliği (*computer security*) kavramları ile ilişkili olarak kullanılmaktadır. Bilgi güvenliği kavramı kişisel ve kurumsal verilerin korunması ile ilgili bir kavram olarak, bilgisayar güvenliği kavramı ise bilişim sistemlerinin güvenliğini ihtiva eden bir kavram olarak kullanılmaktadır. Siber güvenlik kavramının tanımı, bilişim sistemlerinin temel değeri olan bilgi üzerinden yapılmaktadır.

Siber uzayın güvenli olabilmesi için bilgiye dair üç temel hususun sağlanması gerekmektedir. Bilginin gizliliği (*confidentiality*), bütünlüğü (*integrity*) ve erişilebilirliği (*availability*) siber güvenliğin sağlanması için gereken hususlar olarak karşımıza çıkmaktadır (Goodrich ve Tamassia, 2010). Bu üç hususu siber güvenliğin temel hedefleri olarak da söylemek mümkündür (Uluslararası Telekomünikasyon Birliği, 2008).

Siber güvenliğin hedeflerini de esas alarak siber güvenlik basit bir şekilde tanımlanabilir. Siber güvenlik; kurum, kuruluş ve kullanıcıların varlıklarına ait özelliklerini siber uzayda bulunan güvenlik tehditlerine karşı korumak amacıyla kullanılan araçlar, güvenlik teminatları, politikalar, kılavuzlar, risk yönetim yaklaşımları, eğitim ve teknolojiler ile bu kapsamdaki faaliyetlerin bütününü kapsayan bir kavram olarak tanımlanabilir (Ünver, Canbay ve Mirzaoğlu, 2009).

Siber güvenlik, 2000 yılından sonra yaygınlaşan ve tehditleri azaltma konusunda stratejik bir bakış açısına sahip olan yeni bir terimdir. Bilgi devriminde ilk güvenlik kavramı olarak görülmektedir. Daha sonra, kapsamlı bir kavram olan bilgi güvenliği kavramı yaygınlık kazanmıştır. Siber güvenlik, bilgisayar ağlarında işlenen veya depolanan tüm bilgileri sürece dahil ederek büyümüştür. Bilgi dağılırken, bilgi güvenliği sorunu ortaya çıkmıştır. Son zamanlarda toplumun ilgi alanı siber güvenliğe kaydıkça internet güvenliği ile eşitmiş gibi bir algı oluşmuştur. Bundan da öte, aslında, siber güvenlik kavramı bilgi güvenliği, sistem güvenliği ve ağ güvenliği gibi pek çok kavramın toplamıdır. Siber güvenlik olarak aşağıdaki gibi açıklanabilir (Evans, 2011: 19-22):

- ✓ Bilgi ve iletişim sistemleri ile bilgi içeren veya işleyen süreçlerin işlemlerin herhangi bir zarar, anormal işlem, sömürüden korunma önlemleri, faaliyetleri, süreçleri, yetenekleri veya diğer durumları ifade eder. Bu, siber güvenliğin teknik kaynağı ile ilgilidir.
- ✓ Siber alanın güvenliğini artıran strateji, politika, ilkeler, standartlar ve mevzuatı ifade eder. Çeşitli araçların uygulanması ile tehdit ve kırılganlığın azaltılması, caydırıcılık, uluslararası katılım, esneklik konularını içeren; güvenli bir küresel bilgi ve iletişim altyapısı için diplomasi, askeri ve istihbarat faaliyetlerini kapsamaktadır. Bu stratejik güvenliğin mükemmelleştirilmesiyle ilgilidir.
- ✓ Kullanılan önlemler, faaliyetler ve politikaların bir sonucu olarak kişi, şirket veya devletin korumasını ifade eder.

- ✓ Profesyonellik, araştırma ve geliştirme kavramlarını içeren bir araştırma ve inceleme alanını ifade eder.

Siber güvenliğin birçok boyutu olmasına rağmen temel olarak aşağıdaki şekilde gösterilen yedi prensipten oluşmaktadır. Siber güvenliğini en üst seviyede sağlamak maksadıyla, uygulanan söz konusu prensipler aşağıdaki gibi tanımlanabilir (Ada, 2018:10):

- ✓ **Gizlilik:** Veriye sadece yetkili kişi veya sistemlerce erişilebilmesini ifade eder.
- ✓ **Bütünlük:** Verinin, göndericiden çıktığı haliyle bozulmadan ve değiştirilmeden alıcısına ulaşmasıdır.
- ✓ **Erişilebilirlik:** Yetkili kişilerin ve işlemlerin ihtiyaç duyulan zaman içerisinde ve ihtiyaç duyulan kalitede bilişim sistemlerine erişebilmesi demektir.
- ✓ **İzlenebilirlik:** Sistemde gerçekleşen olayların daha sonra analiz edilmek üzere kayıt altına alınmasıdır.
- ✓ **Kimlik Doğrulama:** Alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır.
- ✓ **Güvenilirlik:** Sistemde beklenen davranışlar ile elde edilen sonuçların birbiri ile tutarlı olmasıdır.
- ✓ **İnkâr Edememe:** Göndericinin gönderdiği mesajı, alıcının da aldığı mesajı inkâr edememesidir.

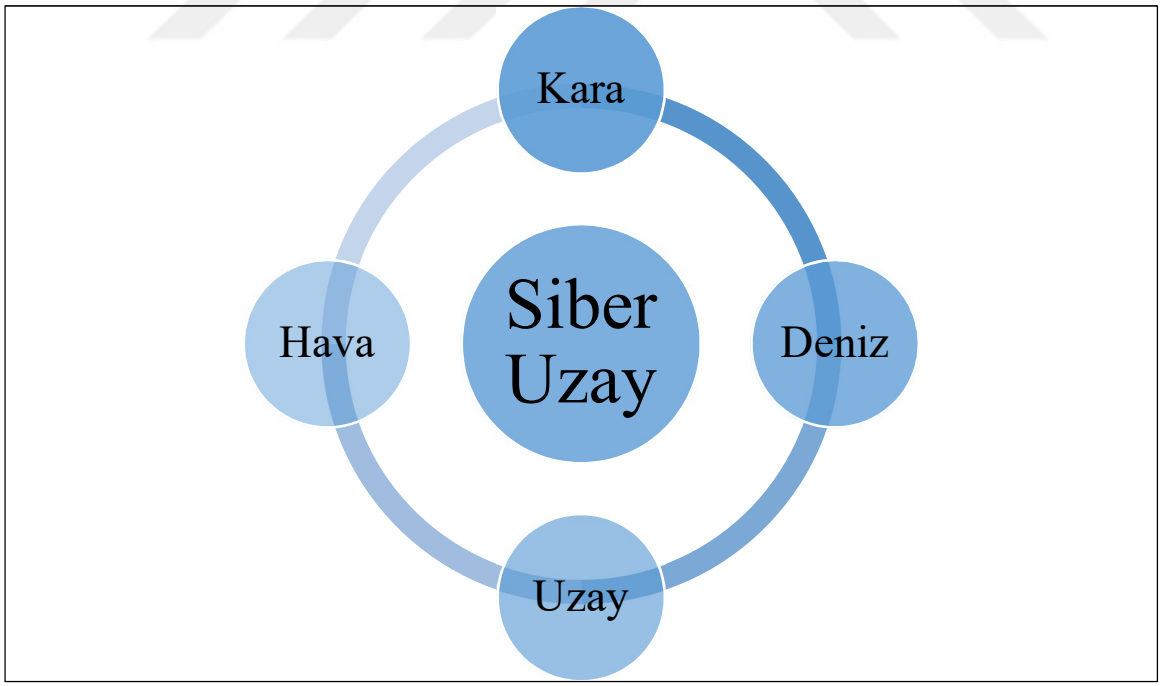
Çalışmalarında siber güvenliği ayrı bir sektör olarak değerlendiren Hansen ve Nissenbaum'un (2009) yaklaşımına göre siber güvenlik sektörü üç ayrı düzlemde değerlendirilmiştir. Bunlar; hiper güvenlikleştirme (*hyper securitization*), günlük güvenlik uygulamaları (ev*eryday security practises*) ve teknikleştirme (*technification*). Hansen ve Nissenbaum siber güvenliği büyük ölçekli, ani basamaklı afet senaryolarının hayata geçirilmesi olarak tanımlamaktadır. Günlük güvenlik uygulamaları, kişilerin gündelik yaşamda karşılaştıkları siber güvenlik olaylarının güvenlikleştirilmesini ifade etmektedir. Teknikleştirme ise siber güvenlik olgusunun normatif olarak istenebilen ya da politik olarak nötr olan konuların teknik bilgiye sahip uzmanlar tarafından yasallaştırılmasını ve kurumsal bir zemine oturtulmasını ifade etmektedir (Hansen ve Nissenbaum, 2009: 1164-1166).

2.1.4. Siber güvenlik kavramları

Siber kavramıyla ilişkili olan terimler bu bölümde kısaca açıklanmış olup çalışmanın literatür kısmı detaylandırılmıştır.

Siber uzay

İnternetin yaygın olarak kullanılmaya başlanması ile coğrafi kısıtlamalar ortadan kalkmış, insanların her türlü elektronik bilgi hizmetine erişimini mümkün kılan yeni bir dünya oluşmuştur. Bu dünya zamanla siber uzay olarak tanımlanmıştır (Ada, 2018: 9). "Siber Uzay" kavramı ilk olarak 1982 yılında bilim kurgu romanlarıyla bilinen William Gibson tarafından "*Burning Chrome"* adlı romanda kullanılmıştır. Ulusal Siber Güvenlik Stratejisinde "*siber uzay*" teriminin yerine "*siber ortam*" teriminin kullanılması tercih edilmiştir. Beşinci boyut olarak tanımlanan siber uzay; aşağıdaki şekilde görüldüğü gibi yeryüzü, hava, deniz hatta uzaydan bağımsız ve iletişim altyapılarını kullanan sanal bir ortamdır (Libicki, 2009: 12-13).



Şekil 2.1. Siber uzay bileşenleri

Siber saldırı

Siber tehditler; kişilerin, kurumların ve ülkelerin bilgi varlıkları ve teçhizatlarını hedef alan, onların mahremiyet, güvenlik ve iş görmesini bozan her türlü siber saldırılar ve yetkisiz müdahalelerdir. Siber korsanlar her geçen gün siber ortamda bulunan varlıklara sızmak için yeni yöntemler geliştirmektedirler. Sanal ortamda gerçekleştirilen bu eylemler karşısında olayın kurbanı olan bireyler gerek maddi gerekse manevi olarak mağdur olmaktadırlar. Siber saldırılardaki amaç; bilginin güvenliğini sağlamaya yönelik üç temel unsur olan gizlilik, bütünlük, erişilebilirlik prensiplerinin olumsuz yönde etkilenmesine neden olmaktır. Siber saldırılar;

- ✓ Sisteme yetkisiz erişim,
- ✓ Bilgilerin ifşa edilmesi,
- ✓ Bilgilerin çalınması,
- ✓ Sistemin bozulması,
- ✓ Bilgilerin değiştirilmesi,
- ✓ Bilgilerin yok edilmesi,
- ✓ Hizmetlerin engellenmesini hedeflemektedir.

General James Cartwright siber saldırıyı; bilgisayar, bilgisayar ağları veya sistemler kullanılarak düşmanın kritik sistemleri, varlıklarını yok etmeyi ve görevlerini yapamaz hale getirmeyi amaçlayan düşmanca bir davranış olarak tanımlamıştır (Cartwright, 2011: 5).

Siber uzayda, bireylerin ve siber güvenlik uzmanlarının kendi bilgisayarlarını korumalarını gerektirecek çok fazla saldırı çeşidi bulunmaktadır. Saldırganlar bu saldırı yöntemlerini kullanarak sızmış oldukları bilgisayar ya da bilgisayar ağlarına değiştirici, yıkıcı, hizmet aksatıcı ya da verileri sızdırma şeklinde çeşitli zararlar verebilmektedir. Bu zararların organizasyon ya da kamu kurumuna maddi zararları olabileceği gibi itibarının azaltılması şeklinde zararları da olmaktadır (Ada, 2018: 9). Siber saldırı tekniklerini aşağıdaki gibi sıralamak mümkündür:

Siber terörizm

Siber terörün tehdit potansiyeli gün geçtikçe artış göstermektedir. Günümüzde teknolojinin sunduğu imkânlardan terörist gruplarda faydalanmakta ve propaganda, eğitim, haberleşme, bilgi toplama gibi faaliyetlerde yaygın olarak kullanmaktadır. Siber terörizm söylemi, 1990'ların başlarında, internet teknolojilerinin hızla büyümeye başladığı, "bilgi toplumu" tartışmasının yapıldığı, teknoloji ve bilgisayar ağına fazlaca bağımlı olan ABD'nin karşılaşabileceği riskleri inceleyen çalışmaların arttığı dönemde başlamıştır.

Terörün bir alt kümesi olarak siber terör, terörist amaçları gerçekleştirmek için bilgisayarların bir silah, bir yöntem ya da bir hedef olarak kullanılmasıdır (Collin, 2004). Denning'e göre siber terörizm, bilgi sistemleri doğrultusunda elektronik araçların, bilgisayar programlarının veya diğer elektronik iletişim birimlerinin kullanılması aracılığıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan eylem veya etkinliktir (Denning, 2000: 1).

Siber casusluk

Son yıllarda siyasi amaçlı olduğuna inanılan birçok olay yaşandı. Söz konusu olayların büyük çoğunluğunu; kurbanın zaaflarından faydalanılarak icra edilen istihbarat toplama faaliyetleri, fikri mülkiyet hırsızlığı ve teknolojik bilgi hırsızlığı oluşturmaktadır. Siber casusluk, düşmanın veya rakibin hassas bilgilerine erişmek ve rakibine karşı avantaj sağlamak için bilgisayarlar veya dijital iletişim faaliyetlerinin kasıtlı olarak kullanılması olarak tanımlanabilir (O'Hara, 2010:241).

İngiliz hükümeti, çoğunlukla siber casusluk ve fikri mülkiyet hırsızlığından kaynaklı siber suçların 2011'de ekonomisine maliyetinin yaklaşık 44 milyon dolar olduğunu ya da bir diğer ifadeyle İngiliz yurt içi gayri safi milli hasılanın %2'sine eşit olduğunu tahmin etmektedir (Özbay, 2015: 12).

Bilgi toplama amacı ile yapılan hedef odaklı saldırıların yaygınlaşması yeni bir kavram olan APT (Advanced Persistent Threat - Gelişmiş Sürekli Tehdit) saldırılarının ortaya çıkmasını sağlamıştır. 2005 yılında sosyal mühendislik yöntemleri kullanılarak geliştirilen ilk APT saldırı uyarıları aynı yıl ABD ve Birleşik Krallık Siber Olaylara Müdahale Ekibi (Computer Emergency Response Team/CERT) makamları tarafından yayınlanmıştır. 2005 yılında ilk

raporların yayınlanmasına rağmen APT kelimesi ilk olarak 2006 yılında ABD Hava Kuvvetleri'nde görevli Albay Greg RATTRAY tarafından ifade edilmiştir. APT, hedef olarak belirlediği bilgi sistemlerine arasına girmek suretiyle kendini belli etmeden bulunduğu sisteme uyum sağlayan ve hassas bilgilere erişmeyi hedefleyen uzun süreli saldırı türüdür (Friedberg, Skopik, Settani ve Fiedler, 2015:35).

Siber suç

Siber suçlar, bilgisayarlar ve bilgi sistemlerini birincil araç ya da birincil hedef olarak kullanmak suretiyle geniş yelpazede işlenen suç faaliyetlerini ifade eder. Siber suçlar; geleneksel suçları (dolandırıcılık, sahtecilik ve kimlik hırsızlığı), içerikle ilgili suçları (internet üzerinden çocuk pornografisi dağıtımı, ırkçılıklar ilgili nefret suçları) ve bilgi sistemlerine özgü suçları (bilgi sistemlerine karşı yapılan saldırılar, hizmet dışı bırakma saldırısı ve kötücül yazılımlar) içermektedir (EC, 2013: 9).

Avrupa Konseyi Siber Suç Sözleşmesi'ne göre siber suçlar, bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar, bilgisayarlarla ilişkili suçlar, içerikle ilişkili suçlar ve fikri mülkiyet haklarının ihlali ile ilgili suçlar şeklinde sınıflandırılmıştır (CE, 2001).

Siber suçların yaygınlaşması ile birlikte siber suçlarla mücadele kapsamında küresel çapta tedbirler alınmaya başlanmıştır. Bu kapsamda, 1996 yılında Avrupa Suç Sorunları Komitesi internet ortamında işlenen suçları gözlemleyebilen uzmanlardan oluşan bir komitenin kurulması konusunda çalışmalar yapmıştır. Oluşturulan bu komite 2001 yılının Haziran ayında Avrupa Konseyi Siber Suç Sözleşmesini (The Council of Europe Convention on Cybercrime) kaleme almıştır. 8 Kasım 2001 tarihinde Avrupa Konseyi Bakanlar Komitesince bu sözleşme onaylanmış 23 Kasım 2001 tarihinde imzaya sunulmuştur. Macaristan'ın başkenti Budapeşte'de imzaya sunulan bu sözleşmeyi 43 Avrupa Konseyi üyesi devlet ve konseye üye olmayan 4 devlet (Kanada, Japonya, Güney Afrika ve ABD) imzalamıştır (Mahmutoğlu, 2002).

Türkiye, 10 Kasım 2010 tarihinde Uluslararası Siber Suç Sözleşmesi'ni imzalayarak anlaşmaya taraf olmuş ancak yürürlüğe girmesi 2 Mayıs 2014'te Resmi Gazete'de yayınlanmasıyla gerçekleşmiştir. Siber suçlar diğer bir ifadeyle bilişim suçları, 3756 sayılı

Kanun'la TCK 1989 Tasarısı'ndan küçük değişiklikler yapılarak alınmış ve 765 sayılı (mülga) TCK'nın 525a-525d maddelerinde ülkemiz bakımından ilk defa 1991 yılında düzenlenmiştir. Bilişim Suçları Türk Ceza Kanunu'nun ikinci kitabının "Topluma Karşı Suçlar" başlıklı üçüncü kısmında, "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde 243, 244, 245 ve 246. maddelerinde ele alınmıştır (Ada, 2018: 22).

Siber savaş

Siber alandaki faaliyetlerin kolay ve arkada iz bırakmadan yapılabilir oluşu terör örgütlerinin yanı sıra devletlerin de ilgisini çekmeye başlamıştır. Hatta kimi ülkeler siber saldırı ve siber savaş yöntemlerini önemli stratejik savunma ve rakibe zarar verme yöntemi olarak görmektedirler. Ülkelerin kendi çıkarları doğrultusunda bilgi ve iletişim teknolojilerini silah olarak kullanması, klasik konvansiyonel savaşın yerini almasını sağlamıştır (Ada, 2018:23).

Eski ABD Başkanı Bush'un Siber güvenlik danışmanı Richard A. Clarke "Cyber War" adlı kitabında siber savaşı şöyle tanımlamıştır: "*Siber savaş, bir devletin, diğer bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da bozmak amacıyla gerçekleştirdiği faaliyetlerdir.*" (Clarke ve Knake, 2010: 11).

Siber savaş, kendi içinde birçok yöntem ve teknik barındırmaktadır. Siber savaş meydanında kullanılabilecek çalışma alanları vardır. Casusluk, manipülasyon, propaganda, iletişimin kontrol altına alınması, virüs ve Truva atlarıyla sistemlerin bozulması, siber bombalarla sabotaj, sistem kilitleme, dolandırıcılık, bilgi kirliliği gibi birçok alan siber savaşın oluşumuna katkı sağlamaktadır (Kara, 2013: 40-41).

2.1.5. Siber saldırı teknikleri

Siber saldırı tekniklerine ilişkin açıklamaların yapıldığı bu bölümde çalışmanın literatür kısmı detaylandırılmıştır.

Oltalama saldırıları (Phishing)

Oltalama, istenmeyen e-posta veya yasadışı web sitesi aracılığıyla güvenilir bir kurumu taklit ederek; kullanıcı adı, parola, banka hesap numarası veya kredi kartı numarası gibi

kurum açısından hassas bilgilerin ele geçirilmesini amaçlayan adli açıdan suç vasfı taşıyan hileli bir süreçtir (Schreier, 2015: 61).

Oltalama saldırısı, Türk Ceza Hukukunda karşılığı olan ciddi bir suçtur. Bu yöntemle bankaların internet sitelerinin benzerlerini yaparak kullanıcıların banka hesap bilgileri ve parolalarını ele geçiren siber korsan 199 yıl hapis cezası ile cezalandırılmış, verilen bu ceza Yargıtay 8 inci Ceza Dairesi tarafından onanmıştır (Ada, 2018: 15).

Kötücül yazılım (Malware)

Kötücül yazılım, bilgisayar kullanıcılarının haberi olmaksızın, kullandıkları bilgisayarlara sızmak ve bu bilgisayarlara zarar vermek amacıyla kodlanmış yazılımların genel adıdır. Bilişim ağlarına yetkisiz erişim sağlamak için ve kullanıcılarının iradesi dışında farklı işlerde kullanılmak üzere yerleştirilir (OECD, 2009: 21). Kötücül yazılımların bulundurulduğu ülkeler bakımından Uzakdoğu ülkeleri miktar bakımından daha yoğun bölgeler olarak karşımıza çıkarken Avrupa ülkelerinde bu oran görece daha az olmaktadır. Bunun sebebi olarak hukuki altyapının oluşturulmuş olmasını ve önleme çalışmalarının daha yoğun olarak uygulanmasını söyleyebiliriz. Çin başta olmak üzere Türkiye ve Tayvan'da bilgisayarlara bulaşan kötücül yazılım oranlarının daha yüksek olduğunu söylemek mümkündür (Statista, 2016).

Truva atı

Truva atı, internet kullanıcıları için faydalı gibi görünen ancak içinde barındırdığı zararlı kodlar sebebiyle bilişim güvenliğine zarar veren bir program türüdür (OECD, 2009: 229). Truva atları, bilgisayarları kullanıcılarının isteğinin dışında yönetmek ve bilgisayarlara erişim sağlamak için arka kapı açan programlardır. Özellikle lisanslı ve ücretli yazılımların ücretsiz olarak sunulduğu siteler aracılığı ile indirilen programların çalıştırılması ile bilgisayarlara bulaşır. Farkında olmadan kullanıcı kendi faydasına olacak ücretsiz bir yazılım indirdiğini düşünürken arka planda bir Truva atı da yüklenmiş olabilir ve kullanıcının bilgisi dışında hatta çoğu zaman haberi bile olmadan çalışmayı sürdürmektedir. Truva atını kullanıcı bilgisayarına yerleştiren bilgisayar korsanları arka kapılar (back door) aracılığı ile kullanıcının bağlı olduğu sistemlere erişim sağlayarak kullanıcın bilgilerini kullandığı şifreleri ele geçirebilir (Canbek ve Sağıroğlu, 2007: 124).

Virüs

Virüsler, en eski ve en tehlikeli kötücül yazılım olarak bilinmektedir. Nitekim bilgisayar belleğine yerleşebilen, yerleştiği zaman programlarda değişikliklere yol açan; en önemlisi de kendi kendini çoğaltabilme özelliği bulunan zararlı yazılımlardır (Nickolov, 2008). Virüsler çoğaldıkları bilgisayarlarda bilgisayardaki verilere zarar vermenin yanında sisteme de zarar vererek sistemin çökmesine de neden olabilir. Virüsler bir dosyanın açılması, virüslü bir e-postanın okunması, virüs bulaşmış bir programın çalıştırılması gibi birçok farklı yolla bulaşabilir (Canbek ve Sağıroğlu, 2007).

Solucan

Solucan, Truva atına ve virüslere göre daha karmaşık yapıya sahip olan kötücül yazılımlardır. Genellikle e-posta aracılığı ile gönderilen ekler, çeşitli web siteleri ve bağlı bulunulan ağ üzerinde paylaşılan dosyaları kullanarak yayılırlar. (Nickolov, 2008: 37) Solucanlar, bir sisteme bulaştıklarında, kullanıcının başka bir eylemine gerek olmadan, kullanıcının veri kaynaklarını kullanabilirler. Bu sayede kendi kaynak dosyalarını hızlı bir şekilde farklı kullanıcılara da ulaştırmayı denerler ve bu yolla kendilerini çok fazla sayıda çoğaltabilirler. Solucanlar bunu yaparken kullanıcıların ağ kaynaklarını kullandıklarından ağların kilitlenmesine, e-posta sunucularının aşırı yüklenmesine veya web kaynaklarına erişim hızının düşmesine sebep olabilmektedirler (OECD, 2009: 227).

1988 yılında ortaya çıkan ve yazılımcısı Robert Tappan Morris'in ismiyle anılan Morris solucanı ilk bilinen solucandır. İnternete bağlı 60000 bilgisayarın 6000 adedine bulaşarak %10 gibi büyük bir orana ulaşmıştır (Nickolov, 2008: 37). Yazılımcısı tarafından, Morris solucanın kötü bir amacı olmadığı ancak yayılma mekanizmasındaki tasarım hatası nedeniyle acımasız bir saldırıya dönüştüğü belirtilmiştir. Ülkelerin bilgisayar uzmanları, solucanı saptamak ve temizlemek için çok zaman harcamışlardır. Binlerce askerin ve sivil araştırmacının bilgisayarlarından yoksun kalması da bilim dünyasına, siyasal ve sosyal yaşama negatif bir çıktı olarak yansımıştır. Solucanın yol açtığı maddi kayıp ise 15 milyon dolar olarak açıklanmıştır (Yıldırımoğlu, 2015).

Reklam içerikli ve casus yazılımlar

Reklam içerikli (adware) ve casus yazılımlar (spyware) bilgisayar kullanıcılarının istekleri dışında, sürekli reklam içerikli mail gelmesini ve bilgisayarlara yerleştirilen yazılımlar aracılığı ile kullanıcı bilgilerinin karşı tarafın eline geçmesini ifade etmektedir. Tarayıcısının varsayılan ayarları bilgisayara bulaşan reklam içerikli yazılım aracılığı ile değiştirilmektedir (Levine, 2016). Örneğin, kullanıcının ayarlamış olduğu arama motoru ya da ana sayfa olarak belirlediği web sayfası bu şekilde değiştirilmiş olabilir. Casus yazılımlar ise daha önce anlatılmış olan Truva atı, şifre kaydediciler, reklam içerikli yazılımları da kapsayan, kullanıcının bilgisayarına yerleşerek üçüncü kişilere bilgi aktaran yazılım türleridir. Bu programlar aracılığı ile elde edilen bilgiler farklı amaçlara ulaşmak için kullanılabilmektedir (Stafford ve Urbaczewski, 2004: 292). Bu kapsama istenmeyen e-postaları (spam) da dahil etmekte fayda vardır. Nitekim bu yolla normal reklam verme koşullarına haiz yöntemler izlenmeden, mali sorumluluklar yerine getirilmeden büyük kitlelere isteğinin dışında mesajlar gönderilmiş olmaktadır. İstenmeyen e-postalar kullanılmaya başladığında sadece rahatsız edici bir içerik gibi görünmesine rağmen teknolojinin de gelişmesiyle birlikte, istenmeyen e-postalara yerleştirilen kodlar ile kötücül yazılımların da yaygınlaşmasına sebep olmaktadır. İstenmeyen e-postalar bu şekilde kötücül yazılımlar aracılığı ile dolandırıcılık için de kullanılabileceği gibi, gelişen teknoloji ile paralel olarak cep telefonlarına, tablet bilgisayarlara da bu içerikler gönderilerek bu tür cihazların da kötücül yazılımlara malzeme olması sağlanmaktadır (OECD, 2006).

Botnet

Botnet, kullanıcıların bilgisi dışında bilgisayarlarına yerleşen kötücül yazılımlar aracılığı ile merkezi bir yerden çok sayıda kötücül yazılım bulaştırılmış bilgisayarlar kümesini ifade etmektedir. Kullanıcısının iradesi dışında kötücül yazılım bulaşmış olan bilgisayarlar terminolojide zombi olarak da nitelendirilmektedir. Botnet tek bir noktadan genellikle bir kişi tarafından kontrol edebilme yeteneği sağlamaktadır (Hogben, 2011). Bir zombiye dönüşmüş olan bilgisayarlar bu kişiden gelecek komutlar doğrultusunda farklı amaçlara hizmet etmek için kullanılabilmektedirler. Bu ağ sistemini yönetmek için tasarlanmış kötücül yazılımlara ise bot adı verilmektedir. Bu sayede bir botnet sahibi kötü niyetli kişi vereceği komutlarla dünyanın farklı yerlerindeki çok sayıda bilgisayarı amaçları doğrultusunda işlem yaptırabilmektedir. Kullanıcısının haberi olmadan gizlice bilgisayara

yerleşmiş olan kötücül yazılımlar aracılığı ile binlerce bilgisayar, botnet sahibi tarafından yönetilebilmekte ve kontrol edilebilmektedir (Uluslararası Telekomünikasyon Birliği, 2008: 7).

Hizmeti engelleme (DoS/DDoS) saldırıları

Hizmeti engelleme saldırıları günümüzde bilişim sistemlerinin erişilebilirliğine yönelik gerçekleştirilen en yaygın saldırı türü olarak karşımıza çıkmaktadır. DoS/DDoS saldırılarının kullandığı birçok yöntemdeki temel amaç, gerçekleştirilen siber saldırılar ile resmi bir kuruluşun ya da şirketin bilgi iletişim ağlarını kilitlemek ve verdiği hizmetleri engellemeye çalışmaktır.

Günümüzde hizmeti engelleme saldırılarının büyük çoğunluğu birden çok bilgisayar kullanılarak gerçekleştirilmektedir. Bir önceki bölümde anlatılan botnetler aracılığı ile bir kişi aynı anda binlerce bilgisayara komut vererek yönlendirdiği hedefe siber saldırı gerçekleştirebilmektedir. Zombi bilgisayarlar aracılığı ile hedef olarak belirlenen sisteme (bilgisayara ya da iletişim ağına) aynı anda çok sayıda giriş yapılmaya çalışılmaktadır. Bu yöntemle kaldırabileceği kapasitenin üzerinde bir yüklenme olması sebebiyle sitemler ve ağlar kilitlenerek iş göremez hale gelmektedir (CISCO, 2013).

Örnek olarak, sunucu hizmeti sağlayan bir firmadan belirli bir bant genişliği edinen ve buna göre maksimum olarak aynı anda bin kişinin girişine elverişli olan bir web sitesi düşünelim. Bu web sitesine aynı anda 10 bin kişinin girmeye çalışması durumunda, bu siteye girmeye çalışan çok sayıda kişinin aynı anda komut yollaması sonucunda web sitesi bu yükü kaldıramadığı için devre dışı kalabilmektedir. DDoS saldırısı, aynı anda çok sayıda kişinin hedef seçilen bir sisteme sürekli giriş yapmaya çalışması şeklinde olacağı gibi, bu işi otomatik bir şekilde yapan yazılımlar aracılığı ile hedef alınan sistemi devre dışı bırakarak hizmet veremez duruma getirebilmektedir (Ahi, 2011).

Sosyal mühendislik saldırıları

Sosyal mühendislik (social engineering), insanlar arasındaki iletişimdeki ve davranışlardaki modelleri “zafiyetler” olarak tanımlayıp, bu zafiyetlerden faydalanılarak güvenlik süreçlerini atlatma yöntemine dayanan eylemlere verilen isimdir (Bican, 2008). Sosyal

mühendislikte kullanılan yöntemler olarak karşımıza hedefe güvenilir bir kaynak olduğunu hissettirmek, ortak tanıdıklar üzerinden yakınlık kurmak, özellikle iletişim araçları ile başkasını taklit etmek, gizlice zor bir durum oluşturarak yardım ediyormuş izlenimi vermek, hedef sistemin çöp olarak attığı kişisel bilgileri karıştırmak örnek olarak verilebilir (Gragner, 2001).

APT (Advanced Persistent Threat/Gelişmiş Kalıcı Tehdit) saldırıları

APT, yetkisiz bir ağa erişildikten sonra orada tespit edilmeden erişilen ağda uzun süre kalınan saldırı çeşididir. APT saldırılarında esas amaç verilerin çalınması ya da ele geçirilmesi değildir. Buradaki asıl amaç erişilen ağda uzun süre kalınarak bu ağa veya kuruluşa zarar vermektir. APT saldırıları, ulusal savunma, imalat ve finans sektörü gibi bilgi değeri yüksek olan sektörler hedef alınarak gerçekleştirilir. (Chen, Desment ve Huygens, 2014: 64)

2.2. İlgili Araştırmalar

Literatür taraması yapıldığında İngiltere ve AB ülkelerinin stratejileri ve/veya eylem planlarının ayrıca incelendiği bir çalışmaya rastlanmamıştır. Ancak Türkiye ve diğer ülkelerin strateji ve/veya eylem planlarının veya politikalarının incelendiği pek çok çalışma hazırlanmıştır. Konu ile doğrudan bağlantılı çalışmalar aşağıda sıralanmıştır:

- Eylül AYDIN tarafından 2021 yılında yayımlanan "*Study of The Cyber Security Measures: Comparative Work of the Unıted States and Turkey*" isimli çalışmada ilgili ülkelerin siber güvenlik politikası karşılaştırılmış ve ülkelerin maruz kaldığı saldırılara karşı gösterdiği tepkiler kıyaslanmıştır.
- Muhammet OĞUZ tarafından 2021 yılında yayımlanan "*Stratejiden Yasaya Avrupa Birliği Siber Güvenlik Politikası*" isimli çalışmada AB'nin ortaya koyduğu yasal düzenlemeler çerçevesinde AB siber güvenlik sisteminin bileşenleri incelenmiştir.
- Sayed Osman SAYEDI tarafından 2020 yılında yayımlanan "*Ulusal Siber Güvenlik Stratejisi Oluşturma Süreç Analizi ve Türkiye İle Afganistan'ın Ulusal Siber Güvenlik Stratejisinin Değerlendirilmesi*" isimli çalışmada ilgili ülkelerin ulusal siber güvenlik stratejileri değerlendirilmiş ve sorunlara karşı alternatif çözüm üretme yolunda adım atılması sonucuna ulaşılmıştır.

- Efe DÜVERLİOĞLU tarafından 2020 yılında yayımlanan "*Kritik Altyapı Siber Güvenlik Politikalarının Karşılaştırılmalı Analizi: ABD, AB ve Türkiye'den En iyi Uygulamalar*" isimli çalışmada incelenen ülkelerin yasal, kurumsal ve ekonomik uygulamaları karşılaştırılmış ve Türkiye'nin kritik altyapıların korunması politikasında ABD ve AB'den geri olduğu saptanmıştır.
- Cihan ATAÇ tarafından 2019 yılında yayımlanan "*Ulusal Siber Güvenlik Stratejisi Oluşturma Sürecine Bir Bakış*" isimli çalışmada Uluslararası Telekomünikasyon Birliği (ITU) ve Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı dokümanları incelenmiş ve çalışma kapsamında oluşturulan modele yönelik çıkarımlar yapılmıştır. Daha sonra ABD, İngiltere, Japonya gibi ülkelerle ile Türkiye'nin stratejisi incelenmiş ve çeşitli yönlerden karşılaştırılmıştır.
- Zeynep Ebru IŞIK tarafından 2019 yılında hazırlanan "*Siber Güvenlik Ekosisteminin Geliştirilmesi*" isimli çalışmasında Türkiye'nin siber güvenlik ekosisteminin oluşturulmasındaki işlemleri incelenmiş ve 2016-2019 Ulusal Siber Güvenlik Stratejisi'nde yer alan kamu kurumlarının siber güvenlik ekosisteminin geliştirilmesine etkileri değerlendirilmiştir. Çalışma sonunda siber güvenlik ekosisteminin geliştirilmesine katkı sağlayacak temel kıstaslar açıklanarak Türkiye'nin siber güvenlik ekosistemi için model önerisi oluşturulmuştur.
- Mehmet ADA tarafından 2018 yılında yayımlanan "*NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi*" isimli çalışmada NATO'nun ve NATO üyesi ülkelerin uyguladığı siber güvenlik stratejisi incelenmiş ve Türkiye'nin uyguladığı siber güvenlik stratejisine yönelik öneriler sunulmuştur.
- Volkan GÖÇOĞLU tarafından 2018 yılında yayımlanan "*Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi*" isimli çalışmada 28 adet resmi yayım incelenmiş ve belgelerin içerikleri NVivo 11 nitel veri analizi programı yardımıyla analiz edilmiştir. Analiz sonucunda, Türkiye'nin siber güvenlik ve kritik altyapı politikalarının kamu politikası analizi yaklaşımları ve karar verme modelleri çerçevesindeki yönelimleri, üretilen politikaların özellikleriyle birlikte ortaya konulmuştur.
- Ali Burak DARICILI tarafından 2017 yılında yayımlanan "*Amerika Birleşik Devletleri Ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi*" isimli çalışmada örnek ülkeler kıyaslanmış ve ABD ve Rusya'nın siber güvenlik

stratejilerini şekillendirme süreçlerinde etkileşim içinde oldukları sonucuna ulaşılmıştır.

- Mehmet EREN tarafından 2016 yılında yayımlanan "*Avrupa Birliği'nin Siber Güvenlik Politikası*" isimli çalışmada AB'nin siber güvenlik politikası incelenmiş ve birçok konuda AB'nin ileri olmasına rağmen iş birliğinin tam gerçekleşmediği sonucuna ulaşılmıştır.
- Akın AYTEKİN tarafından 2015 yılında yayımlanan "*Türkiye'nin Siber Güvenlik Stratejisi ve Eylem Planının Değerlendirilmesi*" isimli çalışmada İngiltere ve Amerika Birleşik Devletleri ile Türkiye'nin strateji belgeleri incelenmiş ve Türkiye özelinde öneriler geliştirilmiştir.

3. TÜRKİYE'NİN SİBER GÜVENLİK STRATEJİLERİ VE EYLEM PLANLARI

Bu bölümde Türkiye'nin Siber Güvenlik Kurulu ve siber güvenlik stratejileri ile eylem planları detaylı olarak ele alınacak olup strateji ve eylem planı ana başlıklar olarak ele alınacaktır.

3.1. Siber Güvenlik Kurulu

Bakanlar Kurulu'nun 11/06/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Bu karar ile Siber Güvenlik Kurulu kurulmuş, Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkileri oluşturulmuş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır.

5809 sayılı Elektronik ve Haberleşme Kanunu'na eklenen Ek Madde 1 ile de Siber Güvenlik Kurulu düzenlenmiş ve Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik ile ilgili yeni görevler verilmiştir. 5809 sayılı Elektronik ve Haberleşme Kanunu'na eklenen Ek Madde 1 ile Kurul'a aşağıdaki görevler verilmiştir (EHK, 2008):

a) Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak,
b) Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak,
c) Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek,
d) Kanunlarla verilen diğer görevleri yapmak.

Kanunun ilk halinde kurulun üyeleri ve görevi sayılmış olmasına rağmen daha sonra 02/07/2018 tarihli 703 sayılı Kanun Hükmünde Kararname'nin 205. maddesi ile müsteşarlıklar kaldırıldığı için mülga edilmiştir. Görevler kanunda yer almasına rağmen kurul ortada olmadığı için yeni bir düzenlemenin yapılması gerektiği düşünülmektedir.

1 sayılı Cumhurbaşkanlığı Kararnamesi'nin 26. maddesi ile Güvenlik ve Dış Politikalar Kurulu oluşturulmuş olup Kurula "*siber güvenlik ile ilgili politika ve strateji önerileri geliştirmek*" görevi verilmiştir. Bunun yanı sıra aynı Kararnamenin 527. maddesi ile kurulan Dijital Dönüşüm Ofisinin bir yetkisi de "*siber güvenlik ve bilgi güvenliğini artırıcı projeler geliştirmek*"tir (1. CK, 2018).

Dijital Dönüşüm Ofisi tarafından 2020 yılının Temmuz ayında Bilgi ve İletişim Güvenliği Rehberi yayımlanmış ve rehber bilgi işlem birimine sahip veya bilgi işlem hizmetlerini dış kaynak kullanarak yürüten kamu kurum ve kuruluşlarıyla birlikte kritik altyapı hizmeti veren

işletmeleri kapsamaktadır. Rehberin temel amacı bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle gizliliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve uygulanması olarak açıklanmıştır. Rehber kapsamında iki yıl içinde ulaşılması planlanan 12 adet hedef belirlenmiş olup söz konusu hedefler aşağıda sunulmuştur (Rehber, 2020):

- Yerli ve milli ürün kullanımının teşvik edilmesi,
- Rehberi uygulayacak kurum ve kuruluşlarda yapılacak mükerrer çalışmaların ve yatırımların önüne geçilmesi,
- Güvenlik tedbirlerinin üç seviyeli olacak şekilde derecelendirilmesi ve varlık gruplarına güvenlik dereceleri ile uyumlu asgari güvenlik tedbirlerinin uygulanması,
- Rehberin güvenlik tedbirleri ile ilgili detayların izlenebilirliğinin sağlanacak şekilde yapılandırılması,
- Güvenlik tedbirlerinin ürün ve teknoloji bağımsız olarak uygulanabilir olması,
- Güvenlik tedbirlerinin uygulanıp uygulanmadığının denetlenebilmesi,
- Güvenlik tedbirlerinin birbirinden bağımsız şekilde uygulanabilirliğini sağlayacak şekilde gruplandırılması ve rehberin modülerliğinin sağlanması,
- Tedbirlerin teknik olarak tüm kurum ve kuruluşlar tarafından uygulanabilir olması,
- İhtiyaçlar, gelişen ve değişen şartlar dikkate alınarak rehberin sürdürülebilirliğinin sağlanması,
- Rehberin format ve içeriğinin özgün olması,
- Rehberin hem güvenlik tedbirlerini uygulayacak personele hem de bu tedbirlerin uygulanıp uygulanmadığını kontrol edecek denetçilere hitap etmesi ve

- Rehber içeriğinin bilgi güvenliği çerçevesinde oluşturulmuş mevzuat ve rehberler ile ulusal/uluslararası standartlara uyumlu olmasıdır.

Yine Dijital Dönüşüm Ofisi tarafından 2021 yılının Ekim ayında Bilgi ve İletişim Güvenliği Rehberi kapsamında yapılması gereken iş ve işlemleri kontrol edilmesindeki süreci tanımlayan Bilgi ve İletişim Güvenliği Denetim Rehberi yayımlanmış olup rehber de kurum ve kuruluşlara bilgi ve iletişim güvenliği uyum faaliyetlerinin denetiminde; denetimin planlanması, denetim prosedürlerinin uygulanması ve denetim sonuçlarının raporlanması konusunda izlenmesi gereken metodolojiye yer vermektedir (Rehber, 2021).

Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı (BTK)'nın 2019-2023 Stratejik Planındaki siber güvenlik ile hedefler aşağıda özetlenmiştir (SP, 2019):

- ✓ Siber güvenliğin artırılması ve elektronik ortamda kullanıcı güveninin oluşturulması (ana stratejik amaç)
- ✓ …elektronik haberleşme güvenliğinin sağlanması ve ulusal siber güvenliğin sağlanmasında yetkinliğin artırılması,
- ✓ Ulusal siber güvenliğe yönelik faaliyetler kapsamında siber saldırılara karşı korunma ile bu saldırılara karşı caydırıcılık sağlamak için gerekli tedbirlerin alınmasını sağlamak ve bu konuda gerekli yaptırımları uygulamak,
- ✓ Ülkelerin siber güvenlik yeteneklerinin geliştirilmesi (siber güvenlik stratejisinin oluşturulması, acil müdahale ekiplerinin kurulması),
- ✓ Ulusal ve/veya uluslararası siber güvenlik tatbikatları düzenlenecek,
- ✓ Siber güvenliğe yönelik kamu spotu için temalar oluşturulacak,
- ✓ Türkiye'nin ülkemizin kritik altyapı sistemlerinin siber güvenliğinin izlenebileceği bir merkeze sahip olması,
- ✓ Yurtiçi ve yurtdışından uzman akademisyenlerin katılımıyla Siber Güvenlik Akademisinin oluşturularak siber güvenlik alanında ihtiyaç duyulan uzman personel açığının kapatılması

olarak belirlenmiştir. Aşağıdaki bölümlerde hazırlanan strateji ve eylem planları ile eylem planlarında yer alan hedefler yer almaktadır.

3.2. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, Siber Güvenlik Kurulu tarafından belirlenen politika, strateji ve eylem planları çerçevesinde kendilerine verilen görevleri yerine getirmek ve belirlenen usul, esas ve standartlara uymakla yükümlüdür. Bu kapsamda hazırlanan, 2013-2014 döneminde gerçekleştirilmesi planlanan işlere ilave olarak bu yılları aşan periyodik faaliyetler ile eğitim ve bilinçlendirme çalışmaları gibi sürekli yürütülmesi gereken faaliyetlere de yer veren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı 20/06/2013 tarih, 28683 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının amacını aşağıdaki gibi özetlemek mümkündür (UDHB, 2013):

- ✓ Kamu kurum ve kuruluşlarınca bilgi teknolojileri (BT) üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
- ✓ Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,
- ✓ Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına yönelik bir altyapı oluşturmaktır.

Söz konusu amaçlardan yola çıkılarak 13 adet ilke belirlenmiştir. Bu ilkelere tüm kamu kurumlarının uygulaması beklenmiş olup hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilmiştir. İlkeler aşağıda sıralanmıştır (UDHB, 2013):

1. Siber güvenlik, risk yönetimini esas alan etkin ve sürekli iyileştirmeye dayalı yöntemler aracılığıyla sağlanır.
2. Siber güvenlik için teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutlarda güçlü ve zayıf yönlerin, tehditlerin ve fırsatların belirlenmesini içeren bütüncül bir yaklaşım benimsenir.

3. Risk yönetiminde, teknik zaafların giderilmesi, saldırı ve tehdidin önlenmesi ile muhtemel zararın en aza indirgenmesi unsurları esas alınır.
4. Siber güvenliğin sağlanmasında birey, kurum, toplum ve devletin tüm hukuki ve sosyal sorumluluklarını yerine getirmesi esas kabul edilir.
5. Kritik altyapıların güvenliğinin sağlanması için, özel sektörle, karar mekanizmalarına katılımı da içeren tam işbirliği yapılır.
6. Siber ortam güvenliğinin sağlanması ve sürdürülmesinde kamu, özel sektör, üniversiteler ve sivil toplum örgütleri işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir.
7. Uluslararası işbirliği ve bilgi paylaşımı için diplomatik, teknik ve kolluk iletişim kanallarının sürekli ve etkin kullanımı esas alınır.
8. İhtiyaç duyulan mevzuat geliştirilirken uluslararası anlaşma ve düzenlemeler göz önünde bulundurulur.
9. Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilir.
10. Siber ortamda şeffaflık, hesap verilebilirlik, etik değerler ve ifade özgürlüğü desteklenir.
11. Güvenlik ile kullanılabilirlik arasında denge kurulur.
12. Denetleyici ve düzenleyici kurumlar sorumlu oldukları alanlarda siber güvenliğin sağlanmasını gözetirler.
13. Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, inovasyon anlayışı esas kabul edilir.

Yukarıda belirtilen amaçlar doğrultusunda ve belirlenen ilkeler ışığında, ulusal siber güvenliğin sağlanmasına yönelik stratejik eylemlerin gerçekleştirilmesi planlanmıştır. 2013-2014 döneminde gerçekleştirilmesi planlanan ve 7 ana başlıkta toplanan stratejik eylemler ve alt eylemler şöyledir (UDHB, 2013):

1. *Yasal Düzenlemelerin Yapılması*
   a. Siber Güvenlik Kurulunun faaliyetlerine başlaması
   b. Siber güvenlik konusunda mevzuat çalışmalarının yapılması
2. *Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi*
   a. Siber olayların delillendirilmesi

3. *Ulusal Siber Olaylara Müdahale Organizasyonunun oluşturulması*
   a. Ulusal Siber Olaylara Müdahale Merkezinin (USOM) kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması
4. *Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi*
   a. Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı
   b. Kamu Bilgi Güvenliği Programı
   c. Siber Güvenlik eğitim altyapısının güçlendirilmesi
   d. Siber güvenlik tatbikatları düzenlenmesi
   e. Kamu Güvenli İletişim Kurallarının Belirlenmesi
   f. Yazılım Güvenliği Programının Yürütülmesi
   g. Siber Tehditleri Önleme Projesinin yürütülmesi
   h. Siber güvenlik konusunda ürünlerin ve hizmet sağlayıcıların akredite edilmesi
   i. Adli bilişim konusunda hizmet sağlayıcılara güvenlik belgesi verilmesine yönelik kuralların belirlenmesi
   j. İş sürekliliği ve veri yedekleme sistemleri kurulması
   k. Kamu kurum ve kuruluşlarının internet sayfalarının yerli veri merkezlerine taşınması
   l. Veri sızmasını tespitine yönelik test altyapısı geliştirilmesi ve uygulamaya alınması
   m. Kamu kurumlarında verilere erişim düzeylerinin belirlenmesi
   n. Açık kaynak kodlu ürünlerin kullanımının teşvik edilmesi
5. *Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirilme Faaliyetleri*
   a. Siber güvenlik konusunda akademisyen yetiştirilmesi
   b. Üniversitelerde siber güvenlik eğitimlerinin yaygınlaştırılması
   c. Siber güvenlik uzmanlığına yönlendirme programının yürütülmesi
   d. İlk, orta, lise öğretimi ve yaygın eğitimde siber güvenlik eğitimlerinin yaygınlaştırılması
   e. Bilgisayar kullanıcılarının siber güvenlik konusunda bilinçlendirilmesi
   f. Ulusal ve uluslararası siber güvenlik etkinlikleri düzenlenmesi
6. *Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi*
   a. Ar-Ge faaliyetlerinin teşvik edilmesi
   b. Siber güvenlik konusunda Ar-Ge laboratuvarlarının kurulması
   c. Siber güvenlikte yerli ürün ve çözüm çalışmaları yerli ürünlerin teşvik edilmesi

7. *Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi Her eylem için sorumlu ve ilgili kurum ve kuruluşlar belirtilmiştir.*
   a. Ulusal siber güvenliğin milli güvenliğe entegrasyonu:

Eylem planında, siber güvenliğe ilişkin eylemlerin planlaması için siber güvenlik alanındaki risklerin belirlenmesi amaçlanmıştır. Siber Güvenlik Eylem Planında bilgi ve iletişim sistemleri ile ilişkili 18 adet siber güvenlik riski belirlenmiş olup söz konusu riskler aşağıda sıralanmıştır:

1. Siber ortamın bilişim sistemlerine ve veriye yapılan saldırılar için anonimlik ve inkâr edilebilirlik fırsatları sunması, saldırı için gerekli araç ve bilginin çoğu zaman ucuz ve kolay elde edilebilir olması, dünyanın herhangi bir yerindeki kişi veya sistemlerin kasıtlı ya da kasıtsız olarak siber saldırılara iştirak edebilmeleri nedeniyle tehdidin asimetrik olması,
2. Siber ortamın bütünleşik ve kesintisiz iletişime açık yapısı ve siber ortamda bulunan kötücül yazılım ve benzeri tehdit ajanları nedeni ile siber ortamda yer alan tüm bilişim sistemlerinin birbirlerine zarar verebilmesi,
3. Günümüzde büyük kitlelere sunulan kritik hizmet ve servislerin birçoğunun bilişim sistemleri tarafından sağlanıyor ya da kontrol ediliyor olması,
4. Kritik altyapılara ait bilişim sistemlerinin çoğunun internete bağlı olması,
5. Siber güvenliğin ulusal düzeyde bütün vatandaşlarca topyekün sağlanabileceği gerçeğine rağmen bu konudaki ulusal bilincin yetersiz olması,
6. Siber güvenlik alanında paydaş kurumların arasında ulusal koordinasyon eksikliği,
7. Kişi ve kurumların kamuoyu önünde saygınlıklarını kaybetmemek amacıyla veya başka sebeplerle kendilerine yönelik saldırıları gizlemesi,
8. Siber güvenlik olaylarının araştırma ve soruşturulmasında ulusal ve uluslararası mevzuat yetersizliklerinin işbirliğini güçleştirmesi,
9. Kritik altyapı hizmet ve servislerinin, gerçekleştirilen siber saldırılara ek olarak bilişim sistemlerinin kendi hatalarından, kullanıcı hatalarından ya da doğal afetlerden de olumsuz olarak etkilenmesi ve bu tür olaylara yönelik alınabilecek tedbirler açısından gerekli yeterliliğe sahip olunmaması,
10. Kurumlarda bilgi güvenliği yönetimi altyapılarının yeterli düzeyde olmaması,
11. Siber güvenlik konusunda kurumsal ve kişisel seviyede yeterli bilgi ve bilinç seviyesine ulaşılamamış olması,

12. Siber güvenlik konusunda kurumların üst düzey yöneticilerinin yeterli bilince sahip olmamaları veya siber güvenlik konusunu yeterince sahiplenmemeleri,
13. Siber güvenlik konusunda kurumların yapılanmalarının yetersiz olması ve siber güvenliğin, kurumların sadece bilgi işlem birimlerinin sorumluluğunda görülmesi,
14. Bilgi işlem birimlerinde çalışanların siber güvenlik konusunda yeterli bilgi seviyesine ve tecrübeye sahip olmaması,
15. Siber güvenlik olaylarının detaylı araştırılması ve ihlal ile ortaya çıkan suçun soruşturulması alanlarında ancak az sayıda yeterli personel bulunması,
16. Kurumsal iç denetim süreçlerinde siber güvenliğe ilişkin denetim adımlarının yeterli seviyede ele alınmaması,
17. Siber güvenliğin, geliştirilen veya tedarik edilen bilişim sistemlerinin vazgeçilmez bir unsuru olarak ele alınmaması, buna bağlı olarak kamu kurumlarının bilgi ve iletişim teknolojileri alanındaki ürün ve hizmet tedariklerinde siber güvenliğin yeterli seviyede göz önünde bulundurulmaması,
18. Donanım ve yazılım alanında yerli üretimin yeterli düzeyde olmaması.

Riskler ve eylemler ile ilgili tüm kurum ve kuruluşların, sorumlu kurum ve kuruluşların koordinatörlüğünde hareket ederek eylemin gerektirdiği çalışmaları yürütmeleri öngörülmüştür. Eylem planında yer alan eylemlerin bir kısmı için bitirilme tarihi belirlenmiş, periyodik olarak tekrarlanması ve sürekli olarak yürütülmesi öngörülen eylemler ise ayrıca belirtilmiştir. 2013-2014 döneminde, gerçekleştirilmesi planlanan toplam 29 adet eylem maddesi bulunmaktadır. Eylem planında yer alan 29 adet eylemin, stratejik eylem başlıklarına dağılımı özetlenmiştir. Ayrıca 29 adet eylem toplamda 86 adet alt eylemden oluşmaktadır.

2013-2014 Siber Güvenlik Eylem Planı'nda belirlenen toplamda 86 alt eylemin sorumlu kurumlara göre dağılımını yine eylem planında belirlenmiştir.

3.3. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

Gelişen bilgi ve iletişim teknolojileri, artan güvenlik gereksinimi ve edinilen tecrübeler doğrultusunda, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından ulusal siber güvenlik stratejisinin güncellenmesi ve 2016-2019 dönemini kapsayan eylemlerin belirlenmesi ihtiyacı doğmuştur. Bu kapsamda öncelikle eski eylem planında sorumlu veya

ilgili olarak yer alan kurumlarla 10 Mart-7 Nisan 2015 tarihlerinde yedi adet değerlendirme toplantısı yapılmıştır. Toplantılarda eski eylem planında yer alan faaliyetlerin gerçekleşme dereceleri ve karşılaşılan güçlüklere ek olarak ileriye dönük değerlendirmeler ve siber güvenlik kapsamında gerçekleştirilmesi gereken faaliyetler de detaylı olarak belirlenmiş ve kaydedilmiştir. Toplantıların ardından kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarını temsilen 73 kurum ve kuruluştan toplam 126 uzmanın katılımı ile Ortak Akıl Platformu gerçekleştirilmiştir. İki gün süren platform çalışmaları kapsamında; Türkiye'nin siber güvenlik boyutunda güçlü ve zayıf yönlerinden hareketle stratejik amaçları ve gerçekleştirmesi gereken eylemler belirlenmiştir (UDHB, 2016).

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanırken paydaşlarla birlikte gerçekleştirilen çalışmalara ilave olarak geri planda kaynak taraması da yapılmıştır. Bu kapsamda, Amerika, Avrupa ve Uzak Doğu'dan çok sayıda ülkenin siber güvenlik stratejileri gözden geçirilmiş, ülkelerin siber güvenlik alanında kapsam, hedefler, öncelikler, organizasyon yapısı, kaynak tahsisi, Ar-Ge (Araştırma ve Geliştirme) koordinasyonu, kamu özel sektör işbirliği, eğitim gibi başlıklarda üretmeye çalıştığı çözümler değerlendirilmiştir.

Bütün kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin, Siber Güvenlik Kurulu tarafından belirlenen politika, strateji ve eylem planları çerçevesinde kendilerine verilen görevleri yerine getirmek ve belirlenen usul, esas ve standartlara uymakla yükümlü olduğu belirtilmiştir (UDHB, 2016).

Tüm bu çalışmalar kapsamında üretilen bilginin toplanması, incelenmesi ve değerlendirilmesi sonucunda "*2016-2019 Ulusal Siber Güvenlik Stratejisi*" ve "*2016-2019 Ulusal Siber Güvenlik Eylem Planı*" hazırlanmıştır.

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının ana amacı; siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu anlayışının tüm kesimlerde yerleşmesi, ulusal siber uzayda bulunan sistem ve paydaşların tamamının güvenliğini sağlamak üzere idari ve teknolojik önlemlerin alınmasını sağlayacak yetkinliğin eksiksiz bir şekilde kazanılmasıdır. Belirlenen ana amaç doğrultusunda (UDHB, 2016):

- ✓ Ulusal siber uzayın tamamını kapsamak şartıyla, BT üzerinden sağlanan her türlü hizmet, işlem ve bilgi/veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin, gizliliğinin ve mahremiyetinin sağlanmasına,
- ✓ Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kolluk kuvvetlerince daha etkin araştırılmasının ve soruşturulmasının sağlanmasına,
- ✓ Siber güvenliğin, gizliliğin ve mahremiyetin sağlanmasında kritik teknolojilerin ve ürünlerin ülkemizde üretilmesine, üretilemiyorsa, dışarıdan alınan teknoloji ve ürünlerin salt bu maksatla ve güvenle kullanılabilmesini sağlayacak önlemlerin alınmasına yönelik bileşenler bu planda yer almaktadır.

Dünya çapında siber güvenlik stratejileri ve eylem planları incelenerek öne çıkan 3 ilke ve 6 risk tespit edilmiştir. Söz konusu ilkeler (UDHB, 2016):

1. Siber güvenliğin sağlanmasında birey, kurum, toplum ve devletin tüm hukuki ve sosyal sorumluluklarını yerine getirmeleri,
2. Kamu, özel sektör, üniversiteler ve sivil toplum örgütleri koordinasyonu, müşterek katılım, iş birliği ve bilgi paylaşımı,
3. Uluslararası Siber Güvenlik Operasyon Merkezleri arasında gelişmiş siber olay yönetimi işbirliği.

Eylemde incelenen dokümanlarda dikkat çeken riskler ise aşağıdaki gibi belirlenmiştir (UDHB, 2016):

1. Toplumun sosyal ağlara bağımlılığı,
2. Kritik kurum ve kuruluşların siber uzaydaki konumları,
3. Çeşitli siber casusluk çalışmaları ve hedefli saldırılar,
4. Personel ve yetkinlik bağlamında yetersizlik,
5. Kurumlar arası koordinasyon eksikliği,
6. Siber uzayda faaliyet gösteren farklı ölçeklerdeki sektörlere yönelik ekonomik kaygılar.

Eylem planının kapsamı, kamu bilişim sistemlerine ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerine ilave olarak küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dâhil olmak üzere ulusal siber uzayın ülkemiz ölçeğindeki bütün bileşenlerini kapsayacak şekilde geniş tutulmuştur. Eylem planında ulusal siber güvenliğin sağlanmasında göz önünde bulundurulacak 8 ilke oluşturulmuş olup söz konusu ilkeler aşağıda sunulmuştur (UDHB, 2016):

1. Siber güvenlik, risk yönetimini esas alan etkin ve sürekli değerlendirmeye ve iyileştirmeye dayalı yöntemler aracılığıyla sağlanır. Oluşturulan risk yönetimi metotlarının tehdit ve açıklıkları ele alarak bunlardan dolayı ortaya çıkacak riskleri belirlemesi, bu riskleri kabul edilebilir düzeye indirmek için yöntemler sunması hedeflenir.
2. Siber güvenliğin sağlanması için tüm paydaşların siber güvenlik risklerini bilmeleri, bu risklerin yönetilmesine ilişkin yaklaşımlarının kendileri kadar başkalarını da etkileyebileceğinin bilincinde olmaları gerekir. Bu farkındalık ve yetkinliğin sağlanması için tüm paydaşların gerekli eğitim ve deneyimi kazanmaları sağlanır. Teknik boyutun yanı sıra; hukuki, idari, ekonomik, politik ve sosyal boyutları da içeren bütüncül bir yaklaşım benimsenir.
3. Risk yönetimi, teknik zaafların hızla giderilmesini, saldırı ve tehditlerin önlenmesini, fark edilmesini, yanıtlanmasını ve muhtemel zararın en aza indirgenmesini içerir. Zararların asgari düzeyde tutulması için siber olaylara karşı bir hazırlık ve süreklilik planının bulunmasına ve uygulanmasına önem verilir.
4. Siber uzay güvenliğinin sağlanması ve sürdürülmesinde; kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlar arasında işbirliğinin yanı sıra uluslararası işbirliği ve bilgi paylaşımı esas kabul edilir ve güven inşa edilir.
5. Tüm paydaşlar, siber uzay güvenliğinin sağlanması için çalışırken, hukukun üstünlüğü, ifade özgürlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkelerini gözetir.
6. Paydaşlar siber uzaydaki risklerin yönetimi ile ilgili sorumluluklarını yerine getirirken şeffaflık, hesap verilebilirlik ve etik değerleri göz önünde bulundurur.
7. Alınan siber güvenlik önlemlerinin ilgili risklerle orantılı olması, olumlu ve olumsuz etkilerinin değerlendirilmesi ve dengelenmesi sağlanır.

8. Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, yenilikçilik anlayışı esas kabul edilir.

Siber Güvenlik Eylem Planında siber güvenlik kapsamında stratejik amaçların en doğru şekilde tanımlanabilmesi amacıyla 10 adet risk belirlenmiştir. Söz konusu riskler (UDHB, 2016):

1. Kritik altyapıların kullandığı bilişim sistemlerine yapılacak hizmet dışı bırakma ve benzeri hedef odaklı saldırılar sonucunda enerji, ulaştırma, vb. kritik hizmetlerin kesintiye uğraması.
2. Kamu ve kritik altyapıların kullandığı bilişim sistemlerine yapılacak hedefe yönelik saldırılar sonucunda; vatandaşa ait kişisel bilgilerin veya kamuya ait gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
3. Araştırma, geliştirme ve üretim yapan kurum ve kuruluşların (özel firmalar, araştırma kurumları ve savunma sanayi) ticari sırlarını ve bilgi birikimini elde etmeye yönelik hedef odaklı saldırılar sonucunda hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
4. Propaganda amaçlı bilgisayar korsanlığı (hacktivizm) saldırıları sonucu çeşitli kurum ve kuruluşların itibarının zarar görmesi veya hassas bilgi/verinin ifşa olması, değiştirilmesi veya yok edilmesi.
5. E-ticaret yapan kuruluşların, E-posta hizmeti veren kuruluşların, sosyal medya hizmeti veren kuruluşların hizmet dışı bırakma ve benzeri saldırılar sonucunda hizmet verememesi nedeniyle maddi kayba uğraması, sahte işlem kaydı oluşturulması, gizli bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.
6. E-ticaret yapan kuruluşların, finans sektörü veya çevrimiçi ödeme ya da para transferine imkan veren diğer kuruluşların müşterilerine ait hassas bilgilerin saldırganlar tarafından ele geçirilmesi nedeni ile itibar kaybına uğraması, toplumda çevrimiçi işlemlere yönelik güven kaybı oluşması, bu hizmetlerden faydalanan müşterilerin maddi kayba uğraması.
7. Küçük ve orta ölçekli sanayi, ticaret ve hizmet sektöründeki kuruluşların faaliyetlerinin bilişim sistemlerindeki güvenlik önlemlerinin eksikliğinden veya

kullanıcı hatalarından dolayı kesintiye uğraması, hassas veya ticari değere sahip bilgilerin saldırganların eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi.

8. Toplumun internete ve sosyal ağlara olan bağımlılığı, siber güvenlik alanında yeterli düzeyde bilgi ve bilinç seviyesine sahip olmaması, mobil ve sabit bilgi sistemlerinde kişisel güvenlik önlemlerini almaması gibi nedenlerle kötücül yazılım ve oltalama saldırılarına, dolandırıcılık ve kimlik hırsızlığına maruz kalması, kişisel bilgilerin ve cihazların saldırganlar tarafından ele geçirilmesi, değiştirilmesi veya yok edilmesi, sahte işlem yapılması.
9. Her türlü kurum ve kuruluşta yığın posta, kötücül yazılım ve benzeri saldırılar sonucunda dolandırıcılıkla karşı karşıya kalınması.
10. Her türlü kurum ve kuruluşta, kullanıcı hataları ya da doğal afetler sonucunda bilişim sistemleri aracılığı ile verilen hizmet ve faaliyetlerin kesintiye uğraması.

Planda belirlenen stratejik amaçlara ulaşmak için gerçekleştirilecek eylemler aşağıda belirtilen beş stratejik eylem başlığı altında toplanmaktadır (UDHB, 2016).

1. Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması
2. Siber Suçlarla Mücadele
3. Farkındalık ve İnsan Kaynağı Geliştirme
4. Siber Güvenlik Ekosisteminin Geliştirilmesi
5. Siber Güvenliğin Milli Güvenliğe Entegrasyonu

Her eylem için sorumlu ve ilgili kurum ve kuruluşlar belirtilmiştir. Bu durumda, ilgili tüm kurum ve kuruluşların, sorumlu kurum ve kuruluşların koordinatörlüğünde hareket ederek eylemin gerektirdiği çalışmaları yürütmeleri öngörülmektedir (UDHB, 2016).

Eylem planında yer alan eylemlerin bir kısmı için bitirilme tarihi belirlenmiş, periyodik olarak tekrarlanması ve sürekli olarak yürütülmesi öngörülen eylemler ise ayrıca belirtilmiştir. Bu Eylem Planı döneminde, gerçekleştirilmesi planlanan toplam 41 adet eylem maddesi bulunmaktadır. 2016-2019 dönemini kapsayan Eylem Planının amaçları aşağıda sunulmuştur (UDHB, 2016):

1. Ulusal kritik altyapı envanterinin oluşturulması, kritik altyapıların güvenlik gereksinimlerinin karşılanması ve bu kritik altyapıların bağlı oldukları düzenleyici kurumlar tarafından denetlenmesi.
2. Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması.
3. Sektör düzenleyici kurum, bakanlık vb. kuruluşların siber güvenlik kapsamında düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi.
4. Kurumların bilişim sistemlerinin sadece saldırılardan değil, kullanıcı hataları ve afetlerden de korunması için düzenlemelerin yapılması.
5. Her kurumun kendi bilgi güvenliği yönetim sürecini çalıştıracak yetkinliğe ulaşması.
6. Siber güvenlik konusunda kurum yöneticilerinin farkındalığının artırılması.
7. Siber güvenlik alanında yetkin personel yetiştirilmesi ve bu alanda uzmanlaşmak isteyen personel, araştırmacı ve öğrencilerin teşvik edilmesi.
8. Toplumun her kesiminde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması.
9. Kamu kurumlarında siber güvenlik alanında uzman personel istihdam edilmesi için mevzuat desteği sağlanması ve personelin özlük haklarının iyileştirilmesi.
10. Kurumsal ve Sektörel SOME'lerin (Siber Olaylara Müdahale Ekibi) etkinliğinin arttırılması için mevzuat desteğinin sağlanması, mali düzenlemelerin yapılması, yetkin personel ihtiyacının karşılanması, bilişim altyapısının sağlanması ve ulusal siber olaylara müdahale organizasyonu kapsamında bilgi paylaşımının geliştirilmesi.
11. Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması.
12. Kamu kurumları, özel sektör, STK'lar (Sivil Toplum Kuruluşu), denetleyici kurumlar, üniversiteler, geliştirici firmalar ve tüm diğer paydaşların katılım ve koordinasyon hedefi ile ulusal siber güvenlik eko-sisteminin oluşturulması.
13. Ulusal Siber güvenlik eko-sistemi içinde iyi örneklerin yaygınlaştırılması, danışmanlık hizmetlerinin verilmesi, açıklık, tehdit ve faydalı uygulamaların paylaşılması.
14. Bilişim sistemlerinin kritik noktalarında kullanılan, yerli veya yabancı donanım ve yazılım ürünlerinin içerdiği açıklıkların kötüye kullanılmasına engel olmak üzere açıklık analizi ve sertifikasyon çalışmalarının yapılması.
15. Güvenli yazılım geliştirme ve tedarik yönetimi kültürünün oluşturulması.

16. Siber güvenlikte dışa bağımlılığı azaltmak için Ar-Ge faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi.
17. Tehdit unsurlarının saldırı yapmadan önce bertaraf edilmesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi.
18. Tehdit unsurlarının siber uzaydaki en büyük avantajı olan anonimliği ortadan kaldırmak için etkin kayıt yönetimi ve IPv6 (Internet Protokolü sürüm 6) teknolojilerinin yaygınlaştırılmasını asgari düzeye indirmeyi

hedeflemektedir. Eylem planı bölümü açıklanmamış olup genel olarak stratejilerden eylemler oluşturulduğu için açıklanan bilgilerin strateji ve eylem planını açıkladığı sonucuna ulaşılmıştır.

3.4. 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 29 Aralık 2020 Tarihli ve 31349 Sayılı Resmi Gazete'de yayımlanmıştır. Eylem planı toplam 12 bölümden oluşmakta olup hizmete özel kısmı tablolar şeklinde kamuoyuna açıklanmamıştır. Yönetici özetinde, ulusal siber güvenlikte çıtanın her geçen gün daha da yukarıya çıkarılması güçlü ulusal stratejilerle mümkün olduğu, Ulusal Siber Güvenlik Stratejisi ve Eylem Planının (2020- 2023), Türkiye'nin siber güvenlik alanındaki vizyonu ve misyonu doğrultusunda gelecek 4 yıllık döneme ilişkin politikalarını konu almakta olduğu, bundan önce hayata geçirilen stratejilerde elde edilen kazanımların daha yukarı taşınmasını hedeflemekte olduğu ifade edilmiştir (UDHB, 2020).

2013-2014 dönemi ile 2016-2019 döneminde gerçekleştirilen ve süreklilik arz eden eylemler, mevcut durum ve planlanan çalışmalar kapsamında yeni eylem planında gözden geçirilmiş ve gerekli iyileştirmelerin yapılmıştır.

Stratejik amaçlar doğrultusunda planlanan kazanımların elde edilmesine yönelik eylemlerin belirlenmesi için ulusal paydaşların katılımıyla düzenlenen Hazırlık çalıştayı düzenlenmiştir. Söz konusu çalıştaylara 67 kurumdan 127 katılımcı iştirak etmiştir. Eylem planının ikinci bölümünde kavramlar ile ilgili tanımlamalara yer verilmiştir. Üçüncü bölümde eylem planının giriş kısmı yer almakta olup dünya çapındaki gelişmeler değerlendirilmiştir. İnternetin kullanıcı sayısının ulaştığı nokta siber güvenlik konusuna

dikkat çekmektedir. Uluslararası Telekomünikasyon Birliği (ITU) verilerine göre 2019 yılı sonu itibarıyla dünya nüfusunun yaklaşık %53,6'sının, yani 4,1 milyar insanın, internet kullanıcısı olduğu değerlendirilmektedir. Türkiye'deki duruma bakıldığında; Bilgi Teknolojileri ve İletişim Kurumu (BTK) Türkiye Elektronik Haberleşme Sektörü 2020 yılı 2. Çeyrek Raporu'na göre 2008 yılında yaklaşık 6 milyon olan genişbant internet abone sayısı, 2020 yılı ikinci çeyreği itibarıyla 78,4 milyona ulaşmıştır. Türkiye İstatistik Kurumu (TÜİK) verilerine göre 2020 yılında Türkiye'de 16-74 yaş arası bireylerde internet kullanım oranı %79 seviyesindedir (UDHB, 2020).

Türkiye'de siber güvenlik başlığı altında aşağıdaki tespit ve değerlendirmelere yer verilmiştir (UDHB, 2020):

- Son dönemde siber güvenliğin sağlanmasına yönelik hız kazanan çalışmalarla, risklerin minimize edilmesi, yönetilebilir ve kabul edilebilir düzeylerde tutulması hedeflenmektedir.
- "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", 20 Haziran 2013 tarihinde yürürlüğe girmiştir. 2 yıllık bu dönem içerisinde siber güvenlik mevzuatının geliştirilmesi, kritik altyapıların güvenliğinin sağlanması, toplumda siber güvenlik farkındalığının oluşturulması, siber tehditlerin tespiti ve önlenmesi konularında çalışmalar yürütülmüştür.
- Ayrıca 2013 yılında, BTK bünyesinde faaliyetlerini sürdüren Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuş, belirlenen kritik altyapı sektörleri başta olmak üzere kurum ve kuruluşlarda Siber Olaylara Müdahale Ekipleri (SOME) faaliyetlerine başlamıştır.
- Sonrasında yayımlanan "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile de siber güvenlik risklerinin yönetilebilir ve kabul edilebilir düzeylerde tutulabilmesi için siber savunmanın güçlendirilmesi, kritik altyapıların korunması, siber suçlarla mücadele edilmesi, farkındalık ve insan kaynağı geliştirilmesi, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin milli güvenliğe entegrasyonu konularında çalışmalar yürütülmüştür.
- Uluslararası Telekomünikasyon Birliği Global Siber Güvenlik Endeksi'nin 2019'da yayımlanan sonuçlarına göre Türkiye bir önceki yıla göre 23 sıra birden yükselerek 2018 yılında dünyada 20'nci sırada, Avrupa'da 11'inci sırada yer almıştır.

- 2020-2023 dönemini kapsayan eylem planında ise siber tehditlerin etkilerinin azaltılması, ulusal kabiliyetlerin geliştirilmesi, daha güvenli bir ulusal siber ortamın oluşturulması ve ülkemizin siber güvenlik alanında uluslararası seviyede en üst sıralarda yer alması hedeflenmektedir.

Eylem planının vizyonu; "*Ülke ekonomisinin geliştirilmesini, toplumsal yaşamın korunmasını ve milli güvenliğin sağlanmasını desteklemek için; ülkemizde güvenli biçimde işleyen bir siber ortama sahip olmak ve siber güvenlikte uluslararası alanda marka haline gelmek.*" ve misyonu ise "*Siber güvenliğin milli güvenliğimizin ayrılmaz bir parçası olduğu bilinci ile kritik altyapılarımız başta olmak üzere siber uzaydaki varlıklarımızın tehditlerden korunmasına ve siber olayların muhtemel etkilerini azaltmaya yönelik çalışmaları ilgili tüm paydaşlarla koordineli olarak gerçekleştirmek.*" olarak belirlenmiştir (UDHB, 2020).

2020-2023 Dönemi Eylem Planının ilkeleri aşağıdaki gibi belirlenmiştir (UDHB, 2020):

1. Siber güvenlik, ulusal güvenliğin ayrılmaz bir parçasıdır. Ulusal güvenliğin tam olarak sağlanabilmesi, siber güvenlik alanında belirlenen hedeflere ulaşılabilmesine dayanır.
2. Siber güvenlik ile ilgili çalışmalar geçmişten geleceğe kazanımlar, hedefler, programlar ve projeler açısından kurumsallık, süreklilik ve sürdürülebilirlik ilkelerine göre yürütülür.
3. Dijitalleşmenin başarılı ve sürdürülebilir olması için siber güvenliğin hayati bir öneme sahip olduğu göz önünde bulundurulur.
4. Siber güvenlik politikalarının uygulanmasına yönelik tüm çalışmalar, paydaşların etkin iletişimi ve koordineli iş birliği içerisinde ve uygun metodolojilerle yürütülür.
5. Paydaşlar, siber uzaydaki risklerin yönetimi ile ilgili sorumluluklarını yerine getirirken şeffaflığı, hesap verebilirliği ve etik değerleri göz önünde bulundurur. Siber güvenliğin milli güvenliğinin ayrılmaz bir parçası olduğu bilinci ile kritik altyapılar başta olmak üzere siber uzaydaki ülke varlıklarının tehditlerden korunmasına ve siber olayların muhtemel etkilerini azaltmaya yönelik çalışmaları ilgili tüm paydaşlarla koordineli olarak gerçekleştirmek.
6. Siber güvenlik riskleri etkin bir şekilde belirlenir ve yönetilir.
7. Özellikle kritik altyapılar aracılığıyla verilen hizmetlerin kesintisiz ve etkin olarak sunulması esastır.

8. Hizmet ve ürünlerin ortaya konmasında, tasarımından son kullanıcıya erişimine kadar baştan sona tüm süreçlerde siber güvenlik kavramının dikkate alınması esastır.
9. Yürütülen iş ve işlemlerde bilginin "*gizlilik-bütünlük-erişilebilirlik*" dengesinin sağlanması ve "*bilmesi gereken prensibi*" gibi temel siber güvenlik prensiplerine sadık kalınması esastır.
10. Güçlü hukuki temeller üzerine güçlü bir siber güvenlik inşa edilmesi esastır.
11. Ar-Ge, yenilikçilik ve güçlü teknolojik altyapı anlayışı ile siber güvenlikte yerli ve milli ürün ve hizmet kullanımı teşvik edilir.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020- 2023) kapsamında belirlenecek ve gerçekleştirilecek hedeflerin, Türkiye'nin kısa, orta ve uzun vadede daha büyük ölçekli hedeflerine de katkı sağlayacağı değerlendirilmektedir. Eylem planının hedefleri aşağıdaki gibidir (UDHB, 2020):

- Kritik altyapılarımızın siber güvenliğinin 7/24 korunması.
- Ulusal seviyede siber güvenlik alanında en son teknolojik imkânlara sahip olunması.
- Operasyonel ihtiyaçlar çerçevesinde yerli ve milli teknolojik imkânların geliştirilmesi.
- Siber olaylara müdahalenin olay öncesi, esnası ve sonrasını kapsayan bir bütün olmasından hareketle; proaktif siber savunma anlayışının geliştirilmeye devam edilmesi.
- Siber olaylara müdahale ekiplerinin yetkinlik seviyelerinin ölçülmesi ve izlenmesi.
- Siber olaylara müdahale ekiplerinin yetkinliklerinin artırılması.
- Kurumsal, sektörel ve ulusal bazda siber olaylara hazırlık seviyelerinin risk temelli analizler ve planlamalara dayalı yaklaşımlarla artırılması.
- Kurum ve kuruluşlar arası veri paylaşımının güvenli biçimde sağlanması.
- Kaynağı ve hedefi yurt içi olan veri trafiğinin yurt içinde kalması.
- Kritik altyapı sektörlerinde düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi.
- Kritik altyapı sektörlerinde, BT ürünlerinde üretici bağımlılığının önüne geçilmesi.
- Yeni nesil teknolojilerin güvenliğinin sağlanmasına yönelik gereksinimlerin belirlenmesi.
- Yenilikçi fikirlerin ve Ar-Ge faaliyetlerinin desteklenerek yerli ve milli ürün ve hizmetlere dönüşümünün gerçekleştirilmesi.

- Toplumun tüm kesimleri tarafından siber uzayın güvenle kullanılması.
- Siber güvenlik farkındalığının tüm toplumda üst seviyede tutulmasına yönelik etkinliklerin sürdürülmesi.
- Kurum ve kuruluşlarda kurumsal bilgi güvenliği kültürünün yerleşmesi.
- Çocukların siber ortamda korunmasının sağlanması.
- Siber güvenliğe ilgi duyan veya uzmanlaşmak isteyen bireylere yönelik projelerle insan kaynağının güçlendirilmesi.
- Örgün ve yaygın eğitimde siber güvenlik eğitiminin yaygınlaştırılması ve eğitim içeriklerinin zenginleştirilmesi.
- Ulusal ve uluslararası düzeydeki paydaşlarla bilgi paylaşımı ve iş birliğini sağlayacak mekanizmaların geliştirilmesi.
- Siber suçların en aza indirgenmesi ve caydırıcılığın artırılması.
- İnternet ve sosyal medyada doğru ve güncel bilgi paylaşımının sağlanmasına yönelik mekanizmaların geliştirilmesi.

2020-2023 dönemi için bu temel odak alanları "*stratejik amaçlar*" olarak ifade edilmektedir. Siber güvenlikte ülkemizin 2023 vizyonunun gerçekleşmesi ve 2023 sonrasına güvenle yol alınması amacıyla belirlenen stratejik amaçlar aşağıda yer almaktadır (UDHB, 2020):

I. KRİTİK ALTYAPILARIN KORUNMASI VE MUKAVEMETİN ARTIRILMASI

a. *"Siber Uzayda Ulusal Güvenlik":* Kritik altyapılar; "*işlediği verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar*" olarak tanımlanmaktadır. Türkiye'de "*Elektronik Haberleşme*", "*Enerji*" "*Finans*", "*Ulaştırma*", "*Su Yönetimi*" ve "*Kritik Kamu Hizmetleri*" olarak tanımlanan kritik altyapı sektörlerinin korunmasına yönelik önemli faaliyetler gerçekleştirilmiştir. Kritik altyapıların ve siber uzaydaki tüm ulusal varlıkların siber tehditlere karşı etkin şekilde korunması ve siber olaylara müdahale kabiliyetlerinin daha da güçlendirilmesi hedeflenmektedir. Buna ilave olarak, sektörel ve ulusal ölçekte bir risk yönetimi anlayışıyla tehditlerin ve oluşturdukları olumsuz etkilerin en aza indirgenmesi amaçlanmaktadır.

II. ULUSAL KAPASİTENİN GELİŞTİRİLMESİ

a. *"İnsan Kaynağının Güçlendirilmesi":* Siber olaylara hazırlık seviyesinin geliştirilmesi amacıyla SOME'lerin olgunluk seviyelerinin ölçülerek mevcut durumun belirlenmesi ve gelişim ihtiyacı bulunan alanlara odaklanılarak yetkinliklerinin daha da üst düzeylere çıkarılması amaçlanmaktadır. Ayrıca sektörel, ulusal ve uluslararası seviyede düzenli olarak gerçekleştirilecek siber güvenlik tatbikatları ve eğitimler ile de yetkinliğin artırılması hedeflenmektedir.

b. *"Toplumsal Farkındalığın Artırılması ve Çocukların Çevrimiçi Korunması":* Bireysel, kurumsal ve ulusal ölçeklerde, yani tüm toplum genelinde, farkındalığı artırıcı çalışmaların gerçekleştirilmesi; aileler, çocuklar, öğrenciler, gençler, kadınlar, yaşlılar ve engellilere yönelik faaliyetlerle her kesime ulaşılması öncelikli hedefler arasında yer almaktadır. Çocukların siber ortamda korunmasına yönelik farkındalık kampanyaları ve ailelere düşen sorumluluklara ilişkin bilinç düzeyini artırıcı etkinlikler de bu kapsamda önem derecesi yüksek çalışmalar olacaktır.

III. ORGANİK SİBER GÜVENLİK AĞI

a. *"İleri Seviye Tehditlerle Mücadele":* Siber tehditlere karşı koymak için ileri seviye uzmanlık projelerinin geliştirilmesi, kalıcı tehditlerin analiz edilmesi ve uzun soluklu çalışmaların yapılması, ekiplerin olgunluklarının geliştirilmesine yatırım yapılacaktır.

b. *"Birlikte Daha Güçlüyüz":* USOM'un mevcut paydaşları ile olan bilgi alışverişinin ve etkileşiminin daha ileriye taşınması hedeflenmektedir. Karşılıklı destek ve geri bildirim mekanizmaları ile ulusal siber güvenliğe katkı sağlanması amaçlanmaktadır.

IV. YENİ NESİL TEKNOLOJİLERİN GÜVENLİĞİ

a. *"Güvenle Gelen Yeni Nesil Teknolojiler":* Yapay zekânın ve blok zincir teknolojilerinin siber güvenlik için kullanım alanlarının belirlenmesi ve geliştirilecek yerli ve milli teknolojiler ile katma değer oluşturması amaçlanmaktadır.

V. SİBER SUÇLARLA MÜCADELE

a. *"Güvenli Siber Ortam":* 2020-2023 döneminde de siber suçla mücadelenin daha güçlü şekilde sürdürülmesi için bu alandaki ulusal kapasitenin ve teknolojik imkânların artırılması amaçlanmaktadır.

b. *"Uluslararası Mücadele":* Siber suçun kaynağına ve suçluya en etkin biçimde ulaşılabilmesi için bilgi paylaşımı ve uluslararası iş birliğinin daha da geliştirilmesi hedeflenmektedir.

VI. YERLİ VE MİLLİ TEKNOLOJİLERİN GELİŞTİRİLMESİ VE DESTEKLENMESİ

a. *"Türkiye'nin Teknolojisi":* Siber güvenlik alanında öncü olmak hedefi ile yürütülen çalışmalar kapsamında özel sektörün gelişimi, büyümesi, ihracat kapasitesini artırarak ekonomiye katkı sağlaması ve teknolojiye yön veren bir konumda olması temel hedeftir.

b. *"Teknoloji Geliştirmede İş Birliği ve Destek Mekanizmaları":* Girişimciliğin, araştırma ve geliştirme çalışmalarının ve faaliyetine yeni başlayan firmalar (start-up) ile küçük ve orta büyüklükteki işletmeler başta olmak üzere özel sektörün desteklenmesi için mevcut mekanizmalardan faydalanmak ve yeni mekanizmalar ile bu desteğin artırılmasını sağlamak amaçlanmaktadır.

c. *Siber Güvenlik Test ve Sertifikasyon Sistemi":* 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 amaçlanmaktadır.

VII. SİBER GÜVENLİĞİN MİLLİ GÜVENLİĞE ENTEGRASYONU

a. *"Ulusal Güvenlik İçin Siber Güvenlik":* Üst düzey milli güvenlik politikalarımızda siber güvenliğe ilişkin hususların da azami derecede dikkate alınması, bu politikalarda kara, hava, deniz ve uzay güvenliğinin yanında siber savunmanın da yerini alması, ülkemizin diğer unsurlarla birlikte siber unsurları da içeren hibrit tehditlerden korunması ve caydırıcılığın artırılması amaçlanmaktadır.

VIII. ULUSLARARASI İŞ BİRLİĞİNİN GELİŞTİRİLMESİ

a. *"Sınıraşan Tehditlerle Mücadele":* Uluslararası siber güvenlik faaliyetlerine artan bir oranda katılım ve katkı sağlanarak Türkiye'nin bu alandaki söz sahibi konumunun daha da pekiştirilmesi ve dünyadaki iyi uygulama örneklerinin tespit edilerek ulusal siber güvenlik çalışmalarına sağlanan girdilerin artırılması amaçlanmaktadır.

Onuncu bölümde ise planının gerçekleştirme yaklaşımı ele alınmıştır. Ana başlığın alt başlıkları aşağıdaki gibidir (UDHB, 2020):

a. *Eylem Planı:* Kamu, özel sektör, akademi ve STK'lardan temsilcilerin geniş katılımıyla gerçekleştirilen hazırlık çalıştayında stratejik amaçlar kapsamında ulusal hedeflere ulaşabilmek için gerekli eylemler ve yürütülecek faaliyetler konusunda ilgili tarafların görüşleri alınmıştır. Gerçekleştirilmesi hedeflenen toplam 8 adet stratejik amaçla ilişkilendirilen 40 adet eylem ve 75 adet uygulama adımı Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023) kapsamında yer almaktadır.
b. *İzleme ve Ölçüm:* Eylemlerin her birinin tamamlanıp tamamlanmadığını ölçümlemek yapılan çalışmaların başarısının somut biçimde ortaya konması anlamına gelmektedir. Bu amaçla, eylemlerin içerdiği her bir uygulama adımına yönelik ölçüm kriterleri belirlenmiş olup Eylem Planı'nın gerçekleşme oranının bu kriterler üzerinden belirlenmesi planlanmıştır. Eylem Planı'nın izlenmesi ve ölçümü; belirlenen uygulama adımları, yürütülen faaliyetler ve ölçüm kriterleri temelinde periyodik olarak eylemlerden sorumlu ve ilgili kurum ve kuruluşlardan alınacak girdilerle sağlanacaktır.
c. *Paydaşlar:* Siber uzayda yer alan paydaşlar arasında Türkiye'den kamu kurum ve kuruluşları, kritik altyapılarda faaliyet gösterenler başta olmak üzere özel sektör kurum ve kuruluşları, üniversiteler, sivil toplum kuruluşları, araştırma toplulukları ve Türkiye'deki bireyler ile uluslararası paydaşlar bulunmaktadır. Tüm paydaşların doğrudan veya dolaylı katkılarıyla, belirlenen hedeflere ulaşılması amaçlanmaktadır.
d. *Kapsam:* Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023); kamu bilişim sistemlerini, kamu ve özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerini, küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dâhil olmak üzere siber uzayın ülkemiz ölçeğindeki tüm bileşenlerini kapsamaktadır.
e. *Güncelleme:* Türkiye'nin siber güvenlik alanındaki vizyon belgesi olma özelliği taşıyan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023); teknolojik gelişmeler, güncel koşullar, değişen ulusal ihtiyaçlar ve gereksinimler göz önünde bulundurularak ihtiyaç duyulması halinde güncellenecektir.

Stratejik Amaçlar-Eylem Maddeleri İlişkisi: Eylem maddelerinde yer alan faaliyetler sorumlu 14 farklı kamu kurumu ve iş birliği yapılacak 34 farklı kamu kurumunun çalışmalarıyla yürütülecektir. Bir önceki eylem planında olduğu gibi bu belgede de eylem planı açıklanmamış sadece stratejiler kamuoyuna duyurulmuştur. Genel olarak stratejilerin eylem planını yansıttığı söylenebilir.

4. AVRUPA BİRLİĞİ ÜLKELERİ VE İNGİLTERE'NİN SİBER GÜVENLİK STRATEJİLERİ VE EYLEM PLANLARI

AB'nin yapısı, kuruluşu ve ülkelerinin kısaca açıklanacağı bu bölümde daha sonra birliğin siber güvenlik stratejisi ve politikası ele alınacaktır. Son olarak AB ve İngiltere'nin (toplam 28 adet ülke) siber güvenlik politikaları, stratejisi ve eylem planı incelenecektir.

4.1. Avrupa Birliği'nin Kuruluşu ve Yapısı

Avrupa kıtasında ülkeler arası bir birlik oluşturma fikrinin düşüncesi oldukça eski tarihlere kadar götürülmektedir. Büyük Roma İmparatorluğu, Napolyon ve Hitler dönemlerinde kıtanın tekliği; etnik kohezyon, ideoloji ya da sert güç kullanma gibi farklı yollar kullanılarak sağlanmaya çalışmıştır. Derebeyliklerin yıkıldığı ve ulus devletlerin ortaya çıktığı 17. yüzyılın ortalarından itibaren filozoflar, siyasetçiler, hükümdarlar ve siyasi düşünürler de tek Avrupa hayalini kurmuşlardır (Dinan, 2014: 1).

Napolyon Savaşları, I. ve II. Dünya Savaşları, Kıta Avrupa'sında büyük yıkımlara yol açmış, maddi ve manevi kayıplara neden olmuş ve büyük insanlık trajedilerini doğurmuştur. Savaşların yeniden ortaya çıkmaması için liderler sürekli olarak arayış içinde olmuştur. II. Dünya Savaşından sonra benzer olayların yeniden yaşanmaması için birtakım girişimlerde bulunulmuştur. 1950'li yıllara gelindiğinde Almanya ile Fransa sınırları arasında yer alan zengin kömür yataklarının işletilmesi konusu Avrupa'da yeni bir tartışma ortaya çıkarmıştır. Bu sorunu çözmek ve ülkeler arasında kalıcı barışın sağlanması için yapılan görüşmeler sonunda, 1951 yılında Avrupa Kömür ve Çelik Topluluğunun (AKÇT) kurulmasına karar verilmiştir.

Avrupa Birliği projesinin hayata geçirilmesini sağlayan en önemli adım AKÇT'nin kurulması ve işletilmesidir. İkinci Dünya Savaşının ardından AKÇT'yi kuran Antlaşmanın imzalandığı 1951 yılına kadar Avrupa'da ortak hareket etmeye yönelik bir takım önemli gelişmeler yaşanmıştır. 19 Eylül 1946'da Winston Churcill, Zürih Üniversitesinde yaptığı konuşmada bir tür Avrupa Birleşik Devletleri kurulması çağrısı yapmıştır. Bunun peşinden Birleşik Avrupa Hareketi 1947'de hayata geçirilmiştir. Ayrıca aynı yıl Marshall Planı da açıklanmıştır. 1948 yılında Marshall Yardımlarının koordine edilmesi amacıyla Avrupa

Ekonomik İşbirliği Örgütü (AET) kurulmuştur. Gelecek yıl ise (1949) Kuzey Atlantik Antlaşması (North Atlantic Treaty Organization/ NATO) imzalanmıştır (Korkmaz, 2018: 3).

5 Mayıs 1950'de Fransa Dışişleri Bakanı Robert Schuman tarafından ilkeleri duyurulan topluluk 18 Nisan 1951 tarihinde Fransa, Batı Almanya, İtalya, Belçika, Hollanda ve Lüksemburg arasında Paris'te imzalanan antlaşma ile resmiyet kazanmıştır. AKÇT'nin oluşturulduğu Antlaşmada "*ortak bir pazarın kurulması, üye devletlerde ekonomik genişlemeye, istihdam ve yaşam standardının yükselmesine katkıda bulunmaktır*" cümlesine yer verilmiştir (AKÇTKA, 1951: 2.- 4. md).

Avrupa Atom Enerjisi Topluluğu ve Avrupa Ekonomik Topluluğu kurumları 25 Mart 1956 tarihinde imzalanan ve 1 Ocak 1957 tarihinde yürürlüğe giren Roma Antlaşması kapsamında hayata geçirilmiştir. Almanya, Fransa, İtalya, Belçika, Hollanda ve Lüksemburg arasında imzalanan Roma Antlaşmasıyla kurulan Avrupa Ekonomik Topluluğu ve Avrupa Atom Enerjisi Topluluğu (EURATOM) ile birlikte daha önce kurulan AKÇT de dahil olmak üzere topluluk sayısı üçe yükselmiştir (Bilici, 2005: 35).

1980'li yılların ortalarında (Roma Antlaşmasından neredeyse otuz yıl sonra) birlik deneyinin mimarları tarafından ortak pazarı tamamlamak için üç yüzü aşkın özel düzenlemeye ihtiyaç duyulduğu tespit edilmiştir. Malların, sermayenin, hizmetlerin ve insanların dolaşımını garanti altına almak için söz konusu düzenlemelere ihtiyaç duyulmuştur. Avrupa Toplulukları Komisyonu Başkanı Jacques Delors, yürütme organı olan Konseye, 1986'da Tek Avrupa Senedi'nin onaylamasının bir ihtiyaç olduğunu belirtmiştir. Konseyin onayıyla sonuçlanan süreç böylelikle birkaç yıl sonra imzalanacak olan Maastricht Antlaşması (1992) için bir anlamda açılan bir yol olmuştur (Roy, 2007: 4-5). Avrupa Tek Senedi, 17 Şubat 1986 yılında Almanya, Belçika, Fransa, Hollanda, İngiltere, İrlanda, İspanya, Lüksemburg, Portekiz, Danimarka, İtalya ve Yunanistan tarafından imzalanarak 1987 yılında yürürlüğe girmiştir. Avrupa Tek Senedi ile Avrupa Topluluklarını kuran Antlaşmalar da revize edilmiştir (Laursen, 2012: 77).

7 Şubat 1992'de imzalanan ve AET'nin AB olması yolundaki son adım olan ekonomik ve parasal birliği de gerçekleştirme istikametine girdiği antlaşma olan Maastricht Antlaşması ile Avrupa Ekonomik Topluluğunun adı Avrupa Topluluğu'na dönüşmüştür. Anlaşma ile sosyoekonomik ilerlemeyi hızlandıran ve güçlendiren 3 temel ilke benimsenmiştir. Bunlar

(a) rekabet ilkesine dayanan serbest piyasa ekonomisi, (b) kamu maliyesinin sağlıklı şekilde idaresi ve (c) yetki ikame etme ilkesidir (Karluk, 1996:82).

Şubat 2001'de, Fransa'nın Nice kentinde yapılan zirvede ve sonrasında imzalanıp 2003'te yürürlüğe giren Nice Antlaşması'nda da AB'de önemli değişiklikler yapılmıştır. AB liderleri, karar-alma konusunda yaşanan sorunları gidermek için pek çok alanda oy birliği ilkesinden oy çokluğu ilkesine geçmişlerdir. Ayrıca bu Zirve ile Avrupa Parlamentosu'nun sayısı 2004'te 10 devletin üye olacağı ve 2007'de ise Bulgaristan ve Romanya'nın üye olacağı göz önüne alınarak 626'dan 732'ye çıkarılmıştır. 2004 yılında 10 devlet –Polonya, Çek Cumhuriyet, Macaristan, Slovenya, Slovakya, Estonya, Letonya, Litvanya, Malta ve Kıbrıs- 2007 yılında ise Bulgaristan ve Romanya birliğe üye olmuş ve AB'nin üye sayısı 27'ye yükselmiştir. Daha sonra 2013 yılında Hırvatistan'ın üyeliği kabul edilmiştir. Son olarak 2020 yılında Birleşik Krallık AB'den ayrılmıştır. Böylece 2020 yılı sonu itibarıyla üye 28 ülke bulunmaktadır (Bilici, 2006, 39-45; AB, 2020).

Özetle, 1951 yılında Almanya, Fransa, İtalya, Belçika, Hollanda ve Lüksemburg'un yer aldığı altı üye ile kurulan Avrupa Birliği'nin hukuki temellerini, AKÇT Kuran Antlaşma (1951), Avrupa Ekonomik Topluluğu (AET) ve Avrupa Atom Enerjisi Topluluğunu (EURATOM) kuran Roma Antlaşması (1957), Avrupa Tek Senedi (1986) ve Avrupa Birliği'ni Kuran Antlaşma (Maastricht 1992) oluşturmaktadır.

4.2. Avrupa Birliği'nin Siber Güvenlik Stratejisi

AB genelinde siber güvenlik politikalarının yasal alanda tartışılması 1990'lı yıllarda başlamıştır. İlk olarak Avrupa Suç Sorunları Komitesi (CDPC) tarafından 1996 yılında siber suçlarla ilgilenecek bir *Uzmanlar Komitesi* kurulmasına karar verilmiştir. Kararın temel gerekçesini ise bilgi teknolojileri alanındaki hızlı gelişmelere koşut olarak siber uzay adı verilen yeni bir alanın ortaya çıkması/çıkmakta olması gösterilmiştir. 4 Şubat 1997 tarihinde toplanan Avrupa Konseyi Bakanlar Komitesi'nin 583 sayılı Kararı ile "*Siber Uzay Suçları Uzmanlar Komitesi (PC-CY)*" adı verilen yeni bir komite oluşturulmuştur. 1 Temmuz 2004 tarihinde yürürlüğe giren Avrupa Siber Suç Sözleşmesi, bu alandaki ilk uluslararası antlaşma olarak kabul edilmektedir (Önok, 2013: 1241).

Elektronik devlet uygulamalarının kullanım sıklığı ve içeriği ile internet ağlarının ve altyapılarının yaygın ve yeterli oluşu doğrudan bağlantılı konular olması nedeniyle internet, Avrupa Birliği tarafından Kritik Bilgi Altyapısı (CII) olarak tanımlanmıştır. Ayrıca Avrupa Birliği Komisyonu'nun Kritik Bilgi Altyapısı Koruma (CIIP) Eylem Planı çerçevesinde 2010 yılında Siber Avrupa 2010 (Cyber Europe 2010) programı uygulanmıştır. Kuşkusuz Avrupa Birliği ülkelerinde siber güvenlik tehditlerine karşı yapılan bu çalışmalar, Avrupa'nın Dijital Ajansı'nda öngörülen hedefler bağlamında Avrupa Ağ ve Bilgi Güvenliği Kurumu'nun (The European Union Agency for Cybersecurity/ ENISA) koordinasyonu ve Avrupa Komisyonu Ortak Araştırma Merkezi'nin (The Joint Research Centre/ ECJRC) katkılarıyla düzenlenmiştir (Karaarslan, 2013: 1-2).

AB açısından ENISA, siber güvenlik politikalarının kurumsallaşmasının başarılı bir örneğidir. Ajans 5 Haziran 2003 tarihinde bir tüzel kişilik olarak oluşturulmuştur. 14 Mart 2014 tarihinden itibaren fiilen faaliyetlerine başlayan ENISA'nın temel misyonu AB'nin siber güvenliğinin korunmasında Avrupa genelinde üst düzey ağ ve bilgi güvenliği sağlamaktır (Kutlu, Kahraman ve Dinçer, 2019: 6).

Avrupa Birliği'nin siber güvenlik politikasını oluşturan temel belge, 7 Şubat 2013 tarihinde "*Avrupa Birliği için Siber Güvenlik Stratejisi*" (Cyber security Strategy for the European Union) başlığı ile Avrupa Birliği Komisyonu tarafından yayınlanmıştır. Strateji belgesinde siber güvenliğe yönelik temel ilkeler sıralanmıştır. Bunlar arasında Avrupa Birliği ortak temel değerleri, hak ve özgürlükler, kişisel verilerin korunması, demokratik ve etkili çok paydaşlı yönetişim ile paylaşılmış sorumluluk ilkeleri yer almıştır (EC, 2013: 3-4).

Avrupa Birliği'nin Siber Güvenlik Strateji belgesinde, söz konusu stratejinin 2017 yılında revize edilmiş versiyonunda "Dir*enç, Caydırıcılık ve Savunma: AB için Güçlü Siber Güvenlik İnşa Etmek*" (Resillience, Deterrence and Defence:Building Strong Cybersecurity for the EU) ve 11 Mart 2019 tarihinde Avrupa Parlamentosu'nda onaylanan ve 27 Haziran 2019 tarihinde yürürlüğe giren "*Siber Güvenlik Yasası*" (Cyber Security Act) içinde siber güvenlik alanında önemli ilerlemelerdir (Eren, 2016: 34).

Siber güvenliğe yönelik ilk izlerin görülmeye başlandığı 1985'ten günümüze kadar AB, beş temel hedef çerçevesinde siber güvenlik politikasını geliştirmeye yönelmektedir. Söz konusu bu beş temel hedef ise ekonomik fayda/maksimizasyonun sağlanması, temel hakların

korunması, siber suçları/saldırıların önlenmesi, dijital sisteme yönelik güven unsurunun artırılması ve aktörler arasında iş birliğinin güçlendirilmesidir. Aşağıdaki alt bölümlerde ENISA sitesinde yer alan son AB ülkeleri ve İngiltere'nin siber güvenlik stratejileri ve eylem planları açıklanmıştır.

4.3. Almanya'nın Siber Güvenlik Stratejisi

Almanya'nın ulusal güvenlik anlayışı özellikle son 10 yılda dönüşüme uğramıştır. Bu dönüşümde, ülkenin dış politika anlayışındaki değişim etkili olmuştur. Ülke, özellikle Soğuk Savaşın sona ermesinden sonra bu son 10 yıla kadar daha durağan, kendi vatandaşlarının güvenliğini ve iç huzurunu sağlamaya yönelik bir güvenlik politikası uygulama anlayışına sahip olmuştur. Dünya siyaset arenasında liderliğe yönelen bir ülke olmamıştır (Kıratlı, 2016: 213). Son yıllarda ise Almanya, dış politikada uluslararası barışa katkıda bulunmak üzere daha müdahaleci ve dışa açık bir rol üstlenmiş (Şahin, 2017: 13) böylece kendi ulusal güvenliğine gelebilecek tehditleri (terör, siber terör vb.) de artırmıştır. Edindiği bu misyon ve dünya arenasında yer aldığı bu konum itibarı ile Almanya'nın ulusal güvenlik anlayışı şu 7 ilke etrafında özetlenebilecektir (WP, 2016: 24-25):

- ✓ Vatandaşların güvenliğini sağlayarak, ülkenin egemenliğinin ve toprak bütünlüğünün korunması.
- ✓ Müttefik ülkelerin vatandaşlarının güvenliğinin, toprak bütünlüğünün ve ulusal egemenliklerinin sağlanması.
- ✓ Kurallara dayalı olan ulusal düzeni, uluslararası hukuka uygun olarak korumak.
- ✓ Özgür ve engelsiz bir dünya ticaretinin yanında, güçlü bir Alman ekonomisi temelinde vatandaşların refahının sağlanması.
- ✓ Dünya genelindeki sınırlı kaynakların adil ve sorumlu şekilde kullanımını teşvik etmek.
- ✓ Avrupa Birliği entegrasyonunu derinleştirmek ve Transatlantik ortaklığını güçlendirmek.

Araştırmalar sonunda Almanya'nın siber güvenlik eylem planı tarzında iki adet belgeye ulaşılmıştır. İlki "*2011 Almanya Siber Güvenlik Strateji Belgesi*" ve diğeri ise "*2016 Almanya Siber Güvenlik Strateji Belgesi*"dir.

2011 Almanya Siber Güvenlik Strateji Belgesi, siber dünyanın, tüm bölgesel sınırların ötesinde, internet üzerinden erişilebilen tüm bilgi altyapılarını içerdiği, Almanya'da sosyal ve ekonomik yaşamın tüm oyuncuların siber alanın sağladığı olanakları kullandığı ve gittikçe birbirine bağlı bir dünyanın bir parçası olarak, devlet, kritik altyapılar, Almanya'daki işletmeler ve vatandaşlar, bilgi ve iletişim teknolojisinin (BİT) ve internetin güvenilir işleyişine bağlı olduğu saptamaları ile başlamaktadır. Ayrıca, BT ürünlerinin ve bileşenlerinin arızalanması, bilgi altyapısının bozulması veya ciddi siber saldırılar, teknolojinin, işletmelerin ve yönetimin performansı üzerinde ve dolayısıyla Almanya'nın sosyal yaşam çizgileri üzerinde önemli bir olumsuz etkiye sahip olabileceği vurgulanmıştır. Belgenin amacı ise, siber alandaki verilerin bütünlüğünü, özgünlüğünü ve gizliliğini korumanın 21. yüzyılın hayati soruları haline geldiğinden yola çıkılarak siber güvenliğin sağlanmasının hem ulusal hem de uluslararası düzeyde devlet, iş ve toplum için hayati olduğu vurgulanmıştır (Almanya, 2011).

BT tehdit değerlendirmesi bölümünde, son yıllarda bilgi altyapısına yönelik saldırıların daha da sık ve karmaşık hale gelirken, aynı zamanda faillerin daha profesyonel hale geldiği ve faillerin teröristler, casuslar siber faaliyetleri yapan kurumlar veya askeri operasyon yürüten devletler olduğu vurgulanmıştır. Bir diğer tehdit değerlemesi ise endüstriler için yapılmış olup ekonomik kaygılar tarafından motive edilen yeni güvenlik açıklarının ortaya çıktığı ifade edilmiştir (Almanya, 2011).

Siber güvenlik stratejisinin temel ilkeleri ise aşağıdaki gibi sıralanabilir (Almanya, 2011):

- ✓ Federal Hükümet, güvenli bir siber alana önemli bir katkı sağlamayı, böylece Almanya'da ekonomik ve sosyal refahı korumayı ve teşvik etmeyi amaçlamaktadır.
- ✓ Almanya'da siber güvenlik, birbirine bağlı bilgi altyapılarının gerektirdiği koruma ile orantılı olarak, fırsatlar ve siber alanın kullanımından kaçınmadan sağlanması amaçlanmaktadır.
- ✓ Siber Güvenlik Stratejisi temel olarak sivil yaklaşım ve önlemlere odaklanmayı amaçlamaktadır.
- ✓ Bilgi ve iletişim teknolojisinin küresel doğası göz önüne alındığında, uluslararası koordinasyon, dış politika ve güvenlik politikası konularına odaklanan yapılar vazgeçilmezdir. Almanya siber güvenlik alanda uluslararası işbirliğini artırmayı amaçlamaktadır.

- ✓ Uluslararası toplumun siber alanı koruma konusundaki tutarlılığını ve yeteneklerini sağlaması amaçlanmaktadır.

Belgede stratejik hedefler ve önlemler başlığı altında kritik altyapıların korumasına ilişkin uygulama planı ve federal yönetim için uygulama planı tarafından oluşturulan yapılar temelinde mevcut tehditlere yönelik önlemlerinin alınacağı ve özellikle on stratejik alana odaklanacağı ifade edilmiştir. Söz konusu stratejik alanlar aşağıda sunulmuştur (Almanya, 2011):

1. *Kritik bilgi altyapılarının korunması:* Kritik bilgi altyapılarının korunması siber güvenliğin temel önceliğidir. Neredeyse tüm kritik altyapılar merkezi bir bileşendir ve gittikçe önem kazanmaktadır. Kamu ve özel sektör, yoğunlaştırılmış bilgi paylaşımına dayanarak daha yakın koordinasyon için gelişmiş bir stratejik ve örgütsel temel oluşturmalıdır. BT krizleri sırasında kritik altyapıları işletmek ve bu amaçla kuralların uyumlaştırılması hedeflenmiştir. Kritik altyapılar, kamu yararı için büyük öneme sahip kuruluşlar veya kurumlar olarak tanımlanmıştır. Kritik altyapıların başarısızlığı veya zararı sürdürülebilir arz darboğazlarına, kamu güvenliğinin ciddi şekilde bozulmasına veya diğer çarpıcı sonuçlara neden olabilir. Belgede kritik altyapılar aşağıdaki gibi sıralanmıştır:
   a. Enerji
   b. BT ve telekomünikasyon
   c. Ulaştırma
   d. Sağlık
   e. Su
   f. Gıda
   g. Finans ve sigorta sektörü
   h. Devlet ve kamu yönetimi
   i. Medya ve kültür
2. *Almanya'da güvenli BT sistemlerinin kurulması:* Toplumdan bilgi ve tavsiyelere uyacağı tutarlı bir şekilde grup olarak çalışabilecek ortak girişimler oluşturulması hedeflenmiştir. Ayrıca, bilgi sağlayıcıların daha fazla sorumluluk almasının gerekip gerekmediğinin incelenmesi ve uygun güvenlik ürünleri ve hizmetlerinin temel bir koleksiyonunun kullanıcılar tarafından sağlanabildiğinin kontrol edilmesi planlanmıştır.

3. *Kamu yönetiminde BT güvenliğinin güçlendirilmesi:* Kamu yönetimi, BT sistemlerinin korunmasını daha da artırmayı hedeflemiştir. Devlet yetkilileri veri güvenliği için rol model olarak görev yapmak zorunda olduğu vurgulanarak elektronik ses ve veri iletişimi için federal yönetimde ("federal ağlar") ortak, tek tip ve güvenli bir ağ altyapısı oluşturulması hedeflenmiştir.
4. *Ulusal Siber Müdahale Merkezi'nin kurulması:* Almanya, tüm devlet otoriteleri arasında operasyonel işbirliğini optimize etmek ve BT olayları için koruma ve müdahale önlemlerinin koordinasyonunu iyileştirmek için bir Ulusal Siber Müdahale Merkezi kuracağını taahhüt etmiştir.
5. *Ulusal Siber Güvenlik Konseyi'nin kurulması:* Krizlere yönelik yapısal nedenlerin belirlenmesi ve ortadan kaldırılması siber güvenlik için önemli bir önleyici araç olarak kabul edilmektedir. Bu nedenle, Almanya içinde ve kamu ile özel sektör arasında, Bilgi Teknolojisi Federal Hükümet Komiserinin sorumluluğunda daha fazla görünür Ulusal Siber Güvenlik Konseyi kurmak üzere işbirliğini kurmak ve sürdürmek amaçlanmıştır.
6. *Siber uzayda da etkili suç kontrolünün sağlanması:* Kolluk kuvvetlerinin, Federal Bilgi Güvenliği Bürosunun ve siber suçlarla mücadelede özel sektörün, casusluk ve sabotaja karşı korunma konusundaki yeteneklerinin güçlendirilmesi gerekmektedir. Almanya, bu alandaki bilgi değişimini geliştirmek için, danışmanlık kapasitesine sahip olacak yetkili kanun uygulayıcı kurumların katılımıyla sanayi ile ortak kurumlar oluşturma amaçlamıştır.
7. *Avrupa'da ve dünya çapında siber güvenliğin sağlanması için koordineli bir eylem planı hazırlanması:* Küresel siber güvenliğin, yalnızca ulusal ve uluslararası düzeydeki koordineli araçlar aracılığıyla sağlanabileceğinden yola çıkarak Almanya AB düzeyinde, kritik bilgi altyapılarının korunması için eylem planına, Avrupa Ağ ve Bilgi Güvenliği Ajansı'nın (ENISA) görevlendirilmesinde bilişim ve iletişim teknolojileri ve Avrupa Birliği'nde değişen tehdit durumunu göz önüne alarak görev süresinin uzatılması ve orantılı bir şekilde genişletilmesini temel alan önlemleri desteklediğini ifade etmiştir.
8. *Güvenilir BT kullanımının yaygınlaştırılması:* Almanya, sosyal ve ekonomik yönleri hesaba katan geliştirilmiş güvenlik için yenilikçi koruma planlarının oluşturulmasını desteklenmektedir. Bu amaçla, BT güvenliği ve kritik altyapı koruması konusundaki araştırmalara devam edeceğini, temel stratejik BT yeterlilikleri alanındaki teknolojik

egemenliğini ve ekonomik kapasitesini güçlendireceğini ve kaynaklarını ortakları ve müttefikleri ile birleştireceğini vurgulamıştır.

9. *Federal makamlarda personel eğitiminin sağlanması:* Alman federal yetkilileri arasında yoğunlaşmış personel değişiminin ve uygun ileri eğitim önlemleri bakanlıklar arası işbirliğinin artırılması amaçlanmıştır.
10. *Siber saldırılara cevap verme araçlarının geliştirilmesi:* Devlet siber saldırılara tamamen hazırlıklı olmak isterse ve devlet yetkilileri ile işbirliği içinde çalışılmasına karar verilirse siber saldırılara yanıt verecek koordineli ve kapsamlı bir araç seti oluşturulması zorunludur. Almanya, tehdit durumunu düzenli olarak değerlendirmeye ve uygun koruma önlemlerini almaya devam edeceğini ve gerekirse, federal düzeyde veya bölge düzeyinde ek yasal güçlerin oluşturulacağını vurgulamıştır.

Sürdürülebilir uygulama başlığının altında ise siber alanı korumak için etkili önlemler almanın Almanya'nın uluslararası düzeyde başarısını doğrudan etkileyeceği vurgulanmıştır. Bu nedenle, belgede Alman Federal Hükümet'i, Siber Güvenlik Stratejisinin amaçlarına Ulusal Siber Güvenlik Konseyi'nin genel kontrolü altında ulaşılıp ulaşılmadığını düzenli olarak gözden geçireceğini, stratejilerini ve önlemlerini verilen şartlara ve çerçeve koşullarına uyarlayacağını ifade etmiştir (Almanya, 2011).

Siber ataklara oldukça fazla maruz kalan Almanya, saldırılara karşı almakta olduğu ve alacağı önlemleri Federal İçişleri Bakanlığı tarafından hazırlanan "Enformasyon Altyapı Savunması İçin Ulusal Plan" başlıklı belgede bir araya getirmiştir ve belirlenen bu ulusal plan "Enformasyon Üyeliğinden Sorumlu Federal Ofis" (BSI) (Bundesamt für Sicherheit in der Informationstechnik) tarafından yürütülmektedir. 13 Haziran 2005 tarihinde Federal Kabine tarafından kabul edilen ve siber ataklara karşı koyabilmek adına oluşturulan ulusal planın 3 stratejik hedefi bulunmaktadır. Bu hedefler şu şekilde sıralanmaktadır (TBMM, t.y.: 761):

- ✓ *Önleme:* Kullanılan teknolojilerin ve enformatik altyapının korunması adına gerekli tedbirlerin alınması.
- ✓ *Hazırlıklı Olma:* Gelebilecek saldırılara daha etkili cevap verebilmek adına ulusal planın yürütüldüğü birim tarafından Enformasyon Teknolojisi Kriz Müdahale

Merkezi'nin kurulması ve bu merkezin ulusal bir kontrol ve analiz birimi haline gelmesi.

- ✓ *Sürdürülebilirlik:* Devlet içerisinde alınan önlemlerin yeterli olmaması sebebiyle halkın ve özel sektörün de bilgilendirilmesi ve ülke genelinde siber güvenliğin önemine dair bir bilinç oluşturularak bireysel önlemlerin alınmasına halkın teşvik edilmesi.

Almanya Siber Güvenlik Strateji Belgesi ve Siber Güvenlik Yasası ile kritik altyapıları işleten kuruluşlara bir takım uyulması gereken BT güvenlik zorunlulukları getirmiştir. Bu zorunluluklar şu şekilde özetlenebilir (TBD, 2015: 26):

- ✓ Kritik altyapıların işlevselliği için gerekli olan BT sistemi bileşen ve süreçlerinin korunması için gereken tedbir ve önlemlerin iki yıl içerisinde uygulanması.
- ✓ Güvenlik denetimlerinin en az iki senede bir olmak üzere düzenli bir şekilde yapılması ve bu denetimler sonucu oluşturulacak raporların Bilgi Güvenliği Federal Ofisine iletilmesi.
- ✓ Kritik altyapılar üzerinde gözlenen güvenlik olaylarının Bilgi Güvenliği Federal Ofisine bildirilmesi.

İncelenecek bir diğer belge olan 2016 Almanya Siber Güvenlik Strateji Belgesidir. Belgede öncelikle siber tehdit durumu ele alınmıştır. Daha sonra siber güvenlik stratejisinin ilkeleri ve 4 eylem alanı belirlenmiştir. Son olarak ise siber güvenlikte süreklilik incelenmiştir.

Siber güvenlik stratejisinin eylemleri ve eylemlere bağlı olan ilkeleri şu şekilde belirlenmiştir (Almanya, 2016):

1. *Eylem 1:* Dijital ortamda güvenli ve kendinden kararlı bir eylem ile ilgili ilkeler;
   a. Tüm kullanıcılar arasında dijital yeterliliği teşvik etmek
   b. Dijital açıklıklarla mücadele etmek
   c. Güvenli elektronik iletişim ve güvenli web siteleri için standartlar oluşturma
   d. Güvenli elektronik kimlikler oluşturmak
   e. Sertifikasyonu ve onaylamayı güçlendirme (BT güvenliği için kalite güvence etiketinin hazırlanması ve sunulması)
   f. Dijitalleştirmeyi güvenli hale getirmek

g. BT güvenliği araştırma ve geliştirme faaliyetlerini yönlendirmek

2. *Eylem 2:* Devlet ve özel sektör ortaklığı ile ilgili ilkeler;
   a. Kritik Altyapıları korumak
   b. Almanya'daki şirketleri korumak
   c. Alman bilişim ekonomisini güçlendirmek
   d. Tedarikçilerle işbirliği yapmak
   e. BT'ye güvenlik servis sağlayıcılarını dahil etmek
   f. Bilgi alışverişini güvence altına almak için bir platform oluşturmak
3. *Eylem 3:* Devlet çapında güçlü ve sürdürülebilir bir siber güvenlik mimarisi ile ilgili ilkeler;
   a. Ulusal Siber Savunma Merkezi'ni daha fazla geliştirmek
   b. Yerel düzeyde analiz etme ve cevap verme yeteneklerini güçlendirmek
   c. Kolluk kuvvetlerini siber alanlara yoğunlaştırmak
   d. Siber casusluk ve siber sabotaj ile etkin bir şekilde mücadele etmek
   e. Yurtdışı kaynaklı siber saldırılara karşı erken uyarı sistemi geliştirmek
   f. Güvenlik Alanında Bilgi Teknolojileri Merkez Ofisi'nin kuruluşu
   g. Siber güvenliğin savunma yönlerini güçlendirmek
   h. Almanya'daki Bilgisayar Acil Müdahale Ekipleri (Computer Emergency Response Teams/ CERT) yapılarını güçlendirmek
   i. Federal işleri ve yönetimi güvence altına almak
   j. Federal hükümetler ile merkezi yönetim arasında işbirliğini geliştirmek
   k. Kaynakları kullanmayı geliştirmek, işe alım süreçlerini hızlandırmak ve personeli güçlendirmek
4. *Eylem 4:* Almanya ve Avrupa'nın uluslararası siber güvenlik politikasında aktif olarak yer almasına ilişkin ilkeler;
   a. Avrupa siber güvenlik politikasını şekillendirmek
   b. NATO'nun siber savunma politikasını geliştirmek
   c. Uluslararası mecrada siber güvenliğin şekillendirilmesine aktif olarak yardımcı olmak
   d. Siber yeteneklerin geliştirilmesinde ikili ve bölgesel destek ile işbirliğini sağlamlaştırmak (siber kapasite geliştirme)
   e. Uluslararası kolluk kuvvetlerinin güçlendirilmesi

Son bölümde Ulusal Siber Güvenlik Konseyi'nin eylem planını sürekli olarak kontrol etmesi gerektiği vurgulanmıştır. Eylem planında ileriye dönük bir siber güvenlik stratejisi, stratejik önlemleri tanımlamakla sınırlı kalmaması gerektiği ve aksine daha fazla stratejik önlemlerin geliştirilebileceği siber güvenlik konularında kalıcı bir strateji geliştirme sürecinin varlığına ihtiyaç duyulduğu saptanmıştır. Bunun sağlanması için yeni tehlikeler erken belirlenmeli ve yenilikçi çözümler araştırılıp geliştirilmelidir. Alandaki kilit bir rolü ise hükümet için stratejik bir danışman olarak kurulan Ulusal Siber Güvenlik Konseyi tarafından yürütülmesi öngörülmüştür. Konseyin görevi, uzun vadeli eylem ve eğilimlere olan ihtiyacı tespit etmek, belirlenen eylem alanlarında siber güvenliğin güçlendirilmesine yönelik itici güçleri ortaya koymak ve toplumdan, iş dünyasından ve üniversitelerden gelen uzmanların bilgisini kullanmak, her bir eylem için önerilerin tartışılmasını ve geliştirilmesini sağlamak olarak belirlenmiştir (Almanya, 2016).

Özetle eylem 1 ile mevcut teknik gelişmelere dayanarak, Ulusal Siber Güvenlik Konseyi'nin siber güvenlik alanındaki ulusal düzenlemelerin daha da geliştirilmesi için önerilerde bulunması; eylem 2 ile, siber güvenlik ve ilgili uygulama önerileri için devlet ve sanayi arasında işbirliği sağlaması; eylem 3 ile, federal siber güvenlik mimarisini oluşturması ve ülke içinde koordinasyonu sağlaması; eylem 4 ile, özellikle, ulusal siber güvenlik politikası için yeni itici güçler üretmek amacıyla, diğer kilit uluslararası ortaklıklar kurulması ve işbirliğinde bulunması hedeflenmiştir. Son olarak Konseyin stratejik konulardaki sonuçlar hakkında yazılı bir raporu düzenli olarak sunması ve hükümeti sürekli olarak bilgilendirmesi amaçlanmıştır.

4.4. Fransa'nın Ulusal Dijital Güvenlik Stratejisi

Fransa'nın siber güvenlik stratejisi 2015 yılında yayımlanmış olup "*Fransız Ulusal Dijital Güvenlik Stratejisi*" başlığını taşımaktadır. Belge giriş ve beş bölümden oluşmaktadır. Belgenin sunumunu ise 31 Mart 2014- 6 Aralık 2016 tarihleri arasında Fransız Başbakanı olan Manuel Valls kaleme almıştır. Valls, Fransa'nın tamamen dijital değişime kendini adadığını, dijital ekonomideki büyümenin sürekli artmasıyla birlikte Fransa'nın, Avrupa ve küresel ilgi dünyasında öncü olduğu, dijital dünyanın aynı zamanda rekabet için kullanıldığını ve siber saldırılar ile haksız rekabet ve casusluk, dezenformasyon ve propaganda, terörizm ve suçluluk kavramlarının yeni bir boyut kazandığını ifade etmiştir. Bunun yanı sıra Fransız hükümeti tarafından değerlerin, ekonominin ve vatandaşlarının

korunması, dijital güvenliği pekiştirerek Fransız şirketleri için sürdürülebilir bir büyüme ve fırsat kaynağı olan bir siber ortamın geliştirilmesi ve böylece demokratik değerleri ortaya koyarak vatandaşların dijital yaşamlarını ve kişisel verilerinin korunması amaçlanmıştır. Son olarak Valls tarafından ulusal dijital güvenlik stratejisiyle, özellikle eğitim ve uluslararası işbirliği konusunda kurulması gerektiği vurgulanmıştır (Fransa, 2015).

Belgenin sunuşundan hemen sonra aşağıdaki saptama tam sayfa olarak sunulmuştur (Fransa, 2015):

"*Fransız toplumunun dijitalleşmesi, dijital hizmetler, ürünler ve işlerde aralıksız büyüme ile hızlanmaktadır. Bu ulusal bir konu haline gelmiştir. Devlet dijital geçiş ve büyümeyi desteklemektedir, ancak ekonomik paydaşlar ve vatandaşlar için riskler taşıdığını da kabul etmektedir. Siber suç, casusluk, propaganda, sabotaj ve kişisel verilerin çalınması dijital güven ve güvenliği tehdit etmektedir. Bu nedenle beş stratejik hedefe dayanan kolektif, koordine bir eylem planı çağrısında bulunuyor.*" Stratejik hedefler aşağıda ana başlık olarak sunulmuş olup ayrıntılı açıklamalar devamında yapılmıştır (Fransa, 2015).

1. *Devlet temel ilgi alanları; bilgi sistemlerinin savunulması ve güvenliğinin sağlanması ile kritik altyapıların korunması, büyük siber güvenlik kriziyle mücadele etmektir:* Fransa, dünya standartlarında teknik uzmanlar tarafından desteklenen özerk stratejik planlamayı geliştirerek, siber uzayda temel çıkarlarını savunmaya devam etmeyi planlamaktadır. Buna paralel olarak, Fransa, ulusal ve uluslararası düzeylerde özel paydaşlarla işbirliğini genişleterek, kritik ağların güvenliğini ve büyük siber saldırılara karşı dayanıklılığını güçlendirmeye devam edeceğini taahhüt etmiştir.
2. *Dijital güvenliğin sağlanması, mahremiyetin korunması, kişisel verilerin güvence altına alınması ve siber zorbalığın engellenmesi amaçlanmaktadır:* Her boyuttaki işletme ve birey için siber alanın güvende kalması amacıyla koruyucu ve iyileştirici önlemler alınması planlanmıştır. Devlet, kamu otoritelerinin kişisel verilerin kontrollü kullanacağını, topluma uyarlanmış bir dizi dijital güvenlik ürününün geliştirilmesi konusunda titizlikle çalışacağını ve düzeltici faaliyetler, teknik ve yasal yardım sağlayan siber zorbalık mağdurlarına yardım edeceğini taahhüt etmiştir.
3. *Farkındalık yaratıcı faaliyetler geliştirilecek, siber güvenlik alanında başlangıç eğitimi verilecek ve diğer eğitimler sürekli kılınacaktır:* Rapor, bireylerin hala dijitalleşmeyle ilişkili riskler konusunda yeterli farkındalığa sahip olmadığı

gerçeğinden yola çıkarak okul ve öğrenci bilincinin artırılması için adımlar atmayı planlamıştır. Ayrıca, kamu ve özel sektörden siber güvenlik konusundaki artan talepleri karşılamak için, bu alandaki uzmanların eğitiminin artırılacağı ifade edilmiştir.

4. *İşletmeleri saran dijital teknoloji, sanayi politikası, ihracat ve uluslararasılaşma ana gündem maddeleri olacaktır:* Dijital pazarın dünya çapında büyümesi ve güvenlik gerekliliklerinin artması, kullanıcıların özelliklerine göre uyarlanmış güvenlik seviyelerine sahip Fransız dijital ürün ve hizmetlerini farklılaştırmak için bir fırsat oluşturduğu ifade edilmiştir. Devlet kamu alımları aracılığıyla, yatırımı, inovasyonı ve ihracatı destekleyerek dijital sektördeki Fransız şirketleri için güvenli ürünler ve hizmetler sunan uygun bir ortam geliştireceğini taahhüt etmiştir.
5. *Avrupa, dijital stratejik özerkliğine ve siber uzay dengesine sahip olacaktır:* Siber uzayda uluslararası ilişkilerin düzenlenmesi önemli bir konu haline gelmiştir. Fransa, aynı üye devletlerle birlikte, Avrupa dijital stratejik özerkliği için bir yol haritası oluşturacağını taahhüt etmiştir. Uluslararası kuruluşlardaki etkisini de güçlendirmeyi hedefleyen Fransa, siber güvenlik yeteneklerini geliştirmek isteyen veya siber alanın genel istikrarına katkıda bulunmayı amaçlayan ülkelere talep etmeleri durumunda destek sağlayacağını taahhüt etmiştir.

Strateji belgesinde dijital güvenliğin, dijital Fransa Cumhuriyeti projesinin temelini oluşturduğu ve bu stratejinin geliştirilmesinde dijital sektör uzmanlarının, kamu, özel karar vericilerin ve vatandaşların desteğinin önemli olduğu ifade edilmiştir (Fransa, 2015).

Raporda dijital teknolojiyle desteklenen geleceğin istikrarının üç paydaş topluluğunun ortak sorumluluklarına bağlı olduğu ifade edilmiştir. İlk topluluk, kullanımlara uyarlanan ve belirlenen riskleri hafifletebilecek güvenlik düzeyine sahip teknolojilerin, ürünlerin ve hizmetlerin önerilmesinden ve uygulanmasından sorumludur. Bu topluluktaki ana paydaşlar araştırmacılar, ürün ve hizmet geliştiricileri, siber güvenlik işletmeleri, elektronik iletişim ağı operatörleri, internet servis sağlayıcıları ve uzak veri işleme hizmeti sunucularıdır. İkinci topluluk, ulusun dijital korsanlardan korunmasından sorumludur. Siber güvenlik politikalarının uygulanmasının yanı sıra, gerekli teknik yeterlilikleri geliştirmek için agresif bir politika benimsenmeli ve vatandaşları, ulusal değerleri ve siber alandaki çıkarları koruyarak toplumun dijital dönüşümünü destekleyen bir güven ortamı oluşturulmalıdır. Bu sorumluluk, nitelikli güvenlik çözümlerinden yana durumunu ifade etmesini ve aynı

zamanda ihracat ile ilgili olarak ulusal sanayiyi teşvik etmesini zorunlu kılmaktadır. Bu toplulukta seçilen yetkililer, hükümet, merkez ve bölge yönetimleri ve sendikalardan oluşmaktadır. Üçüncü topluluk, mevcut hizmetleri ve teknolojileri iyi düşünülmüş bir şekilde kullanmaktan, rasyonel seçimler yapmaktan ve dijital yaşamla ilgili eylemlerde yüksek riskli davranışlardan kaçınmaktan sorumludur. Bu topluluktaki tüm kullanıcılar, şirketler yöneticileri, sivil toplum katılımcıları ve vatandaşlardan oluşmaktadır. Aşağıdaki bölümde her bir ana eylemin alt eylemleri ve temel amaçları sunulmuştur (Fransa, 2015):

1. *Devletin temel ilgi alanları; bilgi sistemlerinin savunulması ve güvenliğinin sağlanması ile kritik altyapıların korunması, büyük siber güvenlik kriziyle mücadele etmektir:* Fransa, siber uzayda ülkenin temel çıkarlarının savunmasını sağlamayı, kritik altyapılarının dijital güvenliğini pekiştireceğini ve temel operatörlerinin ekonomiye kazandırılmasını sağlamak için elinden geleni yapacağını taahhüt etmiştir. Alt eylemler ise aşağıdaki gibi belirlenmiştir:
   a. Ulusal bilgileri korumak, siber güvenliği güvence altına almak ve güvenilir bir dijital ekonomi geliştirmek için gereken bilimsel, teknik ve endüstriyel özelliklere sahip olmak.
   b. Devlet, işletmeler ve vatandaşlar için teknoloji ve ürün güvenliğinin etkin bir şekilde izlenmesini sağlamak.
   c. Devlet Bilgi Sistemleri Güvenliğinin güçlendirilmesi hızlandırmak.
   d. Fransa ve bağlı olduğu çok taraflı örgütleri büyük siber güvenlik krizleriyle karşı karşıya kaldığında korumaktır.
2. *Dijital güvenliğin sağlanması, mahremiyetin korunması, kişisel verilerin güvence altına alınması ve siber zorbalığın engellenmesi amaçlanmaktadır:* Fransa, ulusal değerleri doğrultusunda siber kullanım geliştirmeyi ve vatandaşların dijital yaşamlarını korumayı taahhüt etmiştir. Alt eylemler ise aşağıdaki gibi belirlenmiştir:
   a. Siber suçlarla casusluk ve siber zorbalık mağdurlarına yardımı artıracaktır.
   b. Fransa, ulusal değerlerini elektronik iletişim ağlarında ve uluslararası davalarda savunacaktır.
   c. Siber zorbalık eylemlerin mağdurlarına yerel yardım sağlanacaktır.
   d. Siber suçun zararı ve gücü ölçülecektir.
   e. Fransız halkının dijital kimliği, gizliliği ve kişisel verileri korunacaktır.
   f. Dijital yaşamı koruma amacıyla işletmelere siber güvenlikle ilgili teknik çözümler önerilecektir.

g. Yasal uluslararası karşılıklı yardım mekanizmalarının güçlendirilmesi ve Budapeşte Siber Suçlar Sözleşmesinin ilkelerinin yaygınlaştırılması amaçlanmıştır.

3. *Farkındalık yaratıcı faaliyetler geliştirilecek, siber güvenlik alanında başlangıç eğitimi verilecek ve diğer eğitimleri sürekli kılınacaktır:* Fransa, çocukların dijital güvenlik konusundaki farkındalığını ve okul çağından itibaren bilinçli siber davranışları artıracağını ve yükseköğretim ile sürekli eğitim alanlarında söz konusu sektöre uyarlanmış dijital güvenliğe adanmış bir bölüm içereceği taahhüt etmiştir. Alt eylemler ise aşağıdaki gibi belirlenmiştir:
   a. Tüm Fransız halkının bilincini artırmak.
   b. Siber güvenlik bilincini tüm yüksek ve devam eden eğitim programlarına dahil etmek.
   c. Siber güvenlik eğitimini, bazı BT'yi içeren tüm yüksek eğitime entegre etmek.
   d. Başlangıç ve devam eden eğitim ihtiyaçlarının kaydedilmesi ve öngörülmesini sağlamak.
4. *İşletmeleri saran dijital teknoloji, sanayi politikası, ihracat ve uluslararasılaşma ana gündem maddeleri olacaktır:* Fransa, araştırma ve inovasyon için elverişli bir ortam geliştirmeyi, dijital güvenliği rekabetçiliğin bir faktörü haline getirmeyi ekonominin gelişmesini, dijital ürün ve hizmetlerin uluslararası tanıtımını desteklemeyi, dijital ürün ve hizmetlerin ergonomi, kullanımlara uyarlanmasını siber tehditlerin vatandaşlarına, işletmelerine ve idarelerine ulaşmasını engellemeyi taahhüt etmiştir. Alt eylemler ise aşağıdaki gibi belirlenmiştir:
   a. Siber güvenlik alanında ulusal ve Avrupa güvenlik ürünleri ve hizmetlerini geliştirmek ve uygulamak.
   b. Edinilen bilgileri, siber güvenliğinin artırılmasına katkıda bulunmak için özel sektöre aktarmak.
   c. Kullanımlara, uyarlanmış desteği ve paydaşların bilgisini daha iyi tahmin ederek daha güvenli bir dijital dünya hazırlamak.
   d. Kamu ihalelerinde ve desteğinde siber güvenlik gerekliliklerinin bütünleştirilmesini sağlamak.
   e. Sektördeki işletmelerin ihracatını ve uluslararasılaşmasını desteklemek.
5. *Avrupa, dijital stratejik özerkliğine ve siber uzay dengesine sahip olacaktır:* Fransa, çocukların dijital güvenlik konusundaki farkındalığını ve okul çağından itibaren sorumlu siber davranışları artıracaktır. İlk olarak dijital güvenliğe ayrılmış bir bölüm, yükseköğretim ve sürekli eğitimde yer alacaktır.

a. Gönüllü üye devletlerle Avrupa stratejisi için özerk bir yol haritası oluşturulması.
b. Siber güvenlik ile ilgili uluslararası alanda Fransa'nın varlığını ve etkisini güçlendirmek.
c. Siber uzayın küresel istikrarına katkıda bulunarak gönüllü ülkelere siber güvenlik yetenekleri oluşturmalarında yardımcı olmak.

Fransa'nın eylem planındaki amaçları; ulusal siber acil durum planları geliştirmek, siber güvenlik alıştırmaları düzenlemek, temel güvenlik gereksinimlerini belirlemek, olay raporlama mekanizmaları kurmak, vatandaş farkındalığını artırmak, eğitim ve öğretim programlarını güçlendirmek, siber olay müdahale kabiliyeti geliştirmek, siber suçları tanımlamak, uluslararası işbirliğine girmek, Ar-Ge yatırımlarını artırmak, kritik bilgi altyapısını korunmak, kamu kurumları arasında işbirliğini oluşturmak, güvenliği ve gizliliği dengelemek başlıkları ile özetlemek mümkündür.

4.5. Belçika'nın Siber Güvenlik Stratejisi

Belçika siber güvenlik stratejisinde kendini bir bilgi toplumu olarak tanımlamaktadır. Teknolojik gelişmenin hızlılığı nedeniyle ülkenin daha savunmasız hale geldiği ifade edilmiştir. Siber uzaydaki ekonomik ve siyasi casusluk, ülkenin ekonomik ve bilimsel potansiyelini tehlikeye atmaktadır. Ulusal siber güvenlik stratejisiyle Belçika'nın siber güvenliğini garanti altına almak için üç stratejik hedefi vardır (Belçika, 2012):

- Modern bir toplumun temel haklarına ve değerlerine saygı duyan güvenli ve güvenilir bir siber uzay oluşturmak,
- Kamusal sistemlerin ve kritik altyapıların siber tehditlerine karşı optimum koruma sağlamak,
- Özerk bir güvenlik politikası ve uyarlanmış bir güvenlik tepkisi için kendi siber güvenlik kapasitelerini geliştirmek.

Ülke siber güvenlik yaklaşımını merkezileştirilmeyi ve merkezi bir yapı tarafından entegrasyonunun sağlanması hedeflemektedir. Bu nedenle, çeşitli ulusal kamu, özel ve akademik ortaklar arasında açık anlaşmalara ve bunların yanında önemli bir taahhüde ihtiyaç duymaktadır. Gerekli eğitim ve bilgilendirme kampanyaları sayesinde, siber güvenlikle ilgili siber uzaydaki çeşitli oyuncuların uzmanlığı ve bilgisinin iyileştirilmesi amaçlanmıştır. Bu

amaçtan yola çıkılarak siber uzaya güvenli erişim sağlamak için teknolojik gelişme teşvik edilmelidir (Belçika, 2012).

Tüm ulaşım, havacılık, sağlık vb. alanlardaki sistemlerin entegrasyonu ve kullanılabilirliği, iyi seviyede çalışması esastır. Nitekim enerji arzı, ulaşım, finans sektörü, sağlık hizmetleri ve kamu hizmetleri gibi sektörler hayati işleyişin temelini oluşturmaktadır. Bu bölgelerdeki bilgi teknolojileri altyapısı kazara bozulursa veya hizmet dışı bırakılırsa, hasar çok ciddi hatta ölümcül olabilmektedir (Belçika, 2012).

Eylem planında üç adet kritik tespitte bulunulmuştur. İlk olarak ülke toplumu ve ekonomisi bilgi ve iletişim araçlarına bağlımlıdır. Bu bağımlılık artmaktadır, çünkü çoğu zaman ekonomik süreçlerin siber uzay dışında hiçbir çözümü yoktur. Diğer taraftan ülkenin savunmasız olduğu ifade edilmiştir. Belçika'nın savunmasızlığını belirleyen faktörler (Belçika, 2012);

- Tüm önemli bilgi ve iletişim sistemlerinin geniş bant internete erişilebilirliği,
- Kuruluşlar, bilgi sistemleri için genellikle standart ticari teknolojiyi kullanmaktadır. Bu teknolojiler sürekli olarak incelenmekte ve yeni güvenlik açıkları ile yayınlanmaktadır.
- "Bulut" veri merkezlerindeki çeşitli şirketlerin ve kuruluşların veri ve uygulamalarının yoğunluğu, bu merkezlerin ve ağların siber saldırıya karşı zafiyetini oluşturur.
- Büyük kişisel veri bankaları, vatandaşların mahremiyetini de tehdit etmektedir.
- Genellikle şirketler, altyapılarını etkileyen siber olaylara yeterli müdahaleyi gösterememektedir.
- Son olarak, devlet güvenliğinin korunmasına yönelik uluslararası ittifaklar siber uzayda mutlaka geçerli veya uygulanabilir olmamaktadır.

Son tespit ise siber tehdidin gerçek olmasıdır. Suçluların niyetleri siber alanda da değişmemektedir. İnternetin sınırlı araçlarla evrimi sabotajı, casusluğu, yıkımı, terörizmi, komuta ve yönetimi, propagandayı ve siber operasyonları kolaylaştırmaktadır (Belçika, 2012).

Bu tespitlerden sonra üç adet stratejik hedef belirlenmiştir. Aşağıda hedefler özetlenmiştir (Belçika, 2012):

a. *Belçika, modern toplumun temel haklarına ve değerlerine saygı duyan güvenli ve güvenilir bir siber uzay hedefleyecektir:* Güvenli ve güvenilir bir siber alan, veri ve kayıt ve/veya işleme sistemlerinin kullanılabilirliği, bütünlüğü, gizliliği ve reddedilmemesi dahil olmak üzere bilgi güvenliğinin temel ilkelerini garanti edecektir.
b. *Belçika, kritik kamu altyapılarının ve sistemlerinin siber tehditlere karşı en iyi şekilde korunmasını ve güvenliğini hedefleyecektir:* Kritik altyapılar, topluma, faaliyetlerindeki herhangi bir kesinti veya aksaklıktan mümkün olduğunca kaçınılması gereken temel mal veya hizmetleri sağlayacaktır. Yetkili makamların bilgi ve iletişim sistemleri de yeterince korunmalı ve kontrol edilmelidir.
c. *Belçika, kendi siber güvenlik kapasitesi geliştirmeyi amaçlıyor:* Belçika, kendi siber güvenlik kapasitesi sayesinde, tamamen özerk olarak bir güvenlik politikası yürütebilecek ve olaylara tepki gösterebilecektir. Ayrıca, Belçika, uluslararası düzeyde önemli işbirlikleri kurabilmek için kendi siber güvenlik kapasitelerini yeterince genişletmeyi hedefliyor.

Ülke yukarıdaki üç stratejik hedefe ulaşmak için, bir dizi somut eylem belirlemiştir. Söz konusu eylemler özet olarak aşağıda sunulmuştur (Belçika, 2012):

- *Siber güvenlik merkezi kurulması ve entegre yaklaşım benimsenmesi:* Siber uzayda güvenlik için çalışmak çok iyi bir ulusal ve uluslararası işbirliği gerektirmektedir.
- *Yasal bir çerçevenin oluşturulması:* Siber güvenlik için ulusal bir stratejinin geliştirilmesi, vatandaşın hakları ve özgürlükleri ile yetkilinin gerekli müdahaleleri arasında bir denge sağlayan şeffaf bir yasal çerçeveye dayanmalıdır.
- *Devam eden siber tehditleri izleme:* Hem temel değerlere ve devlet çıkarlarına yönelik genel siber tehdit, hem de temel ve hayati sistemlere yönelik belirli siber tehditler sürekli olarak izlenmeli ve analiz edilmelidir.
- *Bilgisayar sistemlerinin bozulmasına veya ihlaline karşı gelişmiş koruma sağlanması:* Bilgi ve iletişim teknoloji sistemlerinin korumasını iyileştirmek için, çeşitli sistem türleri için kılavuzlar ve standart güvenlik dokümanları oluşturulacaktır.
- *Siber olaylara karşı savunma kapasitesinin güçlendirilmesi:* Ciddi siber olaylara daha etkili savunma yapabilmek için, çeşitli kamu hizmetlerinde ilk etapta siber güvenlik açısından mevcut kapasitelerin bir envanteri yapılacaktır.

- *Siber suçlara özel yaklaşım geliştirilmesi:* Güvenlik önlemleri bir olayın meydana gelmesini engelleyemezse, öncelikle olayların bir araç tarafından tespit edilmesi ve uygun ve yetkin ortaklara bildirilmesi önemlidir.
- *Siber güvenlikte uzmanlık ve bilginin genişlemesine katkı sunulması:* Çeşitli aktör kategorilerine uyarlanmış bilgi profilleri oluşturmak ve temel eğitimden çeşitli üniversite çalışmalarına kadar, iktidar örgütleyicileriyle birlikte gerekli eğitime mümkün olduğunca çok para harcamak gerekmektedir.
- *Teknolojik gelişimin teşvik edilmesi:* Tüm ekonomik sektörlerde pazar, yalnızca verimli değil, aynı zamanda güvenilir, yani kalitesi ve güvenliği kuruluşlar tarafından onaylanmış ürün ve hizmetler talep etmektedir.

Belçika kritik altyapıların korunmasına özel bir önem vermiştir. Ülke siber olayları önleme ve güvenlik alanında, kritik altyapıların güvenliği ve korunmasına ilişkin 1 Temmuz 2011 tarihli kanun ile Avrupa kritik altyapılarının belirlenmesi ve korunmasına yönelik 8 Aralık 2008 tarihli ve 2008/114/CE sayılı Direktife kısmen uymaktadır.

4.6. İtalya'nın Siber Güvenlik Eylem Planı

İtalya Siber Güvenlik Eylem Planı Mart 2017 yayımlanmıştır. 14 bölümden oluşan eylem planında 11 ana hedef belirlenmiştir. İtalya Siber Güvenlik Eylem Planı, ulusal siber güvenlikten sorumlu siyasi otorite olarak İtalya Başbakanı tarafından onaylanmıştır. 2017 İtalya Siber Güvenlik Eylem Planı, Siber Uzay Güvenliği için Ulusal Stratejik Çerçeve tarafından belirlenen yönergeleri karşılamak için gereken eylemleri ana hatlarıyla belirtmeyi amaçlamaktadır. Eylem planındaki stratejik kurallar aşağıdaki gibidir (İtalya, 2017):

1. Ulusal kritik altyapıların ve diğer stratejik oyuncuların savunma yeteneklerinin güçlendirilmesi.
2. Siber aktörlerin teknolojik, operasyonel ve analitik yeteneklerinin geliştirilmesi.
3. Kamu-özel sektör işbirliğinin teşvik edilmesi.
4. Siber güvenlik kültürünün teşvik edilmesi.
5. Siber güvenlik konusunda uluslararası işbirliğinin desteklenmesi.

6. Çevrimiçi suç faaliyetlerine karşı eylem yeteneklerinin güçlendirilmesi.

Ulusal siber güvenlik çerçevesinin hızlı bir şekilde iyileştirilmesini kolaylaştırmak için, öncelikli olarak izlenecek bir dizi temel görev belirlenmiştir. Görevler, önceki stratejinin gözden geçirilmesiyle ve hem ulusal hem de uluslararası düzeyde meydana gelen gelişmeler dikkate alınarak seçilmiştir. Söz konusu temel görevler aşağıdaki gibidir (İtalya, 2017):

- Ulusal Siber Güvenlik Yönetim Kurulunun yönetişim ve sorumlulukları gözden geçirilecek.
- Siber kriz yönetimi için karar verme prosedürü basitleştirilecek.
- Kuruluşların toplulaştırılması/birleşmesi yoluyla ulusal siber güvenlik çerçevesi içindeki karmaşıklık azaltılacak.
- CERT'lerin aşamalı birleşmesi sağlanacak.
- Ulusal bir siber güvenlik değerlendirme ve sertifika merkezi oluşturulacak.
- Bir risk sermayesi fonu veya vakfı oluşturulacak.
- Ulusal siber güvenlik Ar-Ge Merkezi oluşturulacak.
- Ulusal kriptografi merkezi oluşturulacak.

Eylem planının ana ve alt hedefleri aşağıdaki gibi belirlenmiştir (İtalya, 2017):

1. <u>EYLEM MADDESİ: İSTİHBARAT, KANUN UYGULAMASI VE SAVUNMA YETENEKLERİNİ GÜÇLENDİRMEK</u>

1.1. Tehdit ve güvenlik açığı analizi

a. Siber tehditler ve güvenlik açıkları düzenli olarak değerlendirilecek.
b. Potansiyel güvenlik açıklarını tahmin etmek için stratejik alanlarda teknolojik yenilikler izlenecek.
c. Özel kurumsal platformlar aracılığıyla temel hizmetler ve kritik altyapı operatörleri geliştirilecek.
d. Güvenlik açıklarını ve tehditleri tespit etmeyi/analiz etmeyi amaçlayan yeni metodolojiler ve teknolojiler geliştirmek için üniversiteler ve araştırma merkezleri ile işbirliği yapılacak.

1.2.Siber istihbarat ve siber bilgi yönetimi

a. Siber tehditlerle ilgili toplama, analiz ve yayma yetenekleri geliştirilecek.
b. Trafik izleme ve analiz yeteneklerinin geliştirilmesi yoluyla tehdit algılama kapasitesi iyileştirilecek.
c. Erken uyarı prosedürleri uygulanacak.

d. Akıllı entegrasyon yetenekleri geliştirilecek.

1.3.Siber tehditlerle mücadele

a. İlişkilendirme yetenekleri geliştirilecek.
b. Durum bilgisi, tehdit önleme ve karşı önlemleri iyileştirmek için siber faaliyetlerin doğru değerlendirmeleriyle tutarlı bir siber durumsal farkındalık geliştirilecek.
c. Kamu yetkilileri ve özel sektör arasında bilgi paylaşımı kolaylaştırılacak.
d. İlgili siber olaylarda merkezi idareleri, temel hizmet operatörlerini ve kritik altyapıları derhal desteklemek üzere teknik müdahale ekipleri oluşturulacak.

1.4.Siber savunma operasyonel yetenekler

a. Siber uzayda savunma yapıları güçlendirilecek ve varlıklarının uzun vadeli verimliliği ve etkinliği güvence altına alınacak.
b. Etkili siber askeri operasyon planlaması ve uygulaması yapabilen komuta ve kontrol yapıları oluşturulacak

1.5.Siber olay yönetimi: öğrenilen dersler

a. Kamu ve özel kuruluşlar arasında bilinmesi/paylaşılması gereken bir temelde, öğrenilen dersleri işlenecek ve siber olaylar incelenecek.

2. EYLEM MADDESİ: KAMU-ÖZEL İŞBİRLİĞİNİN GÜÇLENDİRİLMESİ

2.1.Entegrasyon

a. Tehditleri tespit etmek, güvenlik açıklarını azaltmak ve siber saldırılara müdahaleyi koordine etmek için kamu-özel mevcut işbirliği planlarının işlerliği kolaylaştırılacak.
b. Kurumsal forumlar, teknik gruplar, kritik altyapılar ve temel hizmet operatörlerinin yanı sıra diğer stratejik oyuncuların da dahil olduğu yetkili organlar tarafından uygulanan destek faaliyetleri yürütülecek.

2.2.Kamu-özel sektör işbirliği araçları

a. Bilgi ve iletişim teknolojileri kritik sistemlerini tanımlamak için bir metodoloji oluşturulacak.
b. Ayrıca ortak bir taksonomiyi benimseyerek bilgi paylaşımı güçlendirilecek.
c. Siber krizleri etkili bir şekilde yönetmek için kritik altyapıların yetkili otoriteleri, bakanlıkları, özel kuruluşları ve ortak milletler arasında sinerji geliştirilecek.
d. Altyapıların güvenlik açığı değerlendirmeleri için özel değerlendirme standartları belirlenecek ve iletişim formatları geliştirilecek.

2.3.Özel aktörlerin ulusal ve uluslararası siber güvenlik etkinliklerine dahil olması

a. Tüm toplum yaklaşımını izleyerek mevcut kamu-özel iletişimi birleştirilecek.

b. Özel operatörlerin kritik altyapıların korunmasına ilişkin uluslararası tatbikatlara katılımı kolaylaştırılacak.

3. EYLEM ÖĞESİ: BİLGİ TEKNOLOJİLERİ GÜVENLİĞİ KÜLTÜRÜNÜ GELİŞTİRMEK İÇİN EĞİTİM VE ÖĞRETİM

3.1.Doktrin geliştirme

a. En son uluslararası stratejik gelişmeler takip edilecek. En iyi uygulamalara dayalı siber güvenlik doktrinleri geliştirilecek.

3.2.Siber güvenlik bilinci

a. Vatandaşlar, öğrenciler, şirketler ve kamu idareleri için farkındalık girişimleri düzenlenecek.

3.3.Eğitim, öğretim ve tatbikatlar

a. AB, NATO ve diğer uluslararası kuruluşların siber güvenlik girişimlerine katılım sağlanacak.
b. Karar vericiler arasında siber güvenlik tehditlerinin en son gelişmeleri hakkında farkındalık yaratılacak.
c. Siber güvenlik operatörleri ve yöneticilerinin yanı sıra bilgi teknolojileri sistemleri ve ağ görevlileri için eğitim uygulamaları düzenlenecek.
d. Simülasyon araçları, ortak uygulamalar ve iş başında eğitimler aracılığıyla siber uzay operasyonel faaliyetleri geliştirilecek.
e. Siber eğitim kapasiteleri, eğitimde mükemmellik merkezlerinde yoğunlaştırılarak, mevcut merkezler birleştirilecek, özel kuruluşların AB ve NATO üyelerinin ve diğer ortak ülkelerin doğrudan katılımı kolaylaştırılacak.
f. Kamu yönetimi ve özel şirketlerin personeline yönelik eğitimler ve özel kurslar düzenlemek için üniversiteler ve araştırma merkezleriyle ortaklıklar geliştirilecek.
g. Ulusal siber güvenlik mükemmellik merkezlerinin haritası çıkarılacak.

4. EYLEM MADDESİ: ULUSLARARASI İŞBİRLİĞİ VE SİBER TATBİKATLARI

4.1.İkili ve çok taraflı işbirliğini geliştirmek

a. AB ve NATO üyeleri ve diğer ortak ülkelerle ilişkiler güçlendirilecek.
b. Savunma Bakanlığı, diğer bakanlıklar arası, NATO, AB ve çok uluslu düzeydeki ortak faaliyetler yoluyla siber güvenlik operasyonlarının planlama ve uygulanmasının entegrasyonu sağlanacak.
c. En son gelişmelere ulusal düzeyde uyum sağlamak için uluslararası forumlara katılım sağlanacak.

4.2.Siber uygulamalar

a. Kritik altyapılar ve temel hizmet operatörlerinin yanı sıra diğer stratejik oyuncularının da dahil olduğu yinelenen ulusal siber tatbikatlar düzenlenecek.
b. Hem çok taraflı (AB ve NATO) hem de ikili düzeyde (örneğin Amerika Birleşik Devletleri ile) tatbikatlara katılım sağlanacak.

4.3.AB projeleri ve diğer uluslararası kuruluşların girişimleri

a. Kamu ve özel operatörler arasında AB finansman girişimlerine erişim teşvik edilecek.
b. AB finansmanına erişim en üst düzeye çıkarılacak.
c. AB tarafından finanse edilen projelere katılım sağlanacak.
d. NATO ve diğer uluslararası kuruluşların projelerine katılım sağlanacak.

5. EYLEM MADDE: OLAYIN ÖNLENMESİ, MÜDAHALE VE TAZMİNAT

5.1.Entegrasyon kapasitesi

a. Tek bir haberleşme noktası ve tam olay müdahale özelliklerine sahip bir veya daha fazla birim oluşturulacak.
b. Bir veya daha fazla siber güvenlik birimi oluşturulacak.
c. Teknik müdahale ekipleri için yasal çerçeve tam olarak uygulanacak.
d. Mevcut ulusal siber güvenlik işbirliği mekanizmaları belirlenecek.
e. Bilgi teknolojilerinin siber olaylardan etkilenmesi en aza indirilecek.
f. Bilgi teknolojileri güvenliği için proaktif bir yaklaşım geliştirilecek.
g. İş sürekliliğini ve olağanüstü durumdan kurtarmayı sağlamak için dayanıklı bir yaklaşım geliştirilecek.

5.2.CERT'lerin geliştirilmesi

a. Eylem planı direktifi iç hukuk kararnamesine göre geliştirilecek.
b. KOBİ'ler de dahil olmak üzere tüzel kişilere yönelik etkinliği artırılacak.
c. Yerel kamu idarelerini desteklemek için verimli yaklaşımlar geliştirilecek.
d. AB ve uluslararası teknolojik projelerine aktif olarak katılım sağlanacak.

5.3.Tedarik

a. Siber güvenliği garanti etmek için kamu idarelerinin satın alma mekanizmaları tanımlanacak.
b. Güvenli bir kamu yönetimi tedarik zinciri için satın alma düzenlemeleri ve prosedürleri belirlenecek.

6. EYLEM MADDESİ: SİBER GÜVENLİK MEVZUATININ GÜNCELLENMESİ VE ULUSLARARASI DÜZEYDE UYUMUN YÖNETİLMESİ

6.1.Mevzuat güncellemesi

a. Kamu idarelerinin en iyi uygulamaları paylaşılacak ve hukuki siber güvenlik yetenekleri koordine edilecek.
b. Siber güvenlikle ilgili mevcut mevzuat değerlendirilecek.
c. Eylem planı kapsamındaki sektörler dikkate alınarak kritik altyapıların ulusal mevzuatı tamamlanacak.
d. Siber güvenlik politikalarının etkinliğini en üst düzeye çıkarmak amacıyla kamu ve özel operatörler için ulusal yükümlülükler uyumlu hale getirilecek ve olay bildirim süreçleri basitleştirilecek.
e. Yasal yükümlülükleri uyumlu hale getirmek ve süreçleri basitleştirmek için AB düzeyinde girişimler teşvik edilecek.

6.2.Ulusal yasal çerçeve

a. AB mevzuatı ve uluslararası hukuka uygun olarak siber operasyonlarla ilgili faaliyetler de dahil olmak üzere siber güvenlikle ilgili yasal çerçeve güncellenecek.
b. Siber tehditleri tespit etmeyi ve bunlarla mücadele etmeyi amaçlayan araçların dağıtımı için yasal hükümler oluşturulacak.

6.3.Atıf ve yaptırımlar

a. Ağ yöneticileri ve kullanıcıları tarafından güvenlik ihlallerinin (ve ilgili yaptırımların) ilişkilendirilmesi için yasal bir çerçeve ve metodoloji oluşturulacak.

6.4.Birlik genelindeki ağlar ve bilgi sistemleri için yüksek düzeyde ortak güvenlik önlemlerine ilişkin 6 Temmuz 2016 tarihli ve 2016/1148 sayılı Avrupa Parlamentosu ve Konseyi'nin Direktifi

a. Eylem planı aktarım sürecini kolaylaştırmak için özel operatörler ile diyalog teşvik edilecek.
b. Ulusal düzenlemeleri uyumlu hale getirmek için eylem planının Ulusal Siber Güvenlik Mimarisi üzerindeki etkisi değerlendirilecek.
c. Eylem planı hedefleri aktarılacak ve yeni gereksinimleri kritik altyapılar ile ilgili olanlarla birleştirmek için uygulama hükümleri tanımlanacak.

7. EYLEM MADDESİ: GÜVENLİK PROTOKOLLERİ VE STANDARTLARA UYUM

7.1.Standardizasyon ve uyum

a. Ulusal çerçeve uluslararası onaylanmış standartlara ve en iyi uygulamalara göre güncellenecek.
b. Kamu yönetimi ve kritik altyapılar ağı ve bilgi sistemleri için temel güvenlik önlemleri belirlenecek ve güncellenecek.

c. Ağların ve bilgi sistemlerinin güvenliğini artırmak için standartlar, en iyi uygulamalar ve minimum gereksinimler benimsenecek.
d. Dijital ve bilgi teknolojileri güvenlik sertifikalarını vermekten sorumlu kuruluşlar için bir doğrulama ve denetim sistemi oluşturulacak.

7.2.Referans dokümanlar

a. Bilgi paylaşımını kolaylaştırmak için yönergeler, standartlar, en iyi uygulamalar ve sınıflandırmalar yayınlanacak.

7.3.Siber güvenlik yönetimi programlarını güncelleme

a. Siber güvenlik çerçeveleri (kurallar ve prosedürler gibi) için düzenli güncellemeler ve incelemeler gerçekleştirilecek.

7.4.Bilgi ve iletişim teknolojisi güvenlik sertifikası

a. Bilgisayar Güvenliği Sertifikasyon Kuruluşu (Organismo di Certificazione Informatica OCSI) aracılığıyla sınıflandırılmamış ürün ve hizmetlerin Ulusal Bilgi ve İletişim Teknolojisi Sertifikasyonu Çerçevesi oluşturulacak.
b. Bilgi sistemleri süreçlerinin sertifikasyonu için ulusal düzen güncel tutulacak.
c. Bilgi ve iletişim teknolojisi ürünlerinin ve sınıflandırılmış verilerle ilgilenen sistemlerin teknik değerlendirmesi için Değerlendirme Merkezi (Centro Valutazione CE.VA) laboratuvarının operasyonel kapasitesi artırılacak.
d. Sertifikasyon standartlarının karşılıklı tanınmasını yöneten uluslararası kuruluşların yürüttüğü faaliyetlere katılım sağlanacak.
e. Sınıflandırılmış ve sınıflandırılmamış bilgiler için değerlendirme prosedürleri oluşturulacak.

7.5.Temel hizmet sağlayıcıları ve kritik altyapılar için siber savunma önlemleri

a. Savunma sistemleri düzenli olarak teknik ve prosedürel kontrollerle test edilecek.
b. Bağımsız bir kontrol sistemi oluşturulacak.

8. EYLEM MADDESİ: SANAYİ VE TEKNOLOJİK GELİŞİMİN DESTEKLENMESİ

8.1.Üretim, İnovasyon ve Teknoloji İşbirliği

a. Esnek ve verimli bir değerlendirme, onaylama ve sertifikasyon süreci ile desteklenen, bilgi ve iletişim teknolojisi bileşenleri için güvenli ve esnek bir tedarik zincirinin oluşturulması teşvik edilecek.
b. Ulusal ve uluslararası düzeyde rekabetçi bir endüstriyel taban geliştirmek ve tasarım gereği güvenliğe dayalı dikey bir tedarik zincirinin oluşturulmasını kolaylaştırmak için ayrıca potansiyel bir teşvik paketi yoluyla bilgi ve iletişim teknolojisi yeniliği teşvik edilecek.

c. Hem AB düzeyinde hem de uluslararası düzeyde, ulusal araştırma ve geliştirmeyi iyileştirmek için ikili ve çok taraflı işbirliği programları geliştirilecek.

8.2.Karşılaştırmalı analiz için ulusal laboratuvar

a. Kamu idareleri ve kritik altyapılar tarafından benimsenecek bilgi ve iletişim teknolojisi sistemlerinin karşılaştırmalı analizi için bir devlet laboratuvarının oluşturulması sağlanacak.

9. EYLEM MADDESİ: STRATEJİK İLETİŞİM

9.1.Stratejik ve operasyonel iletişim

a. İletişim verimliliğini artırmak, müdahale ve iyileştirme faaliyetlerini kolaylaştırmak, ne zaman genele yayılması gerektiğini değerlendirmek ve uygun iletişim kanallarını belirlemek için durumsal farkındalık konusunda koordinasyon kapasitesi geliştirilecek.

10. EYLEM MADDESİ: KAYNAKLAR

10.1. Finansal planlama

a. Kritik altyapıların siber güvenlik ve siber savunma ile ilgili öncelikleri ve bütçesinin yanı sıra hem fiziksel kaynaklar hem de insan sermayesi açısından temel kapasitenin geliştirilmesiyle ilgili maliyet belirlenecek.

10.2. Siber olaylarla ilgili maliyetlerin değerlendirilmesi

a. Siber olayların ekonomik etkisinin değerlendirilmesi için ilgili ölçütler belirlenecek.
b. Bir "*domino etkisi*" durumunda siber olayların ekonomik etkisinin değerlendirilmesini iyileştirmek için kritik altyapıların karşılıklı bağımlılıkları analiz edilecek.
c. Ekonomik açıdan olaylar ve potansiyel senaryolar haritalanacak.

10.3. Verimli harcamayı teşvik etmek

a. Ulusal (kamu, kamu-özel) ve uluslararası (işbirliği programları aracılığıyla) düzeyde verimli siber savunma harcama önlemleri uygulanacak.

10.4. Beşeri sermaye

a. Uluslararası en iyi uygulamaları da takip ederek, uzmanlaşmış kaynakların kurumlar arası koordineli işe alım faaliyetleri kolaylaştırılacak.

11. EYLEM MADDESİ: ULUSAL SİBER RİSK YÖNETİMİNİN UYGULANMASI

11.1. Metodoloji

a. Ulusal düzeyde risk değerlendirme önlemleri benimsenecek.
b. Temel hizmetler, kritik altyapılar ve diğer ulusal stratejik aktörler için benzersiz ve üzerinde anlaşmaya varılmış bir siber risk yönetimi metodolojisi belirlenecek.

c. Performans gösteren risk yönetimi araçları geliştirmek için araştırma sektör ve üniversiteler teşvik edilecek.

4.7. Lüksemburg'un Ulusal Siber Güvenlik Stratejisi

Lüksemburg'un III. Ulusal Siber Güvenlik Stratejisi 26 Ocak 2018 yılında yayımlanmıştır. Üç ana bölümden oluşan eylem planı oldukça detaylı ve kapsamlıdır. Eylem planındaki tespit ve değerlendirmeler dikkate değerdir. Dijital ortamı geniş anlamda ve özellikle bilgi ve iletişim teknolojileriyle karakterize ederek gelişen doğa, günlük yaşamlarımız üzerinde doğrudan bir etkiye sahiptir. Günümüzde, büyük ölçekli ve çok hızlı gelişen yeni teknolojilerin ortaya çıkmasıyla birlikte yeni risk vektörleri de oluşmaktadır. Toplumun bu sürekli değişen dijital manzaraya eşlik eden büyük dönüşümlere adaptasyonu karmaşık bir süreç olmaya devam etmektedir.

Lüksemburg Siber Güvenlik Kurulu (CSB), yeni bir ulusal siber güvenlik stratejisi geliştirmek amacıyla, ikinci ulusal siber güvenlik stratejisinin kapsadığı dönemin sonuna kadar, Ulusal Koruma Yüksek Komiserliği yetkisi altında faaliyet gösteren bir görev gücü oluşturulmuştur. Eylem planının amacı, yukarıda değinilen geniş kapsamlı değişikliklere yanıt vermek ve genellikle ulus ötesi düzeyde organize edilen çok çeşitli nitelikteki siber saldırıların ortaya çıkmasına karşın, halkın yeni teknolojilere olan güvenini pekiştirmektir. Stratejinin doğasında bulunan bir diğer endişe, dijital ekonominin gelişmesi adına, nesnelerin interneti, yapay zeka gibi yeni konuların daha derinlere inme gerçeğini desteklemeye olanak tanıyan bir ortam yaratmaktır (Lüksemburg, 2018).

Yeni ulusal siber güvenlik stratejisi, hükümetin yeni teknolojilerin doğasında bulunan hem fırsatlardan hem de risklerden yararlanabildiğini göstermektedir. 2018-2020 dönemini kapsayan strateji, bu bağlamda aşağıdaki üç ana kılavuz etrafında yapılandırılmıştır (Lüksemburg, 2018):

- Lüksemburg'un BM'nin ekonomik, sosyal, çevresel ve politik açıdan sürdürülebilir politikasıyla "a*kıllı ulus*" modeline geçişi için dijital ortamda halkın güveninin güçlendirilmesi.
- Bilgi bütünlüğü ve gizliliği kadar temel olan hizmetlerin kullanılabilirliğini sağlamak için dijital altyapının korunması sağlanacaktır.

- Özellikle dijital alanda etkin olan şirketlerin kurulmasına ve gelişmesine elverişli bir ekonomik teşvikin sağlanması.

"*Siber güvenlik*", siber ortamı, kuruluşunu ve kullanıcılarının varlıklarını korumak için kullanılabilen araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, en iyi uygulamalar, güvence ve teknolojilerin toplamıdır. Genel güvenlik hedefleri aşağıdakileri içerir (Lüksemburg, 2018):

- Kullanılabilirlik;
- Doğruluk ve inkar edilemezlik;
- Gizlilik.

Siber güvenlikle ilgili mevcut ve gelecekteki zorluklar, yalnızca verimli ve etkili ulusal siber yönetişim aracılığıyla çözülebilir. Lüksemburg'un NATO ve Avrupa Birliği düzeyindeki siber savunma taahhütleri, farklı düzeylerde Avrupa ve uluslararası işbirliği ve bilgi paylaşımı anlaşmaları göz önünde bulundurulduğunda, AB Direktifi'nin uygulanmasının ağ ve bilgi sistemleri güvenliği üzerindeki etkisi siber güvenlikle ilgili konuların yatay karakteri olarak, mevcut yönetişim modeli, bakanlıklar arası siber önleme ve siber güvenlik koordinasyon komitesinin oluşturulmasıyla güçlendirilmesi planlanmaktadır. Öncelikli hedefler aşağıdaki üç kılavuzda listelenmiştir. Aşağıda bu kılavuzlar ve eylemler sınıflandırılmıştır (Lüksemburg, 2018):

Dijital Ortamda Halkın Güveninin Güçlendirilmesi (Klavuz No 1): Her vatandaş, bilgi ve iletişim teknolojisinin sunduğu fırsatlardan tam olarak yararlanabilmelidir. Bu bağlamda, kullanıcıların bu teknolojilere olan güvenini üst düzeyde tutarken, bu güvenin dış etkenlerden (örn. siber saldırılar, online dolandırıcılıklar vb.) etkilendiğini bilmek önemlidir.

- Hedef 1: Tüm Paydaşlar Arasında Bilgi Paylaşımı
- Hedef Ek 2: Risklere İlişkin Bilgilerin Yaygınlaştırılması
- Hedef 3: İlgili Tüm Tarafların Ortaklıklarını Artırmak
- Hedef 4: Sorumlu Açıklama
- Hedef 5: Siber Suçla Mücadele

Dijital Altyapıyı Koruma (Kılavuz No 2): Tüm sektörlerin artan iş süreci, uzman aktörler tarafından sağlanan altyapı ve dijital hizmetlere dayanmaktadır. Lüksemburg'un dijital bir ulusa dönüşümü, bu gelişimi hızlandırmakta ve gizlilik, bütünlük ve erişilebilirlik açısından altyapı ve hizmetlerin güvenliğine olan ihtiyacı artırmaktadır. Sonuç olarak, dijital altyapılar, fiziksel dünyada saldırı yüzeyini artırdıkları için, ülkenin hayati çıkarlarının korunmasında önemli bir rol oynamaktadır. Bu nedenle hükümet, dijital altyapının dayanıklılığına özel önem vermektedir.

- Hedef 1: Temel ve Kritik Dijital Yapı Sayımı
- Hedef 2: Güvenlik Politikaları
- Hedef 3: Kriz Yönetimi
- Hedef 4: Standardizasyon
- Hedef 5: Uluslararası İşbirliğini Güçlendirmek
- Hedef 6: Siber Savunma
- Hedef 7: Devletin Dijital Altyapısının Güçlendirilmesi

Ekonominin Tanıtımı (Kılavuz No 3): Saldırganların profesyonelliği, teknolojinin hızlı evrimi ve doğal olarak ortaya çıkan tehditler ile karşı karşıya kalan tüm kamu ve özel sektör paydaşları arasında yoğun işbirliği oluşmuştur. Hükümet, belirli hizmetlerin bir havuzda toplanması ve mevcut sinerjilerden yararlanılması da dahil olmak üzere bilgi güvenliğine erişimi demokratikleştirmek için gerekli önlemleri uygulamayı amaçlamaktadır. Bu yaklaşımın, siber güvenlikle ilgili karmaşıklığı ve maliyetleri azaltması ve dolayısıyla bu alana yatırımın cazibesini artırması beklenmektedir.

- Hedef 1: Yeni Ürün ve Servisler Geliştirmek
- Hedef 2: Altyapıların Güvenlik Havuzu
- Hedef 3: Gereklilik Karşılaştırmaları ve Yüklenici
- Hedef 4: Siber Güvenlik Yeterlilik Merkezinin Oluşturulması
- Hedef Ait 5: Risk Yönetimi ve Bilgilendirilmiş Yönetim
- Hedef 6: Eğitim ve Eğitim Yardımı
- Hedef 7: Bilgi Güvenliği Yükümlülüğündeki Taraflar Arası İşbirliği
- Hedef 8: Olaylara Müdahalede Uzmanlar Arasında İşbirliği
- Hedef 9: Araştırma Önceliği: Start-Ups

- Hedef 10: Kod Sökme (disassembly) ve Güvenlik Açığını Belirleme

Bu eylem planı, 2018 yılından sonraki üç yıl içinde ulaşılması önemli olan hedefleri tanımlamaktadır. Bu hedefler, belirli bir zaman dilimi sonrasında uygulanacak somut önlemleri ve bunların uygulanmasına katkıda bulunmaya çağrılan aktörleri özetleyen bir uygulama eylem planı ile tamamlanacaktır (Lüksemburg, 2018).

Ulusal Siber Güvenlik Stratejisi İle İlgili Geri Bildirim (Ek Kılavuz)

Genel anlamda toplumun karşılaştığı bir zorluk olarak bilgi güvenliğine vurgu yapmıştır. Herhangi bir şirket, kamu hizmetleri veya vatandaş olması; taraflar için, güvenli bir dijital toplumun inşasının sorumluluğunu taşımaktadır. Bu ek kılavuz, eylem noktalarının ilerlemesi ve uygulanmasına ilişkin bir güncelleme sağlarken, siber güvenliğin evrimsel bir karaktere sahip sürekli ve dinamik bir süreci temsil ettiği göz önüne alındığında bazı eylemlerin tekrarlandığı gözlemlemektedir.

- Hedef 1: Ulusal İşbirliğini Güçlendirmek
- Hedef 2: Uluslararası İşbirliğini Güçlendirmek
- Hedef 3: Dijital Altyapının Saldırılara Karşı Direncinin Artırılması
- Hedef 4: Siber Suçla Mücadele
- Amaç 5: İlgili Risklere İlişkin Bilgilendirme, Eğitim ve Bilinçlendirme
- Hedef 6: Hükümet ve Kritik Altyapılar İçin Uygulama Standartları, Normları, Sertifikaları, Etiketleri ve Referans Çerçeveleri
- Hedef 7: Akademik ve Araştırma Kümesi ile İşbirliğinin Güçlendirilmesi

Siber güvenliğe yönelik ulusal tehditlerin analizi aşağıdaki eylem noktalarını ifade etmiştir (Lüksemburg, 2018):

- *Fidye Yazılımları:* Saldırganlar, kurbanın sisteminde şifreledikleri dosyayı erişilemez kılıp şifre çözme anahtarını kurbana teslim etmek için, belli bir fidye ödemesini ister. Bu yazılımlarla tamamen finansal amaçlı saldırılarda önemli bir artış kaydedilmiştir. Bu tür yasadışı faaliyetler, bitcoin, ethereum, vb. gibi sanal para birimlerinin ortaya çıkmasıyla yeniden kolaylaştırılmaktadır.

- *Nesnelerin İnterneti Yoluyla Dağıtılmış Hizmet Reddi (DDoS) Tarafından Yapılan Saldırılar:* DDoS saldırılarının etkisi giderek daha önemli hale gelmektedir. Nesnelerin internetinin (IoT) yaygın kullanımının bir sonucu olarak bu saldırı biçimi, eşi görülmemiş bir önem kazandırmaktadır. Bu araçlar internette ücretsiz olarak elde edilebilir durumdadır ve genellikle şantaj amacıyla kullanılırlar. Bu tür araçlar aynı zamanda internet bağlantılı nesneleri kitlesel gözetleme veya bir tür endüstriyel casusluk gerçekleştirmek için kullanılabilir.
- *Brıckerbot (Nesnelerin İnterneti Cihazlarını Kalıcı Olarak Yok Etmeye Çalışan Kötü Amaçlı Yazılımı):* Hizmetlerin çalışmasını bir süre engelleyen DDoS saldırıları gibi diğer saldırıların aksine "BrickerBots" internet bağlantılı nesneleri yok etmek için tasarlanmıştır. Bu saldırılar çok gizli ve tespit edilmesi zor olabilir. Zayıf korumaya sahip nesneleri hedeflerler ve başarılı kimlik doğrulamasından sonra, nesneyi kullanılamaz hale getirmek için sistem ayarlarını değiştirmeye çalışırlar.
- *Akıllı Şehirlerin ve Ev Otomasyonunun Geliştirilmesinde Bulunan Riskler:* Günlük hayatımızın bir parçası olan ve yüksek değerli hizmetler sağlamak için kullanımı giderek daha fazla artan sistemler, bileşen ve gerçek zamanlı dijital altyapıdan gelen bilgileri kullanmaktadır. Akıllı şehirler, veri toplayan sensörlerle donatılmıştır ve yüksek derecede bağlanabilirlikleri ile karakterize edilen hizmetleri optimize etmek için bilgi sistemlerine güvenirler. Bu altyapılara yönelik saldırılar, genellikle en yüksek güvenlik düzeyini karşılamayan kimlik doğrulama sistemleri ve kriptografik protokollerin varlığında çoğalacaktır.
- *Minimum Güvenlik Standartlarına Uygun Olamama:* Bilgisayar güvenliği, yazılım ve BİT araçlarının üretiminde her zaman bir öncelik değildir. Çoğunlukla milyonlarca kullanıcıya dağıtılan bu tür yazılımlar, manipüle edilmek için saldırıya uğrayabilir ülkenin ekonomisi ve güvenliği için gerçek bir tehdit oluşturur.
- *İş Sürecine Yönelik Tehditler:* Son saldırılar, saldırganların eylemlerini ve hedeflerini çeşitlendirdiğini gösteriyor. Şantaj, veri hırsızlığı veya veri sabotajı yoluyla zarar vermek yerine, iş sürecini de hedefliyorlar. BİT alanında kalifiye insan kaynağı eksikliği bu bağlamda bir kırılganlık olarak değerlendirilmelidir. Sonuç olarak çok sayıda şirketin BİT sistemlerini, bu alanda uzmanlaşmış önemli aktörlere dış kaynak sağlamaktan başka seçeneği yoktur. Bu şirketlerin personelinin artık iş veya endüstriyel süreçleri korumak için gerekli olan becerilere sahip olmadığı

anlaşılmaktadır. Avrupa Komisyonu tarafından Eylül 2017'de sunulan siber güvenlik paketi, bu tehditlerin çoğunu ele almayı hedefliyor.

- *Düzenleyici Tehditler:* "WannaCry" ile bilgisayar solucanlarının yeniden dirilişi tüm dünya çapında hissedilmiştir. Saldırı ayrıca, bir riskin çok katı düzenleme yükümlülüklerinden kaynaklanabileceğini de gösterdi. Bu süreç, standartlarıyla uyumluluk sağlamak için ana kaynakları birbirine bağlarken yanlış bir güvenlik duygusu verebilir.
- *Sosyal Ağlar ve Sosyal Mühendislik Hakkında Bilgilerin Açıklanması:* Günümüzde sosyal ağların kullanımı giderek artıyor. Kullanıcılar, kişisel verileri hakkında bol miktarda bilgi vermektedirler. Sosyal güvenlik halkası tekniği, suç amaçlı, hatta casusluk veya sabotaj için kullanmak üzere şirketler tarafından saklanan gizli bilgilere erişmek için tasarlanmıştır. Ancak bunu önleyebilecek güçlü kimlik doğrulama sistemleri bulut ortamlarında pek yaygın değildir.
- *Çok Sayıda İnternet Erişim Araçlarından Kaynaklanan Tehditler:* Günümüzde kullanıcılar internete girmek ve çevrimiçi işlem yapmak için sıklıkla cep telefonlarını kullanıyorlar. Bazı akıllı telefonların korunması ne yazık ki zordur ve bu nedenle ideal bir hedefi temsil eder.
- *Dijital Araçların Destabilizasyon Aracı Olarak Kullanımı:* Son zamanlarda büyük bir etkiye sahip olan tehditlerden biri, dijital araçların bir istikrarsızlaştırma aracı olarak kullanılmasıdır. Burada, bir güvenlik otoritesinden çok sayıda bilgisayar aracını, belirli sistemlere ve ağlara erişmek için kullandığı araçları ele geçirmey, başaran "shadow-rokerler" grubundan bahsetmek gerekir. Böyle bir silahın kullanımının çok ciddi sonuçları olabilir. Tüm bir ülkenin dijital yollarla dijital sabotajı ve kapatılması fikri giderek daha gerçekçi hale geliyor.
- *Yapay Zeka Geliştirilmesindeki Tehditler:* Genel olarak yapay zeka, kötü amaçlı yazılımların tasarlanması ve çalıştırılması bağlamında ortaya çıkmaktadır. Şu anda akademi dünyasında bir araştırma konusudur ve yakında gerçek anlamda uygulanacak kadar olgunlaşacak, bununla birlikte, kuruluşların ağlarını ve altyapılarını savunan ekipler tarafından alınan güvenlik önlemlerine dinamik olarak uyum sağlama becerisine sahip olunması hedeflenmektedir.

4.8. Hollanda’nın Ulusal Siber Güvenlik Stratejisi

Hollanda Ulusal Siber Güvenlik Stratejisi beş ana bölümden oluşmaktadır. Dijital alanda güvenlik, hükümet için en önemli önceliktir. Bu nedenle, koalisyon anlaşmasında siber güvenlik için 95 milyon Euro’luk yapısal bir yatırımı taahhüt edilmiştir. Güvenli, dijital bir Hollanda'ya toplu olarak katkıda bulunacak yedi zorlu hedef belirlenmiştir. Tüm bunlar için çok önemli olan, Hollanda’nın siber tehditleri tespit etmek, azaltmak ve kararlı bir şekilde yanıt vermek için yeterli dijital yeteneklere sahip olmasıdır. Ulusal sınırlar dijital dünyada neredeyse hiç rol oynamadığı için, yaklaşımın da güçlü bir şekilde uluslararası odaklı olması gerekecektir. Bu nedenle Hollanda, AB ve NATO düzeyinde dijital güvenliğin güçlendirilmesi için çalışmaya devam etmelidir. Aşağıdaki ilkeler Hollanda’nın siber güvenlik stratejilerine yol göstermektedir (Hollanda, 2018):

- Siber güvenlik, ayrılmaz bir şekilde ulusal güvenlikle bağlantılıdır: dijitalleşmenin bir sonucu olarak, ulusal güvenlik çıkarları dijital saldırılara karşı savunmasızdır.
- Dijital alandaki güvenlik, yalnızca iş dünyasıyla ve kısmen iş dünyası tarafından işbirliği içinde şekillendirilebilir. Bu nedenle kamu-özel işbirliği, siber güvenliğe Hollanda yaklaşımının temelini oluşturur.
- Hükümet, hayati çıkarlara yönelik tehditleri kabul ederek kamu çıkarlarını temsil eder.
- Mevcut bilginin paylaşılması, kamu ve özel sektör tarafından bilgi paylaşımının teşvik edilmesi, yönetim kurulu genelinde siber güvenliği güçlendirmek için gereklidir.

Hollanda siber güvenlik bilgi konumunu geliştirmek için siber güvenliğe yönelik hem temel hem de uygulamalı araştırmaları teşvik etmeyi amaçlamaktadır. Aşağıda bu teşvik sistemleri açıklanmıştır (Hollanda, 2018):

- Dijital güvenlik, her kuruluşun günlük süreçlerinin bir parçası olmalıdır. Amaç, siber güvenliğin yaygınlaştırılmasıdır.
- Dijital alan, ulusal sınırlarla sınırlı değildir. Hollanda’nın siber güvenliğe yaklaşımı, veriler, bağlantılar, internet yönetişimi ve dijital saldırılar gerçekleştiren aktörlerin uluslararası boyutunu dikkate almaktadır.
- Son olarak: özgürlük, güvenlik ve ekonomik büyüme çıkarları arasındaki gerilim, siber güvenliğin gelişiminin doğasında vardır.

Siber güvenlik dijital alanda ekonomik fırsatların ve sosyal değerlerin temelidir. Hollanda, dünyanın en dijitalleşmiş ülkelerinden biridir. Bu bize yeni teknolojileri güvenli, özgür ve hızlı bir şekilde benimseme ve kullanma konusunda uluslararası bir lider olmak için olağanüstü koşullar sunmaktadır. Bu yeni teknolojiler günlük yaşamımızda giderek daha önemli bir rol oynamaktadır. Dahası, bakımda geniş kapsamlı dijitalleşme (e-sağlık), mobilite (e-otomotiv), internete bağlı cihaz ve cihazlardaki büyüme (Nesnelerin İnterneti), büyük veri, 5G, kuantum bilgisayarlar ve yapay zeka gibi anahtar teknolojiler dijital alanın ve fiziksel alanın daha yakından iç içe geçmesini sağlamaktadır (Hollanda, 2018).

Siber güvenliğin tanımı: Siber güvenlik, bilgi ve iletişim teknolojilerinin kesintiye uğraması, arızalanması veya yanlış kullanımından kaynaklanan zararları önlemek ve hasar meydana gelmesi durumunda kurtarmaya yönelik önlemlerin tamamıdır (Hollanda, 2018).

Siber casusluk, sabotaj ve profesyonel suçun dijital alandaki şeklidir. Dijital sabotaj veya kesinti, doğrudan ulusal güvenliğin zarar görmesine neden olabilir. Dijital alandaki en büyük tehdit suçlular ve devlet aktörlerinden gelmektedir. Dijital saldırıların neredeyse maliyetsiz ölçeklenebilirliği, suçlular için özellikle ilgi çekicidir. Örneğin; bir hizmet olarak siber suç ve fidye yazılımıdır. Saldrıganlar hiçbir şekilde bir saldırının tüm adımlarını kendileri gerçekleştirmezler. Genellikle hizmet ve uzmanlık satın alırlar. Buna bir örnek fidye yazılımıdır: sistemleri ve/veya içerdikleri bilgilere erişimi engelleyen ve yalnızca fidye ödenmesi karşılığında yeniden erişilebilir kılan bir tür kötü amaçlı yazılımdır. Bir suçlu fidye yazılımı dağıtmak isterse, onu geliştirmesi için birine ödeme yapar ve fidye yazılımını milyonlarca adrese e-posta yoluyla dağıtması için başka birine para verir. Bu hizmetler, teknik kaynaklardan altyapıya ve yardım masası işlevselliğine kadar çok profesyonelce ve eksiksiz olarak sağlanır. Bu bağlamda eylem planın stratejik ilkeleri aşağıdaki gibi belirlenmiştir (Hollanda, 2018):

1. Siber güvenlik, ulusal güvenliğin bütünleşik bir parçasıdır.
2. Kamu-özel işbirliği temel amaçtır.
3. Hükümet kamu çıkarlarını temsil etmektedir, kendi sorumluluklarının kabulünü teşvik eder ve iyi bir örnek belirtir.
4. Bilgiyi geliştirme ana amaçtır.
5. Paylaşım önemlidir.
6. Siber güvenliğin ana akışı bir ön koşuldur.

7. Dijital alanın ulusal sınırı yoktur.

Hollanda'nın siber güvenliğe yaklaşımının şu hedefi vardır: Hollanda, dijitalleşmenin ekonomik ve sosyal fırsatlarından güvenli bir şekilde yararlanma ve dijital alanda ulusal güvenliği koruma becerisine sahip olmayı amaçlamaktadır. Bu nedenle, aşağıdaki hedefler belirlenmiştir (Hollanda, 2018):

1. *Hollanda, siber tehditleri tespit etmek, azaltmak ve kararlı bir şekilde yanıt vermek için yeterli dijital yeteneklere sahiptir.* Artan dijital tehdide etkili bir şekilde yanıt vermek için, Hollanda'daki devlet kurumları ve özel kuruluşlar işbirliği yapmalı ve uygun kapasite ve kaynaklara sahip olmalıdır. Bu kuruluşların bir kısmı hala bu kapasiteleri geliştiriyor ve çeşitli olgunluk seviyelerindeler. Alt hedefler ve ulaşılması planlanan sonuçlar;
   a. Kamu yetkilileri ve işletmeler, dijital tehditlere ve saldırılara uygun şekilde yanıt verebilir. Bunu yapmak için gerekli (önleyici) tedbirleri uygularlar.
   b. Hollanda, ulusal güvenliğe tehdit oluşturan büyük ölçekli siber olaylara hazırlıklıdır.
   c. Ulusal güvenlik açısından hayati öneme sahip kuruluşlar, dijital tehditleri ve saldırıları daha iyi anlar ve kendilerini ve ulusal güvenliği tehdit eden saldırıları tespit edebilir.
   d. Siber güvenlik ile ilgili bilgilerin kamu ve özel sektör tarafları arasında daha yaygın, verimli ve etkili bir şekilde paylaşılabileceği ülke çapında bir siber güvenlik ortaklıkları ağı oluşturulacaktır. Ülke çapındaki bu ağın amacı, kamu ve özel tarafların yeteneklerini güçlendirmektir.
   e. Dijital alanda etkin eylem için yasal araçlar düzenli kalır ve tehdit, teknolojik gelişmeler ışığında güncel tutulur.
2. *Dijital alanda uluslararası barış ve güvenlik.* Devlet aktörleri, güç kullanma araçlarının ayrılmaz bir parçası olarak veya somut çatışma durumlarında casusluk, hedefleri etkilemek ve sabote etmek için dijital kaynakları giderek daha sık kullanıyor. Saldırı amaçlı, askeri siber yetenekler geliştiren ülkelerin sayısında da artış olmaktadır. Bu tehdit son yıllarda önemli ölçüde artmıştır ve uluslararası güvenlik için ciddi bir tehdittir. Alt hedefler ve ulaşılması planlanan sonuçlar;
   a. Hollanda, insan haklarının korunması dahil olmak üzere dijital alanda uluslararası hukuk düzenini teşvik etmektedir.

b. Hollanda, tek başına veya bir koalisyonun parçası olarak, devlet aktörlerinin dijital saldırılarına anında ve uygun şekilde yanıt vererek caydırıcılığa katkıda bulunan saldırı yeteneklerine sahiptir.
c. Hollanda, küresel siber güvenlik zincirinin yeteneklerinin geliştirilmesine yatırım yaparak suçlulardan ve devlet aktörlerinden gelen siber tehditlerin azaltılmasına katkıda bulunur.

3. *Dijital olarak güvenli donanım ve yazılım.* Nesnelerin internetinin tanıtılması ve sürekli gelişmesinin bir sonucu olarak, giderek daha fazla cihaz internete bağlanmaktadır. Alt hedefler ve ulaşılması planlanan sonuçlar;
   a. Hollanda, donanım ve yazılımda dijital güvenlik risklerini önlemek için standardizasyon ve sertifikasyon girişimlerini teşvik edecek, denetim ve yaptırımı güçlendirecektir.
   b. Hollanda, dijital ürünleri test ederek ve dijital güvenlik risklerini netleştirerek dijital güvenlik risklerinin tespitini iyileştirmek için çalışacaktır.
   c. Hollanda, bir sorumluluk rejimi yoluyla ve farkındalığı artırarak, vatandaşlar ve işletmeler için bir eylem perspektifi sunarak dijital güvenlik risklerinin azaltılması üzerinde çalışacaktır.
   d. Hollanda, donanım ve yazılımın dijital güvenliğini artırmak için bir dizi temel ilkenin gerçekleştirilmesi için çaba gösterecektir.
4. *Esnek dijital süreçler ve sağlam bir altyapı.* Hollanda toplumuyla giderek daha fazla iç içe geçmektedir. Bunun sonuçlarından biri, işletmelerin ve kamu otoritelerinin faaliyetlerinin akıllı uygulamalar aracılığıyla giderek daha fazla veri odaklı hale gelmesidir. Kuruluşlar artık tüm görevleri kendi başlarına yerine getirme yeteneğine sahip değildir. Zincirler halinde çalışırlar. Diğer şeylerin yanı sıra, verileri sağlamak, veri işlemlerini yürütmek, desteklemek için diğer kuruluşlara bağlıdırlar. Alt hedefler ve ulaşılması planlanan sonuçlar;
   a. Tüm zincirin dayanıklılığını artıran kritik süreçlerin sürekliliğini ve dijital esnekliğini sağlamaya ilgili tüm taraflar dahil olacaktır.
   b. Hollanda, açık kaynak yazılımın kalitesini ve modern internet protokolleri ve internet standartlarının hızlı bir şekilde benimsenmesini geliştirmeyi amaçlamaktadır.
   c. Hollanda hükümeti, güvenli bilgi ve iletişim teknolojilerinin ürün ve hizmetlerinin geliştirildiği ve benimsendiği yenilikçi bir siber güvenlik ortamını teşvik etmektedir.

5. *Siber suçlara karşı başarılı engeller.* Suçlular, faaliyetlerini büyük ölçekte internet üzerinden sürdürüyorlar: 2017 yılında her dokuz kişiden biri siber suç mağduru olmuştur. Siber suç terimi, dijital biçimdeki klasik suçtan yeni suça kadar çok çeşitli cezai eylemleri kapsamaktadır. Alt hedefler ve ulaşılması planlanan sonuçlar;
   a. Saldırganlara karşı koyan etkili engeller vardır.
   b. Siber güvenliği güçlendirme ve siber suçla mücadele çabaları birbiriyle bağlantılı olarak uygulanmaktadır. Kamu yetkilileri ile iş dünyası, vatandaşlar ve sivil toplum kuruluşları arasındaki işbirliği bu açıdan son derece önemlidir.
   c. Siber güvenlik için, soruşturma yetkilerinin, saldırganların çalışma yöntemlerindeki gelişmelere ayak uydurması, böylece ulusal güvenliğe yönelik tehditlerin ele alınabilmesi önemlidir.
6. *Siber güvenlik bilgisini geliştirme.* Bilgi, Hollanda'da son derece önemli bir varlıktır. Hollanda toplumu ve özellikle dijital güvenlik bilgisinin geliştirilmesine ve kullanımına bağlıdır. Alt hedefler ve ulaşılması planlanan sonuçlar;
   a. Hollanda, yüksek kaliteli siber güvenlik araştırması yürütmektedir.
   b. Hollanda, akademik topluluğun yüksek kaliteli bilgiyi geliştirip iyileştirdiği uzun vadeli bir bilgi geliştirme programına sahiptir ve siber güvenlik alanında bağımsız bir bilgi pozisyonu elde etmek için yeterli sayıda akademisyen bulunmaktadır.
   c. Vatandaşlar ve işletmeler, dijital tehditleri ele almanın önemini görebilir ve siber suçlara karşı daha dayanıklı hale gelebilir.
7. *Siber güvenlikte kamu-özel yaklaşım.* Son yıllarda, Hollanda'da siber güvenliği iyileştirmek için kamu, özel ve kamu-özel sektörleri çeşitli girişimlerde bulunmuştur. Yaklaşımın seyri ve hızı, bu yönü korumak için koordine edilmelidir. Koordinasyon daha güçlü olabilir ve olmalıdır ve bu elbette hükümete bağlıdır. Alt hedefler ve ulaşılması planlanan sonuçlar;
   a. Siber güvenliğe entegre yaklaşımda hükümetin koordinasyon rolü güçlendirilecektir.
   b. Hollandalı işletmeler, vatandaşlar ve devlet kuruluşları siber güvenlikle ilgili sorumluluklarını, haklarını ve yükümlülüklerini yerine getirir.
   c. Dijital hükümetin bilgi güvenliği için, bir Devlet Bilgi Güvenliğinin oluşturulması ve uygulanması da dahil olmak üzere, dijital temel altyapının bilgi güvenliğini artırmak, bilgi güvenliğine ilişkin norm çerçevelerini daha da standartlaştırmak ve uyumlu hale getirmek için tutarlı bir önlemler paketi vardır.

4.9. İngiltere'nin Ulusal Siber Güvenlik Stratejisi

İngiltere'nin ulusal siber güvenlik stratejisi 2016-2021 dönemini kapsayacak şekilde hazırlanmıştır. Plan 10 bölümden oluşmakta olup bölümler başlıklar halinde aşağıda sunulmuştur (İngiltere, 2016):

1. Yönetici özeti
2. Giriş
3. Stratejik içerik
4. Ulusal Tepki
5. Savunma
6. Caydırıcılık
7. Gelişim
8. Uluslararası Tepki
9. Ölçüm
10. Sonuç

Planın oldukça kapsamlı ve geniş alanları içinde barındıran bir yapıda olduğunu söylemek mümkündür. Planda başlık altına alınmayan önsöz Maliye Bakanı Philip Hammond tarafından yazılmıştır. Hammond, İngiltere'nin Dünya'nın önde gelen dijital ülkelerinden birsi olduğunu, artık refahlarını korumak için teknolojilerini, verilerini ve ağlarını koruma yeteneklerine bağlı olduğunu, siber saldırıların daha sık, sofistike ve başarılı olduklarını, bu yüzden hem ekonomiyi hem de İngiltere vatandaşlarının mahremiyetini korumak için kararlı adımlar attıklarını ifade etmiştir. Siber güvenlik için 1.9 milyar sterlinlik harcama yapmayı planladıklarını ve İngiltere'yi hızlı ve hareketli bir dijital dünyada kendinden emin, yetenekli ve esnek kılma amacını taşıdıklarını vurgulamıştır (İngiltere, 2016).

Başlık içinde yer almayan bir diğer bölüm olan giriş ise 14 Temmuz 2016 - 11 Haziran 2017 döneminde Kabine Ofisi Bakanlığının Genel Müdürü olan Benedict Michael Gummer tarafından yazılmıştır. Gummer, başlıca sorumluluklarının ülkeyi güvende tutmak olduğunu, İngiltere'nin siber alanda karşılaştığı birçok tehdidin üstesinden gelebildiğini, siber tehditleri yönetmenin ve azaltmanın herkesin sorumluluğunda olduğunu, ancak Hükümet olarak gereken ulusal çabayı önderlik etme konusundaki özel sorumluluklarını kabul ettiklerini ve bu stratejide belirtilen taahhütlerin yerine getirilmesini sağlamayı taahhüt ederek bunları

yerine getirmedeki ilerlemeleri doğru bir şekilde izleyip raporlanacağını ifade etmiştir (İngiltere, 2016).

Raporun genişliği ve kapsamlı olmasından dolayı yönetici özetinde ayrıntılı olarak ele alınacak olup diğer bölümler daha çok başlıklar olarak açıklanacaktır. Önemli görülen ve eylem planıyla doğrudan alakalı yerlere ise özel önem verilecektir (İngiltere, 2016).

Birinci bölüm olan yönetici özetinin alt bölümleri doğrudan aşağıda sunulmuştur (İngiltere, 2016):

1.1. İngiltere'nin güvenliğinin ve refahının geleceği dijital temellere dayanıyor. Bizim neslimizin zorluğu hem siber tehditlere dirençli hem de fırsatları maksimize etmek ve riskleri yönetmek için gereken bilgi ve yeteneklerle donatılmış, gelişen bir dijital toplum oluşturmaktır.

1.2. Kritik olarak internete bağımlıyız. Ancak, doğası gereği internet güvensizdir ve her zaman siber saldırıları başlatmak için zayıf yönlerinden faydalanma girişimleri olacaktır. Bu tehdit tamamen ortadan kaldırılamaz, ancak risk, toplumun gelişmeye devam etmesini ve dijital teknolojinin getirdiği devasa fırsatlardan yararlanmasını sağlayacak bir seviyeye kadar büyük ölçüde azaltılabilir.

1.3. İngiliz Hükümeti'nin 860 milyon sterlinlik Ulusal Siber Güvenlik Programının desteklediği 2011 Ulusal Siber Güvenlik Stratejisi, İngiltere siber güvenliğinde önemli gelişmeler sağlamıştır. Güvenli siber davranışları yönlendirmek için piyasaya bakarak önemli sonuçlar elde etti. Ancak bu yaklaşım, hızlı hareket eden tehdidin önünde kalmak için gereken değişim ölçeğini ve hızını gerçekleştiremedi. Şimdi daha ileri gitmemiz gerekiyor.

1.4. 2021 için vizyonumuz, Birleşik Krallık'ın dijital dünyada müreffeh ve kendine güvenen, siber tehditlere karşı güvenli ve esnek olmasıdır.

1.5. Bu vizyonu gerçekleştirmekte aşağıdaki hedeflere ulaşmak için çalışacağız:

1.5.1. SAVUNMA: İngiltere'yi gelişen siber tehditlere karşı savunmak, olaylara etkin şekilde yanıt vermek, İngiltere ağlarının, verilerin ve sistemlerin korunmasını ve esnekliğini sağlamak için araçlarımız var. Vatandaşlar, işletmeler ve kamu sektörü kendilerini savunma bilgi ve becerisine sahiptir.

1.5.2. CAYDIRICILIK: İngiltere, siber uzayda her türlü saldırganlık için zor bir hedef olacaktır. Suçluları takip ederek ve kovuşturma yaparak, bize karşı yapılan

düşmanca eylemleri tespit eder, anlar, soruşturur ve bozarız. Siber alanda saldırgan harekete geçme yoluna sahibiz, bunu yapmayı seçtik.

1.5.3. *GELİŞİM: Dünyanın önde gelen bilimsel araştırma ve geliştirme çalışmalarının temelini oluşturan yenilikçi, büyüyen bir siber güvenlik endüstrisine sahibiz. Kamu ve özel sektördeki ulusal ihtiyaçlarımızı karşılama becerisi sağlayan kendi kendine yeten bir yetenek hattımız var. Gelişmiş analiz ve uzmanlığımız İngiltere'nin gelecekteki tehditleri ve zorlukları karşılamasını ve üstesinden gelmesini sağlayacaktır.*

1.6. *Bu hedefleri temel alarak Uluslararası Eylem'i izleyeceğiz ve siber uzayın küresel gelişimini daha geniş ekonomik ve güvenlik çıkarlarımızı artıracak şekilde ortaklıklara yatırım yaparak etkimizi göstereceğiz. Toplu güvenliğimizi geliştirdiğimizi kabul ederek, en yakın uluslararası ortaklarımızla mevcut bağlantıları derinleştireceğiz. Ayrıca, siber güvenlik seviyelerini artırmak ve İngiltere'nin yurtdışındaki çıkarlarını korumak için yeni ortaklarla ilişkiler geliştireceğiz. Bunu AB, NATO ve BM de dahil olmak üzere hem iki taraflı hem de çok taraflı olarak yapacağız. İlgi alanlarımıza veya müttefiklerimizin siber dünyaya zarar verme tehdidinde bulunan rakiplere sonuçları hakkında net mesajlar sunacağız.*

1.7. *Önümüzdeki beş yıl boyunca bu sonuçları elde etmek için, Birleşik Krallık Hükümeti daha aktif bir şekilde müdahale etmeyi ve artan yatırımları kullanmayı amaçlarken, Birleşik Krallık''ta siber güvenlik standartlarını yükseltmek için pazar güçlerini desteklemeye devam edecek. İngiltere Hükümeti, İskoçya, Galler ve Kuzey İrlanda'nın Geliştirilmiş İdareleri ile ortaklaşa olarak, bireylerin, işletmelerin ve kuruluşların internette güvende kalmak için gereken davranışları benimsemelerini sağlamak için özel ve kamu sektörleriyle birlikte çalışacaktır. Ulusal çıkarları olan, özellikle de kritik ulusal altyapımızın siber güvenliğiyle ilgili iyileştirmeleri teşvik etmek amacıyla müdahale etmek için (gerektiğinde ve güçlerimizin kapsamı dahilinde) önlemleri alacağız.*

1.8. *Birleşik Krallık Hükümeti, Birleşik Krallık ağlarındaki siber güvenlik seviyelerini önemli ölçüde artırmak için aktif siber savunma önlemlerini geliştirme ve uygulama yeteneklerini ve endüstrilerini kullanacaktır. Bu önlemler arasında en yaygın kullanılan kimlik avı saldırısı biçimlerinin en aza indirilmesi, bilinen kötü IP adreslerinin filtrelenmesi ve kötü niyetli çevrimiçi etkinliklerin aktif olarak engellenmesi yer almaktadır. Temel siber güvenlikteki gelişmeler, İngiltere'nin en yaygın kullanılan siber tehditlere karşı dayanıklılığını artıracaktır.*

1.9. İngiltere'nin siber güvenlik ortamındaki otorite, bilgi paylaşımı, sistemik zayıflıkları ele alma ve kilit ulusal siber güvenlik konularında liderlik sağlama konusunda bir Ulusal Siber Güvenlik Merkezi (NCSC) kurduk.

1.10. Silahlı Kuvvetlerimizin esnek olmasını ve siber tehditlere rağmen küresel manevra özgürlüğünü sürdürmeye devam ederek ağlarını ve platformlarını korumak için ihtiyaç duydukları güçlü siber savunmalara sahip olmasını sağlayacağız. Askeri Siber Güvenlik Operasyon Merkezimiz NCSC ile yakın bir şekilde çalışacak ve önemli bir ulusal siber saldırı durumunda Silahlı Kuvvetlerin yardımcı olmasını sağlayacağız.

1.11. Siber saldırılara, saldırgan bir siber yetenek de dahil olmak üzere, en uygun olanı kullanarak, herhangi bir saldırıya yanıt verdiğimiz şekilde yanıt verme imkânımız olacak.

1.12. İngiltere Hükümetinin, okullardan üniversitelere ve işgücüne kadar siber güvenlik becerilerinin yetersizliğini giderecek programlara yatırım yapmak için yetki ve etkisini kullanacağız.

1.13. En gelişmiş siber ürünlerin ve dinamik yeni siber güvenlik şirketlerinin gelişimini teşvik etmek için iki yeni siber yenilik merkezi açacağız. Savunma ve güvenlik alanındaki yenilikçi tedarikleri desteklemek için 165 milyon sterlinlik Savunma ve Siber İnovasyon Fonu'nun bir kısmını tahsis edeceğiz.

1.14. İngiltere'nin siber güvenliğini önemli ölçüde dönüştürmek için önümüzdeki beş yıl boyunca toplam 1.9 milyar sterlin yatırım yapacağız.

Belgede Birleşik Krallık'ın 2021 için vizyonu; "*İngiltere, dijital dünyada müreffeh ve kendinden emin, siber tehditlere karşı güvenli ve dayanıklıdır.*" şeklinde belirlenmiştir. Plan temel olarak 4 eylem üzerine kuruludur. Eylemleri ve alt eylemleri aşağıda sıralamak mümkündür (İngiltere, 2016):

Savunma: Bu stratejinin unsurları; kamusal, ticari ve özel alanlardaki iletişim altyapılarının, verilerinin ve sistemlerinin siber saldırılara karşı sağlam ve korunaklı olmasını sağlamayı amaçlamaktadır. Her siber saldırıyı durdurmak asla mümkün olmamasına rağmen (tıpkı her suçu durdurmanın mümkün olmadığı gibi) siber olaylara maruz kalınma olasılığını önemli ölçüde azaltacak, bilgi ve sırları koruyacak savunma katmanları oluşturabilir. Devletler ile iyi siber güvenlik uygulamaları arasındaki işbirliğini teşvik etmek, aynı zamanda kolektif güvenliğimizin de çıkarlarıdır. Hükümet, vatandaşların, işletmelerin, kamu ve özel sektör kuruluşlarının ve kurumlarının kendilerini savunmak için doğru bilgilere erişmelerini

sağlamak için önlemler alacağını taahhüt etmiştir. Ulusal Siber Güvenlik Merkezi, tehdit istihbaratı ve bilgi güvencesi için hükümette birleşik bir tavsiye sağlayacak, siber savunma için özel rehberlik sunacak ve siber uzaydaki büyük olaylara hızlı ve etkin bir şekilde yanıt verilmesini sağlayacaktır. Aktif Siber Savunma Mekanizması (ACD), bir ağdır ve tüm sistemi saldırılara karşı daha sağlam kılmayı, güçlendirmeyi ve güvenlik önlemlerini uygulamayı ifade eder. ACD'yi yaparken, Hükümet "*Aktif Siber Savunma*" başlığı altında şunları amaçlamaktadır (İngiltere, 2016):

1. Birleşik Krallık ağlarının direncini artırarak devlet destekli siber korsanlar ve siber suçlular için İngiltere'yi daha zor bir hedef haline getirmek;
2. Hackerlar ve mağdurları arasında kötü amaçlı yazılım iletişimini engelleyerek İngiltere ağlarında yüksek hacimli / düşük karmaşıklığa sahip kötü amaçlı yazılımları engellemek;
3. Devlet destekli veya bireysel siber suç tehditlerinin etkilerini azaltmak ve savunmanın kabiliyetini, kapsamını ve ölçeğini geliştirmek;
4. İnternet ve telekomünikasyon trafiğini, kötü niyetli aktörlere karşı korumak;
5. İngiltere'nin siber tehditlere karşı kritik altyapısını ve vatandaşlara yönelik hizmetlerini sağlamlaştırmak;
6. Her türlü saldırganların iş modelini bozmak, onları hayal kırıklığına uğratmak ve saldırılarının neden olabileceği zararı azaltmak olarak belirlenmiştir. Bunun yanı sıra İngiltere sonuçlara yönelik ilerlemeyi değerlendirerek etkili bir kontrol mekanizması geliştirmeyi hedeflemiştir.

"*Daha Güvenli İnternet Kurmak*" alt eylemiyle İngiltere, 2021'e kadar kullanıma sunulan çevrimiçi ürün ve hizmetlerin çoğunun, "*varsayılan olarak güvenli*" hale geleceğini tahmin edip tüketiciler veya bireyleri yani siber uzaya en güvenli şekilde girmek isteyen tüketicileri otomatik olarak korumayı hedeflemektedir.

"*Devlet Koruma*" alt eyleminin amaçlarını ise aşağıdaki gibi sıralamak mümkündür:

1. Vatandaşlar devletin çevrimiçi hizmetlerini güvenle kullanacağına: hassas bilgilerinin güvende olduğuna ve ardından hassas bilgilerini güvenli bir şekilde çevrimiçi olarak sunulduğuna ilişkin güven kazanması;

2. Hükümet, tüm devlet kollarının ağlarını, verilerini ve hizmetlerini güvence altına alma yükümlülüklerini anlamalarını ve yerine getirmelerini sağlamak için en uygun siber güvenlik standartlarını belirlemek ve bunlara uymak;
3. Hükümetin en yüksek sınıftakiler de dahil olmak üzere kritik varlıkları siber saldırılara karşı korumak.

"*Kritik Ulusal Altyapı ve Diğer Öncelik Sektörlerin Korunması*" alt eyleminin amacı İngiltere'nin en önemli kuruluşlarının ve şirketlerin siber saldırı karşısında yeterince güvenli ve esnek olmasını sağlamaktır. Hükümet, hem bu şirketlerin hem de örgütlerin karşılaştıkları tehditlerle ve saldırılarının sonuçlarıyla orantılı destek ve güvence sağlayacaktır.

"*Kamu ve Özel Sektör Davranışlarının Değiştirilmesi*" alt eylemiyle büyüklük veya sektörden bağımsız olarak bireylerin ve kuruluşların, kendilerini ve müşterilerini siber saldırıların neden olduğu zararlardan korumak için uygun adımları atmalarını sağlamak amaçlanmıştır.

"*Olayların Yönetimi ve Tehditlerin Anlaşılması*" alt eyleminin 3 amacı aşağıda sunulmuştur:

1. Hükümet, tehdit ve eylemlerin daha iyi anlaşılması, farkındalığın artırılması ve olay yönetimine tek ve birleşik bir yaklaşım sunacaktır;
2. Mağdur profiline göre uyarlanmış olayları rapor etmek için net süreçler tanımlanması;
3. En yaygın siber olayları önleyecek ve olay öncesini anlamak için etkili bir bilgi paylaşım yapısı kurulacaktır.

Caydırıcılık: Ulusal Güvenlik Stratejisi, savunma ve korunmanın caydırıcılıkla başladığını belirtmiştir. Siber tehditlere karşı güvenli ve dayanıklı, dijital dünyada müreffeh ve kendinden emin bir ulus vizyonunu gerçekleştirmek için Hükümete ve çıkarlarına zarar verme olasılığı olanların caydırılması amaçlanmıştır. Bunu başarmak için siber güvenlik seviyelerini yükseltmeye devam etmeleri gerektiği ve böylece siber uzayda saldırmak isteyenlerin önlenmesi hedeflenmiştir. Küresel ittifaklar kurmaya ve uluslararası hukukun siber dünyaya uygulanmasını desteklemeye devam edeceklerini ve ayrıca, siber alanda tehdit edenlerin faaliyetlerini ve güvendikleri altyapıyı daha aktif olarak bozmayı taahhüt etmiştir. Alt eylemler ise aşağıdaki gibidir:

1. *Tehlikedeki Siber Güvenliğin Rolü:* Caydırıcılık ilkeleri, fiziksel alanda olduğu gibi siber alanda da uygulanabilir. İngiltere, yeteneklerini tüm yelpazesinin rakipleri caydırmak ve ülkeye saldırma fırsatlarını engellemek üzerine hedeflemiştir. İngiltere'yi daha zor bir hedef haline getirecek, faydaları azaltacak ve maliyetleri yükseltecek (siber güvenlik ve caydırıcılığa yönelik kapsamlı bir ulusal yaklaşım izlemek amaçlanmış) politik, diplomatik, ekonomik veya stratejik hedefler belirlenmiştir.
2. *Siber Suçun Azaltılması:* Siber suçluların İngiltere'yi hedeflemekten alıkoymak ve İngiltere'ye saldırmaya devam edenlerin aralıksız takip edilmesi ve siber suçların İngiltere ve çıkarları üzerindeki etkisini azaltmak hedeflenmektedir.
3. *Yabancı Düşmanlara Karşı Koymak:* Tehditlere karşı önlem almak ve gelecekte siber olayların sayısını ve ciddiyetini azaltmak için proaktif, iyi kalibre edilmiş ve etkili bir yaklaşımın alınmasını sağlamak için her bir rakip için stratejilerini, politikalarını ve önceliklerini belirlemek amaçlanmıştır.
4. *Terörizmin Önlemesi:* Teröristlerin (şu anda İngiltere ulusal güvenliğini tehdit edebilecek kapasiteye sahip olan ve geliştirmeyi hedefleyenler) siber kullanım tehdidini siber aktörlerin belirlenmesi ve engellenmesi yoluyla hafifletmek hedeflenmiştir.
5. *Ülke Yeteneklerini Geliştirme - Saldırgan Siber Yaklaşım:* Hem caydırıcı hem de operasyonel amaçlarla, ulusal ve uluslararası hukuka uygun olarak kullanılabilecek uygun siber yeteneklere sahip bir İngiltere hedeflenmiştir.
6. *Ülke Yeteneklerini Geliştirme – Şifreleme Yaklaşımı:* İngiltere'nin, ulusal güvenliği için hayati önem taşıyan şifreleme yetenekleri üzerinde her zaman politik kontrol sahibi olmak ve bu nedenle de İngiltere sırlarını koruma yolunun güvenilmesini sağlamak amaçlanmıştır.

Geliştirmek: İngiltere siber tehditten korunmak için ihtiyaç duyduğu araçları ve yetenekleri nasıl kazanacağını ve güçlendireceğini ana hedeflerinden biri olarak belirlemiştir. Bu yaklaşımı kendi göbek bağını kendisi kesmeye çalışmak olarak tanımlamak mümkündür. İngiltere daha yetenekli ve nitelikli siber güvenlik uzmanlarına ihtiyaç duymaktadır. Hükümet kilit siber güvenlik rolleri için talep ve arz arasındaki artan boşluğu kapatmak, bu eğitim ve öğretim alanına yenilenmiş gücü enjekte etmek için harekete geçeceğini ifade etmiştir. Bu uzun vadeli, dönüştürücü bir amaçtır ve bu strateji, zorunlu olarak 2021'in ötesinde devam edecek amaçlardan biri olarak belirlenmiştir. Nitelikli bir işgücü, hayatidir

ve dünya lideri bir siber güvenlik ticari ekosisteminin can damarıdır. Bu ekosistem, siber start-up'ların gelişmesini sağlayacak ve ihtiyaç duydukları yatırım ve desteği hükümetten alacaklardır. Bu yenilik ve canlılık ancak özel sektör tarafından sağlanabileceğini, hükümetin doğrudan destek sunacağı vurgulanmıştır. Alt eylemler ise aşağıdaki gibidir:

1. *Siber Güvenlik Becerilerinin Güçlendirilmesi:* İngiltere mümkün olan en iyi seviyelerde yetiştirilen siber güvenlik yeteneklerinin sürekli olarak kullanılmasını amaçlamaktadır. Çevrimiçi olarak güvenli bir şekilde çalışabilmesi için nüfus ve işgücünde ihtiyaç duyulan siber güvenlik becerilerini de aktarmak hedeflenmiştir. Siber uzmanların, yalnızca etkili bir şekilde eğitilmemiş aynı zamanda ulusal güvenliği korumaya hazır olmaları ve alanın askeri operasyonlar üzerindeki etkisinin anlaşılması arzulanmaktadır.
2. *Siber Güvenlik Sektöründe Büyümenin Desteklenmesi:* İngiltere'de siber güvenlik ekosistemi oluşturmak amacıyla büyüyen, yenilikçi ve gelişen sektör yaratılması hedeflenmiştir. Bunun için güvenlik şirketlerini geliştirmek yönünde gereken yatırımlar sağlanacak; hükümet, üniversite ve özel sektörden gelen en iyi beyinlerle yakın işbirliği geliştirecek ve sektör müşterileri bilgilendirilecektir.
3. *Siber Güvenlik Bilim ve Teknolojisinin Teşvik Edilmesi:* 2021 yılına kadar, İngiltere siber bilim ve teknolojide bir dünya lideri olmayı hedeflemektedir. Üniversiteler ve sanayi sektörü arasındaki esnek ortaklıkların araştırmayı ticari olarak başarılı ürün ve hizmetlere dönüştürmesi ve finans sektörü gibi olağanüstü ulusal güce sahip alanlar dahil olmak üzere yenilikçi mükemmellik konusundaki itibarını koruyacağı beklenmektedir.
4. *Etkili Ufuk Açıcı Araştırmalar Yapılması:* Hükümet, ufuk tarama programlarıyla sıkı bir siber risk değerlendirmesi yapmayı ve bunun siber güvenlik ile diğer teknoloji politikası geliştirme alanlarında kullanılmasını planlamaktadır. Ortaya çıkan zorlukların ve fırsatların bütünsel bir değerlendirmesini sağlamak için ulusal güvenlik ile diğer politika alanları arasında ufuk taraması yapılması hedeflenmiştir.

Uluslararası eylem: İngiltere, ekonomik ve sosyal refahının giderek artan oranda, ülke sınırlarının ötesine geçen ağların açıklığına ve güvenliğine bağlı olduğunun farkındadır. Siber konularda uluslararası işbirliği, daha geniş küresel ekonomik ve güvenlik tartışmalarının önemli bir parçası haline gelmiştir. İngiltere müttefikleriyle birlikte, kurallara dayalı uluslararası sistemin bazı unsurlarının yürürlükte kalmasını sağlamada başarılı

olduğunu iddia etmektedir. Bununla birlikte, ulusal güvenliği bireysel hak ve özgürlüklerle uzlaştırmanın ortak zorluğunun nasıl ele alınacağına dair artan bir bölünmeyle karşı karşıya kaldıklarını ifade etmiştir. Eylemin amacı ise; ücretsiz, açık, barışçıl ve güvenli bir siber alanın uzun vadeli geleceğini korumak, ekonomik büyümeyi teşvik etmek ve ulusal güvenliği desteklemek olarak açıklanmıştır. İngiltere internetin çok paydaşlı modelini savunacak; veri lokalizasyonuna karşı çıkacak ve ortaklarıyla birlikte kendi siber güvenliğini geliştirecektir. Bu durum denizaşırı kökenli olan tehdidi azaltmak için, siber suç, siber casusluk ve yıkıcı siber faaliyetlerde bulunanların karar vermelerini etkilemeye çalışılması ve uluslararası işbirliğini desteklenmesi ile mümkün görünmektedir.

Ölçüm başlığı altında ise elde edilmesi beklenen sonuçlara yönelik ilerlemeyi ölçmek ve söz konusu ölçümün titiz ve kapsamlı kriterler ile yapılması hedeflenmiştir. Özet olarak 2016-2021 dönemini kapsayan eylem planındaki hedef ve çıktılar aşağıda sunulmuştur (İngiltere, 2016):

Çizelge 4.9. İngiltere'nin siber güvenlik eylemleri ve beklenen çıktıları

Ana Eylem	Stratejik Çıktı
Caydırıcılık	İngiltere, rakiplerinin siber faaliyetlerinden kaynaklanan tehditleri etkili bir şekilde tespit etme, araştırma ve bunlara karşı koyma kabiliyetine sahiptir.
Caydırıcılık	Siber suçların İngiltere ve çıkarları üzerindeki etkisi önemli ölçüde azaltılır ve siber suçlular İngiltere'yi hedeflemekten alıkoyulur.
Savunma	İngiltere, verilerini siber rakiplerine karşı korur ve bunun için siber olayları etkin bir şekilde yönetir.
Savunma	Aktif bir siber savunma endüstrisi ile olan ortaklıklar, büyük çapta kimlik avı ve kötü amaçlı yazılım saldırılarının artık etkili olmadığı anlamına gelmektedir.
Savunma	İngiltere, siber güvenliğe sahip ve bunlara varsayılan olarak etkinleştirilmiş teknoloji ürünleri ve hizmetleri sayesinde daha güvenlidir.
Savunma	Hükümet ağları ve hizmetleri, ilk uygulamalarından itibaren mümkün olduğu kadar güvenli olacaktır. Halk, devletin dijital hizmetlerini güvenle kullanabilecek ve bilgilerinin güvende olduğuna emin olacaktır.

Çizelge 4.9. (devam) İngiltere'nin siber güvenlik eylemleri ve beklenen çıktıları

Ana Eylem	Stratejik Çıktı
Savunma	Büyük ve küçük, İngiltere'deki tüm kuruluşlar, siber risklerini etkin bir şekilde yönetiyor. Kuruluşlar doğru düzenleme ve teşvik ile desteklenmiş yüksek kaliteli tavsiyelerle destekleniyor.
Gelişim	İngiltere, ulusal güvenlik taleplerini karşılayabilecek siber güvenlik sektörü geliştirmek ve sürdürmek için yeterli ekosisteme sahip.
Gelişim	İngiltere, hem kamu hem özel sektör hem de savunma sektöründe artan dijital ekonominin taleplerini karşılamak için sürdürülebilir siber yetenekli profesyonel kaynağına sahiptir.
Gelişim	İngiltere, siber güvenlik araştırma ve geliştirmesinde küresel bir lider olarak kabul edilir. İngiltere endüstrisi ve üniversite alanındaki yüksek uzmanlık seviyesine sahiptir.
Gelişim	İngiltere hükümeti, gelecekteki teknolojiler ve tehditlerden önce politika uygulamalarını planlıyor. Bu durum "*geleceğe yöneliktir*".
Uluslararası Eylem ve Etkileme	İngiltere'ye karşı yurtdışından gelen tehdit, uluslararası uzlaşma, barışçıl girişimler ve güvenli bir siber ortamdaki sorumlu devlet davranışları sayesinde azaldı.
Kesişen Eylem	İngiltere politikaları, organizasyonları ve yapıları, ülkenin siber tehditlere verdiği yanıtın tutarlılığını ve etkinliğini en üst düzeye çıkarmak için basitleştirmiştir.

Özetle İngiltere oldukça kapsamlı ve sistematik bir eylem planı hazırlamıştır. 2011-2016 dönemini kapsayan Siber Güvenlik Strateji belgesi yıllık olarak izlenmiş ve raporlanmıştır. Bu durum İngiltere'nin ne kadar ciddi bir işle uğraştığının açık bir göstergesidir. Bunun yanı sıra hükümetçe sahiplenmenin temel bir göstergesi hem sürecin takip edilmesi hem de belgeye çok üst düzeyde katılımdır. İngiltere eski planı döneminde yaklaşık 900 milyon sterlin yatırım yaptığını ifade ederek ilerlemeyi hem finansal hem de nitelik olarak takip etmektedir. Böylece, İngiltere'nin hedeflerini; siber suçun tanımlanması, vatandaş farkındalığının yükseltilmesi, kritik bilgi altyapısının koruması, uluslararası işbirliğine gidilmesi, kamu-özel sektör ortaklığının kurulması, olay müdahale kabiliyetinin kazanılması, kamu kurumları arasında kurumsal bir işbirliğinin sağlanması, temel güvenlik gereksinimlerinin belirlenmesi, olay raporlama mekanizmalarının kurulması, Ar-Ge'ye

yapılan yatırımların yükseltilmesi, siber güvenlik alıştırmalarının desteklenmesi ve eğitim ve öğretim programlarının güçlendirilmesi olarak sıralanabilir. Kontrol sisteminde kurulmuş olması İngiliz siber güvenlik eylem planını diğer ülkelerin hem önüne geçirmekte hem de birçok ülkeye örnek olabilecek kapasitesinin bir göstergesidir.

4.10. Danimarka Siber ve Bilgi Güvenliği Stratejisi

Danimarka Siber ve Bilgi Güvenliği Stratejisi 2018-2021 belgesi beş ana bölümden oluşmaktadır. Strateji üç temel sacayağına oturtulmuştur. Bunlar; (1) günlük güvenlik, (2) daha iyi yetkinlikler ve (3) ortak çabalar şeklindedir. Giriş kısmında ülke, dünya ve siber güvenlik ile ilgili tespitler ve değerlendirmeler yapılmıştır. Dünyanın geri kalanıyla ortak olarak, Danimarka'daki teknolojik gelişmeler hızlanıyor. Dahası, Danimarka dijital çözümlerle giderek daha fazla bağlantı kuruyor. Kamu yetkilileri, işletmeler ve vatandaşlar internete ve internetin sağladığı fırsatlara her zamankinden daha bağımlı hale geliyor (Danimarka, 2018).

Vatandaşlar, dijital çözümler aracılığıyla işletmeler ve kamu otoriteleri ile etkileşim kurmaya alışkındır. Veri ve bilgi alışverişinin, bireyin mahremiyetine saygı duyan sorumlu ve güvenli bir şekilde gerçekleştiğine dair temel bir güvene sahiptir. Danimarka hükümeti gelecek birkaç yıl içinde siber ve bilgi güvenliğine 1,5 milyar Euro yatırım yapmayı planlamaktadır (Danimarka, 2018).

Son dönemde siber güvenlik çok daha önemli hale gelmiştir. Eylem planında bu durum "*daha fazla güvenlik açığı*" başlığı altında incelenmiştir. Yetersiz güvenlik kültürü, güvenlik becerilerinin eksikliği ve bilgi eksikliği, kötü niyetli üçüncü şahıslar tarafından istismar edilebilecek önemli bir güvenlik açığı oluşturur. Yetkili makamların ve işletmelerin yöneticilerinin ve çalışanlarının güvenlik davranışı, yeterli düzeyde koruma sağlamak için hayati önem taşımaktadır. Eylem planındaki tespitleri ve değerlendirmeleri aşağıdaki gibi sıralamak mümkündür (Danimarka, 2018):

1. *Kıyaslamalar*: Danimarka hükümeti, önümüzdeki dört yıl içinde bir ülke olarak daha güçlü ve dijital olarak daha güvenli hale gelmek için üç açık kriter belirlemiştir.
   a. *Vatandaşlar ve İşyerleri için Günlük Güvenlik Merkezi:* Hükümet, kritik sektörlerle birlikte, temel toplumsal işlevleri siber saldırılara veya diğer büyük bilgi güvenliği

olaylarına karşı koruyabilmek için tehdit senaryosu geliştikçe teknolojik hazırlığını artırmaktadır.

b. *Daha İyi Yetkinlikler:* Vatandaşlar, işletmeler ve yetkililer gerekli bilgiye erişebilir ve artan siber ve bilgi güvenliği zorluklarının üstesinden gelme yeterliliğine sahiptir.
c. *Ortak Çalışmalar:* Risk temelli güvenlik yönetimi, merkezi hükümet yönetiminin ve kritik sektörlerin yönetiminin ayrılmaz bir parçasıdır. Önemli toplumsal işlevleri sağlayan yetkililer ve işletmeler için siber ve bilgi güvenliği alanında net bir rol ve sorumluluk dağılımı olmalıdır.

Eylem planının ana hedef konuları ve alt hedefleri aşağıda ana başlıklar halinde sunulmuştur (Danimarka, 2018):

1. Günlük Güvenlik
   a. Ulusal bir siber durum merkezi oluşturulacak.
   b. Yetkililerin siber ve bilgi güvenliği konusundaki çalışmaları için minimum gereksinimler belirlenecek.
   c. Siber alandaki düzenleyici girişimler yapılacak.
   d. Merkezi hükümette kritik bilgi ve iletişim sistemleri izlenecek.
   e. Raporlama için ortak dijital portal oluşturulacak.
   f. Bilgi ve iletişim suçlarıyla ilgili davaların işlendiği ulusal merkez kurulacak.
   g. Bu tür saldırılara yanıt olarak bilgi ve iletişim teknolojisi ile ilgili saldırıların önlenmesi ve yaptırım konusunda gelişmiş işbirliği sistemi kurulacak.
   h. Kimlik belgeleri için daha yüksek güvenlik standartları geliştirilecek.
   i. Ulusal bilgi ve iletişim teknolojisi altyapısının iyileştirilmesi önceliklendirilecek.
   j. Merkezi hükümette güvenli iletişim kanalı sağlanacak.
2. Daha İyi Yetkinlikler
   a. Eğitim sistemi aracılığıyla edinilen dijital farkındalık ve dijital yetkinliklerin gelişmesi.
   b. Bilgi portalı kurulacak.
   c. Yeni teknolojiye yönelik araştırma yapılacak.
   d. Danimarka iş dünyasında bilgi ve iletişim teknolojisi güvenliğini artırmak için kurumsal ortaklık kurulacak.

e. Yetkinlik geliştirme ve merkezi hükümette bir güvenlik kültürünün teşvik edilmesi konusunda işbirliği yapılacak.
f. Vatandaşları ve işletmeleri hedefleyen gelişmiş farkındalık teşvikleri sunulacak.

3. Ortak Çabalar
   a. Sektörel düzeyde alt stratejiler ve merkezi olmayan siber güvenlik birimleri kurulacak.
   b. Kritik sektörlerde siber ve bilgi güvenliğini desteklemek için sektörler arası işbirliği yapılacak.
   c. Dış kaynaklı bilgi ve iletişim teknolojisi hizmetleri tedarikçilerinin yönetimi konusunda çalışılacak.
   d. Ulusal koordinasyonun güçlendirilmesi sağlanacak.
   e. Uluslararası işbirliğine artan katılım düzeyi teşvik edilecek.
   f. Siber ve bilgi güvenliğinin mevcut durumunun değerlendirilmesi yapılacak.
   g. Korunmaya değer bilgilere genel bakış yapılacak.
   h. Bilgi güvenliği mimarisi güçlendirilecek.
   i. Veri etiğini ve kişisel verilerin korunmasını sağlamak için ulusal ve uluslararası çabalar geliştirilecek.

Siber güvenlik konusunda günlük sorumluluğu olan makam, büyük bir kaza veya doğal afet durumunda da sorumlu tutulmalıdır. Çünkü yetkili makam her türlü koşulun sorumluluğunu da üstüne almak zorundadır. Normal günlük operasyonlar sırasında uygulanan prosedürler ve sorumluluklar, mümkün olduğu ölçüde, kriz yönetim sisteminde de geçerli olmalıdır. Acil müdahale görevleri, mümkün olduğu ölçüde, yerel olarak ve etkilenen vatandaşlara mümkün olduğunca yakın ve buna göre en düşük uygun ve ilgili organizasyon düzeyinde yönetilmelidir. Yetkililerin, acil durum müdahale planlaması ve kriz yönetimi konusunda diğer yetkililer ve kuruluşlarla işbirliği yapmak ve koordinasyon sağlamak için ayrı bir sorumluluğu vardır. Bilginin net olmadığı veya eksik olduğu durumlarda, acil duruma hazırlık düzeyi çok düşük olmaktan ziyade tercihen çok yüksek olmalıdır. Ayrıca, kaynak israfını önlemek için acil duruma hazırlık düzeyini kolayca ve hızlı bir şekilde düşürmek mümkün olmalıdır. Bunların yanı sıra siber güvenlik alanıyla ilgili olarak sorumluluk ilkesi aşağıdakileri ifade etmektedir (Danimarka, 2018):

- Tüm bakanlar, kendi sorumlulukları dahilinde uygun bir acil durum müdahalesi sağlamalıdır;

- Sektöre özgü sorumluluk, politik veya idari olarak yasaların gerektirdiği tüm kritik işlevleri ve hizmetleri kapsar;
- Yetkililerin acil durum müdahale planlaması, yönetimin genel sorumluluğu üstlendiği, devam eden ve sistematik bir risk değerlendirme sürecini temel almalıdır;
- Kamu yetkilileri, kendi sektörleri için risk senaryosunu düzenli olarak izlemelidir.

Siber ve bilgi güvenliği ile ilgili devam eden çalışmalar, ilgili makamlarla yakından koordine edilmeli ve bunlar arasında bilgi paylaşımına konu olmalıdır. Bu amaçla, sektörlerin, yetkililerin ve işletmelerin çalışmalarını desteklemek için bir dizi girişim başlatılacaktır. Bu girişimler, özellikle bilgi ve iletişim teknolojisi güvenliğiyle ilgili önleyici çalışmalarla ilgili olarak sahada daha yakın ulusal koordinasyonu sağlayacaktır. Danimarka'da siber güvenlik ile ilgili olarak eylem planında Siber Güvenlik Merkezi, Polis, Dijitalleştirme Ajansı, Savunma Birimleri, Danimarka Ticaret Kurumu ve Danimarka Güvenlik ve İstihbarat Servisi yetkili ve sorumlu tutulmuştur (Danimarka, 2018).

4.11. İrlanda'nın Ulusal Siber Güvenlik Stratejisi

İrlanda Ulusal Siber Güvenlik Stratejisi belgesini 2015-2017 dönemi için hazırlamış ve yayınlamıştır. Strateji belgesi 5 ana bölümden oluşmaktadır. Özet ve giriş kısmı detaylı bir şekilde ülke ve plan detayı içermektedir. Ulusal Siber Güvenlik Stratejisi (2015-2017), İrlanda'nın dijital teknolojideki gelişmelerin dinamik ve zorlu bir yönü ile nasıl etkileşimde bulunacağını belirleyerek, İrlanda hükümetinin bilgisayar ağlarının esnek, güvenli ve sağlam çalışmasını kolaylaştırmaya yönelik yaklaşım sunmaktadır (İrlanda, 2015).

Strateji özellikle, İletişim, Enerji ve Doğal Kaynaklar Dairesi bünyesinde Ulusal Siber Güvenlik Merkezi'nin kurulmasını içermektedir. Bu organın üç ana sorumluluk alanıyla nasıl etkileşimde bulunacağı detaylandırılmıştır. Bunlar; devlet ağları, kişisel ve iş sistemleri ve kritik ulusal altyapının korunmasıdır (İrlanda, 2015).

Ulusal Siber Güvenlik Stratejisi (2015-2017), İrlanda'nın dijital teknolojideki gelişmelerin dinamik ve zorlu bir yönü ile nasıl ilgileneceğini ortaya koymaktadır. İnternet teknolojilerinin ve bilgi ve iletişim teknolojilerinin daha genel olarak hükümetin, iş dünyasının ve bireylerin kendilerini güvende hissetmeleri, katılmalarını ve bilgi vermelerini sağlamak için kullanılması dönüştürücü olmuştur. 2013 yılında Dünya Ekonomik Forumu,

2014 Ulusal Risk Değerlendirmesinde ulusal düzeyde yansıtılan bir bulgu olarak, siber ile ilgili tehditleri hem etki hem de olasılık açısından tüm küresel risklerin en yükseklerinden biri olarak tanımlanmıştır. Bu Strateji, devlet, kamu ve özel ortaklar, akademi ve sivil toplum arasında görev paylaşımı ve güven ilişkileri oluşturmaya vurgu yaparak, siber uzayın güvenli, emniyetli ve güvenilir kalmasını sağlamak için hükümetler arası bir çerçeve sunmaktadır. Olaylar ve teknoloji gelişmeye devam ettikçe, esneklik gerekli olacak ve Stratejinin uyarlanabilir ve esnek bir şekilde uygulanmasına yansıtılacaktır(İrlanda, 2015).

Strateji belgesinin 4 ana sacayağı vardır. Bunlar insanlar, ekonomi, risk ve hükümettir (İrlanda, 2015).

- *Vatandaşlar açısından:* Siber güvenlik, ağların, cihazların veya verilerin güvenliğini artırmak için teknik çözümlerin uygulanmasıyla sınırlı değildir. Aksine, zorluğun doğası öyledir ki, hükümetler tarafından zamanında ve uygun düzenleyici yanıtların verilmesi, devam eden bir teknolojik adaptasyon ve iyileştirme sürecini teşvik etmek ve konunun önemi hakkında kültürel bir anlayışı teşvik etmek dahil olmak üzere çeşitli önlemler gereklidir. Bilgi odaklı bir toplum olarak İrlandalı vatandaşlar sosyalleşir, eğlendirir, iletişim kurar, öğrenir, işlem yapar ve değişen derecelerde çevrimiçi olarak yaşar. Bu yaşam tarzını ve bireylerin kişisel verilerini korumak, refah, sosyal gelişme ve insan haklarının korunması için bir ön koşuldur.
- *Ekonomi açısından:* İrlanda ekonomisi, sürdürülebilir büyüme ve gelişme için etkili ve güvenli dijital altyapılara bağlıdır. Dijital ekonomi, ulusal GSYİH'nın %5'ine katkıda bulunuyor ve yılda yaklaşık %20 oranında büyümektedir. Elektrik, gaz, finansal hizmetler ve su temini gibi çok çeşitli kritik ekonomik altyapı da dahil olmak üzere, operasyonları için bilgi ve iletişim teknolojilerine güvenmeyen birkaç sektör vardır. Eyalette gelişen bulut bilişim ve büyük veri sektörü temelinde İrlanda için gerçek bir siber güvenlik merkezi olma potansiyeli var.
- *Riskler açısından:* Cihazların son derece yaygın bir şekilde kullanılmasıyla birlikte, ağa bağlı teknolojilerin kullanıldığı çeşitli yollar, tehdit türü açısından çok geniş bir risk yelpazesinin ortaya çıktığı anlamına gelir. Tehdit türü, tanıtım oluşturma, bankacılık veya diğer bilgileri elde etme, büyük ölçekli veri hırsızlığı ve hatta bilgi ve iletişim teknolojileri sistemlerinin sabotajına kadar nispeten düşük seviyeli girişimlerden oluşur. Bazı durumlarda, saldırılar ekipman ve altyapıya fiziksel zarar vermiştir. Bu tür saldırıların kökenleri, yalnız bireylerden suç gruplarına kadar

uzanmaktadır ve bazı durumlarda büyük olasılıkla istihbarat toplamak veya alt yapıya zarar vermek isteyen ulus devletleri içerir. Çok sayıda durumda, bireyler, şirketler ve devlet için riskler benzerdir ve iş sürekliliği planlaması, yazılımı güncel tutma veya bireylerin çevrimiçi olarak ortaya çıkan risklerin farkındadır ve bunlarla başa çıkmak için eğitilmiştir.

- *Hükümet açısından:* İrlanda hükümeti tarafından ekonomik ve sosyal büyüme için bilgi sistemlerinin kullanımını optimize eden ve teşvik eden bir dizi girişim başlatılmıştır. Bunlar;
  - ✓ Hükümetin Ulusal Geniş Bant Planı, tüm vatandaşların ve işletmelerin güvenilir yüksek hızlı geniş banda erişimini sağlamayı ve yeni iş, ekonomik ve sosyal fırsatlar yaratmayı amaçlamaktadır.
  - ✓ İrlanda'nın Haziran 2013'te yayınlanan Ulusal Dijital Stratejisi "*Dijitalle Daha Çok Şey Yapmak*", çevrimiçi katılımın kapsamını ve kalitesini artırmaya odaklanmıştır.
  - ✓ e-Devlet Stratejisi 2012-2015 raporu (Nisan 2012), halkın katılımı ve hizmet sunumu için çevrimiçi kanallara doğru ilerleyen, reformdan geçirilmiş bir kamu yönetimini açıklar.
  - ✓ Ocak 2015'te yayınlanan Kamu Hizmeti BİT Stratejisi, vatandaşlar ve işletmeler için yeni ve gelişmekte olan dijital teknolojilerin yenilikçi kullanımından elde edilen gelişmiş verimliliklerden yararlanmaya odaklanmaktadır.

Kritik Ulusal Altyapı (Critical National Infrastructure/CNI), elektrik, su, ulaşım, telekomünikasyon, ticaret ve sağlık gibi temel hizmetleri kapsamaktadır. Ağların ve bilgi sistemlerinin yakınsaması artık bu hizmetlerin sağlanmasının büyük ölçüde bilgi ve iletişim teknolojilerinin sorunsuz çalışmasına dayandığı anlamına geliyor. 2001 yılından bu yana, Ağ ve Bilgi Güvenliğini geliştirmeyi amaçlayan bir dizi AB ve uluslararası önlem alınmıştır. Bunlar arasında 2005 yılında Avrupa Ağı ve Bilgi Güvenliği Ajansı'nın (ENISA) kurulması, farkındalık artırma etkinliklerinin kolaylaştırılması, eğitim, siber güvenlik uygulamaları ve 2009 Kritik Bilgi Altyapısının Korunmasına İlişkin İletişim gibi politika önerileri ve platformlarının geliştirilmesi yer almaktadır. AB Telekomünikasyon Çerçeve Direktifi (2009/140 / EC) halihazırda telekomünikasyon operatörleri için zorunlu ve güvenlik gereksinimleri sağlamaktadır. Direktifin ayrıca aşağıdakiler de dahil olmak üzere bir dizi özel gerekliliği vardır (İrlanda, 2015):

- Ulusal düzeyde bir stratejinin geliştirilmesi;

- Ulusal yetkili makam veya makamların atanması;
- Bir veya daha fazla ulusal bilgisayar güvenliği olay müdahale ekibinin kurulması ve bunlara kaynak sağlanması;
- Üye Devletler arasında stratejik ve operasyonel seviyelerde işbirliği düzenlemelerinin geliştirilmesi;
- Enerji, ulaştırma, bankacılık, finansal hizmetler ve sağlık sektörlerinde bilgi toplumu hizmetleri sağlayan veya kritik altyapıyı işleten belirli teşebbüsler için ağ ve bilgi güvenliği olaylarının raporlanması ve risk yönetimi ve güvenlik gerekliliklerine uygunluk.

Devletin rolü, ağları ve altyapı işletmelerini ve özel kişileri korumak için sağlam, istikrarlı ve tutarlı bir düzenleyici çerçeve oluşturmak ve özel alanda öz denetimi desteklemektir. Bunda izlenecek ilkeler aşağıda belirtilmiştir (İrlanda, 2015):

- *Hukukun Üstünlüğü:* Hukukun üstünlüğünü uygulamaya odaklanılacağı ve İrlanda vatandaşlarının Anayasa ve Avrupa İnsan Hakları Sözleşmesi kapsamındaki haklarının her zaman korunmasının sağlanacağı ifade edilmiştir.
- *Bağlılık:* Devlet, bilgi ve iletişim teknolojisi sahipleri ve operatörleri, öncelikle sistemlerini ve müşterilerinin bilgilerini korumakla sorumludur.
- *Risk Temelli Yaklaşım ve Orantılılık:* Koruma düzeyini artırmaya yönelik tedbirler, bireyler, işletmeler, kamu sektörü organları ve toplu bir bütün olarak devlet olarak karşı karşıya olduğumuz risk ve tehditlerin değerlendirilmesiyle bilgilendirilmelidir. Ayrıca, bu tür önlemlerin karşı karşıya olduğumuz ilgili riskler ve tehditlerle orantılı olması gerekecektir. Hedefler;
  - ✓ Önemli ekonomik sektörlerde ve özellikle kamu sektöründe kritik bilgi altyapısının dayanıklılığını ve sağlamlığını geliştirmek.
  - ✓ Siber alanın açık, güvenli, üniter ve özgür kalmasını, ekonomik ve sosyal kalkınmayı kolaylaştırmasını sağlamak için uluslararası ortaklar ve uluslararası kuruluşlarla ilişki kurmaya devam etmek.
  - ✓ İşletmelerin ve özel bireylerin ağlarını, cihazlarını ve bilgilerini güvence altına alma konusundaki sorumlulukları konusunda farkındalık yaratmak ve bilgilendirme, eğitim ve gönüllü uygulama kuralları aracılığıyla bu konuda onları desteklemek.

- ✓ Devletin, güçlü, orantılı, adil olan ve hassas veya kişisel verilerin korunmasına gereken önemi vererek siber suçla mücadele için kapsamlı ve esnek bir yasal ve düzenleyici çerçeveye sahip olmasını sağlamak.
- ✓ Kişisel veri sahipleri için geçerli olan düzenleyici çerçevenin sağlam, orantılı ve adil olmasını sağlamak.
- ✓ Kamu idaresi ve özel sektör genelinde siber olayların acil durum yönetimine tam anlamıyla dahil olmak için kapasite oluşturmak.

Eylem planında belirlenen ana ve alt hedefler aşağıda sunulmuştur (İrlanda, 2015):

1. *Ulusal Siber Güvenlik Merkezinin Kurulması*: İletişim, Enerji ve Doğal Kaynaklar Departmanı bünyesinde Ulusal Siber Güvenlik Merkezi (National Cyber Security Centre/NCSC) resmi olarak kurulacaktır. NCSC, öncelikli olarak devlet ağlarının güvenliğini sağlamaya, sektöre ve bireylere kendi sistemlerini korumalarında yardımcı olmaya ve kritik ulusal altyapıyı korumaya odaklanarak, siber güvenlik etrafında kapsamlı bir görevler dizisi gerçekleştirecektir.
2. *Kamu Kurumları İçin Ağ ve Bilgi Güvenliği*: Kapsamlı bir olay raporlama ve sorun giderme politikası dahil olmak üzere Devlet Daireleri ve Ajansları tarafından kullanılan ağ ve bilgi güvenliğini iyileştirmek için bir dizi önlem alınacaktır.
3. *Birincil Mevzuat Aracılığıyla 2016/1148 Ağ ve Bilgi Sistemleri Direktifine Tam Olarak Uyulacak*: Ulusal siber güvenlik düzenlemelerini yürürlüğe koymak ve ağ ve bilgi güvenliği ile ilgili önerilen Avrupa Birliği Direktifini aktarmak için birincil mevzuat geliştirilecek. Bu süreç, düzenleyici etki analizi ve yasal incelemeyi içerecek şekilde şeffaf ve istişari bir tarzda gerçekleştirilecektir.
4. *Tutarlı Uluslararası Angajman*: İnternet yönetişiminin geleceği konusundaki küresel tartışma bağlamında da dahil olmak üzere, ağ ve bilgi güvenliği konusunda Avrupa ve küresel tartışmalara katılmaya devam edilecektir. Çevrimiçi temel hakların korunmasını tam olarak kapsayan, ekonomik ve sosyal kalkınmayı kolaylaştırmaya devam eden güvenli, esnek bir internet mimarisine duyulan ihtiyaç vurgulanmaya devam edilecektir.
5. *Ulusal Güvenlik ve Kontrol*: Kontrol ve güvenlik hizmetleri sağlama sorumluluklarının kabulünde, önleyici ve soruşturma stratejileriyle ilgili uygun tavsiye ve rehberlik sunabilecek bir konumda olunacağı öngörülmektedir. Ayrıca, ortaya çıkan tehditleri, güvenlik açıklarını ve en iyi uygulama önleyici tedbirleri

belirlemede diğer güvenlik hizmetleriyle irtibat ilişkilerinden yararlanabilecek bir yapı oluşturulacaktır.

6. *Siber Suçla Mücadele*: Adalet ve Eşitlik Bakanı, Budapeşte Siber Suçlar Konvansiyonu ve 2013/40 / EU Direktifi'nin bilgi sistemlerine yönelik saldırılara ilişkin hükümlerini yürürlüğe koymak için mevzuat getirecektir. Söz konusu mevzuatın uygulanması konusunda tanınmış yasal ve düzenleyici kurumlarla yakın çalışmalara devam edilecektir.
7. *Sivil-Askeri İşbirliği*: Savunma Kuvvetleri, kendi ağlarını ve kullanıcılarını korumak amacıyla siber güvenlik alanında bir kabiliyete sahiptir. Teknik beceri setlerinin geliştirilmesi, teknik bilgi paylaşımı ve tatbikata katılım gibi alanlarda NCSC ve Savunma Kuvvetleri arasında halihazırda güçlü bir işbirliği kültürü vardır. Bu düzenlemeler, ulusal bir siber olay veya acil durum anında teknik uzmanlığın paylaşılmasına yönelik bir mekanizma da içerecek olan Savunma Bakanlığı ile bir Hizmet Seviyesi Anlaşması yoluyla resmileştirilecektir.
8. *Kritik Altyapıların Korunması*: Devlet Acil Durum Planlama Görev Gücü ve Savunma Bakanlığı Acil Durum Planlama Ofisi tarafından denetlenen ulusal acil durum yönetim sistemi dahil olmak üzere, kritik ulusal altyapının korunmasında merkezi bir rol oynamaya devam edilecektir. Bu itibarla, İletişim, Enerji ve Doğal Kaynaklar Bakanlığı, bilgi ve iletişim teknolojilerin başarısızlıkları veya saldırıları ile ilgili acil durumlar için Sorumlu Devlet Departmanı olarak çalışacak ve olayların siber içerikli olabileceği durumlarda diğer departmanlara ikincil bir rol oynayacaktır.
9. *Bilgi Paylaşımı Politikası*: Tehdit ortamının dinamik doğası, tüm paydaşlar arasında bilgiye açık, hızlı erişimin ve paylaşımın kritik olduğu anlamına gelir. Diğer ülkelerdeki benzer kuruluşlarla ve Avrupa Ağı ve Bilgi Güvenliği Ajansı ENISA ile güçlü ikili ilişkiler geliştirmektedir. Aynı şekilde, birimin diğer kamu sektörü organları ve endüstri ile resmi ve aktif bir bilgi paylaşım politikası uygulanacaktır.
10. *Sanayi / KOBİ'ler İçin Eğitim ve Öğretim Faaliyetleri*: Vatandaşların ve Küçük ve Orta Ölçekli İşletmelerin (KOBİ) çevrimiçi ortamda kendilerini daha iyi korumalarına yardımcı olmak için gözden geçirilmiş "*Bilgi ve İletişimi Güvenli Hale Getir*" web sitesinden başlayarak bir eğitim ve öğretim programı geliştirilecektir. Ayrıca, kritik ulusal altyapı sahipleri ve kamu sektörü kuruluşları için uluslararası meslektaşlar ve akademik sektör ile ortaklaşa yapılandırılmış bir tatbikat programı geliştirilecektir.

11. *Kamu Bilincinin Oluşturulması*: Eğitim sistemi, endüstri ile işbirliği ve Avrupa Siber Güvenlik Ağı gibi etkinliklerin tanıtımı yoluyla toplumda bir siber güvenlik kültürü geliştirmek için çalışılacaktır.
12. *Üçüncü Kademe Kurumlarla İlişkiler*: Bilgi, deneyim ve en iyi uygulama paylaşımına yardımcı olmak ve bu sektörde gelişen araştırma gündemini desteklemek için "*Mutabakat Muhtırasını*" kullanarak üçüncü düzey kurumlarla bu tür ortaklıkları geliştirmeye ve derinleştirmeye devam edilecektir.

4.12. Yunanistan'ın Ulusal Siber Güvenlik Stratejisi

Yunanistan'ın Ulusal Siber Güvenlik Strateji üç ana bölümden oluşmaktadır. Strateji belgesi geniş bir literatür girişi ile başlayıp hedefler ile devam etmekte ve sonuç ile nihayete ermektedir. Strateji belgesi, Yunan Devletinin siber uzay güvenliği ile ilgili merkezi planlamasının geliştirildiği Ulusal Siber Güvenlik Stratejisini açıklamaktadır. İnternet ve BİT kullanımının kamu ve özel sektör faaliyetlerinin her alanında artmaya devam ettiği göz önüne alındığında, güvenli bir çevrimiçi ortam, altyapı ve hizmetlerin kurulmasına özel önem verilmelidir. Vatandaşların güvenini artırarak onları yeni dijital ürün ve hizmetlerden daha fazla yararlanmaya yönlendirilmelidir. Bir yandan yeni hizmetlerin ve ürünlerin tanıtımı ile birlikte güvenli bir ortam ve diğer yandan yeni dijital dünyada vatandaşların mahremiyetinin ve haklarının korunması, Yunanistan'da ekonomik kalkınmanın hızlandırılması ve teşvik edilmesi için temel koşullar olarak kabul edilmektedir (Yunanistan, 2017).

Ulusal Siber Güvenlik Stratejisinin uygulanması, Yunanistan'da hem kamu hem de özel sektörde siber uzay güvenliğine dahil olan paydaşlar arasındaki örgütsel ve koordinatif boşluğu doldurmak için oluşturulan Ulusal Siber Güvenlik Otoritesi tarafından gerçekleştirilecektir. Ayrıca, Ulusal Siber Güvenlik Kurumu gerekirse ve en geç üç yılda bir Ulusal Siber Güvenlik Stratejisini değerlendirecek, revize edecek ve güncelleyecektir (Yunanistan, 2017).

Dijital hizmetlerin ve pazarların büyümesi ve korunması, ulusal ekonomi için önemli bir destek direğidir ve hem ulusal hem de Avrupa düzeyinde rekabet avantajı sağlamaktadır. Yunanistan büyümeyi deneyimlemeye ve hem kamu hem de özel sektörde dijital pazarlara, ağlara ve hizmetlere yatırım yapmaya devam ederken, Ulusal Siber Güvenlik Stratejisinin

oluşturulması bir zorunluluk haline gelmiştir. Ulusal Siber Güvenlik Stratejisinin ana ilkeleri şunlardır (Yunanistan, 2017):

- Ulusal, AB ve uluslararası kurallara, standartlara ve iyi uygulamalara uygun olarak düzenlenecek ve vatandaşların, kamu ve özel sektör paydaşlarının uygun şekilde aktif olabileceği ve güvenli bir şekilde etkileşim kurabileceği güvenli ve esnek bir siber alanın geliştirilmesi ve kurulması ana amaçlardandır.
- Kritik altyapı ve operasyonel devamlılığın korunması vurgulanarak, siber saldırılara karşı koruma yeteneklerimizin sürekli iyileştirilmesi ana amaçlardandır.
- Siber saldırı olaylarının etkili bir şekilde ele alınması ve siber uzay tehditlerinin etkisinin en aza indirilmesi için ulusal siber güvenlik çerçevesinin kurumsal koruması ana amaçlardandır.
- Akademik topluluğun ve diğer kamu ve özel sektör paydaşlarının ilgili yeteneklerini kullanarak vatandaşlarda, kamu ve özel sektörde güçlü bir güvenlik kültürünün geliştirilmesi ana amaçlardandır.

Ulusal Siber Güvenlik Stratejisinin hedefleri şu şekilde özetlenebilir (Yunanistan, 2017):

- BİT sistemleri ve altyapısının güvenliğine yönelik tehditlerin önlenmesi, değerlendirilmesi, analizi ve caydırıcılık düzeyini yükseltmek.
- Kamu ve özel sektör paydaşlarının siber güvenlik olaylarını önleme ve yönetme becerilerini geliştirmek ve bir siber saldırı sonrasında BİT sistemlerinin dayanıklılığını ve kurtarılabilirliğini iyileştirmek.
- Ulusal Siber Güvenlik Stratejisinin uygulanmasında yer alan çeşitli kamu ve özel sektör paydaşlarının bireysel yeterliliklerini ve rollerini belirleyerek etkili bir koordinasyon ve işbirliği çerçevesi oluşturmak.
- Yunanistan'ın ulusal güvenliğin artırılmasına yönelik uluslararası siber güvenlik girişimlerine ve uluslararası kuruluşların eylemlerine aktif katılımını sağlamak.
- Tüm sosyal kurumları bilinçlendirmek ve kullanıcıları siber uzayın güvenli kullanımı konusunda bilgilendirmek.
- Ulusal kurumsal çerçeveyi, siber uzay faaliyetleriyle bağlantılı yasadışı eylemlerin etkili bir şekilde ele alınması için yeni teknolojik gerekliliklere ve AB yönergelerine sürekli olarak uyarlamak.

- Güvenlik konularında yenilik, araştırma, geliştirmeyi ve ilgili paydaşlar arasında işbirliğini teşvik etmek.
- En iyi uluslararası uygulamalardan yararlanmak.

Ulusal Siber Güvenlik Stratejisi iki ayrı aşamadan oluşur. Stratejinin ilk aşamada geliştirilmesi ve uygulanması, ikinci aşamada değerlendirilmesi ve gözden geçirilmesi yapılacaktır. Bu aşamalar, ulusal stratejinin önce geliştirilmesi ve uygulanması, ardından önceden belirlenmiş değerlendirme göstergelerine göre değerlendirilmesi ve gerekli görülmesi halinde revize edilmesi, güncellenmesi anlamında sürekli bir yaşam döngüsü belirlenmiştir. Ulusal Siber Güvenlik Stratejisinin uygulanması için gerekli eylemlerin çerçevesi aşağıda tanımlanmıştır (Yunanistan, 2017):

- *Eylem Planına Katılan Paydaşların Belirlenmesi*: Ulusal eylem planı, esas olarak toplumun sorunsuz işlemesi için hayati öneme sahip paydaşlarla ilgilidir. Bu nedenle, ulusal stratejinin geliştirilmesine ve uygulanmasına katkıda bulunacak olan ilgili kamu ve özel paydaşların açıkça belirlenmesi önemlidir.
- *Kritik Altyapının Tanımlanması*: Kritik altyapıların (hem kamu hem de özel sektörde) ve karşılıklı bağımlılıklarının tanımı ve tescili yapılacaktır.
- *Ulusal Düzeyde Risk Değerlendirmesi*: Özet olarak, riskin etkisinin tanımlanmasına, analizine ve değerlendirilmesine dayanan ve kritik altyapının korunması için bir planın belirlenmesine yol açan bilimsel ve teknolojik bir prosedürü takiben ulusal düzeyde bir risk değerlendirme çalışması hazırlanacaktır.
- *Mevcut Kurumsal Çerçevenin Kaydedilmesi ve İyileştirilmesi*: Eylem planını geliştirmenin ve uygulamanın birincil aşaması, mevcut kurumsal çerçevenin ve eylem planının hedeflerini karşılamak için mevcut yapıların kaydedilmesini ve değerlendirilmesi gerekmektedir. Bu değerlendirme kriterleri aşağıdaki gibidir:
  - ✓ Siber güvenlik ile bağlantılı paydaşların mevzuatı, rolleri ve yeterlilikleri (örneğin kişisel verilerin işlenmesi, elektronik iletişim, iletişim gizliliğinin dalgalanması, ağ bütünlüğü ve kullanılabilirliği, vb.).
  - ✓ Sektör bazında uzmanlaşmış düzenleyici eylemler (örn. bankacılık) ve siber güvenliğin iyileştirilmesi üzerindeki etkileri (örn. Yunanistan bankasının düzenlemeleri ve prosedür rolü).
  - ✓ Siber güvenliği korumada operasyonel bir role sahip kamu veya özel sektör yapıları, paydaşları ve hizmetleri (örn. bilgisayar güvenliği olay müdahale ekipleri).

- *Ulusal Siber Uzay Acil Durum Planı*: Ulusal siber güvenlik stratejisine katılan paydaşların kritik bilgi ve iletişim sistemlerinde meydana gelen önemli olayların üstesinden gelmek için yapıları ve önlemleri belirleyecek bir "*Ulusal Siber Uzay Acil Durum Planının*" geliştirilmesi ve bu paydaşların topluma sunduğu hizmetlerin eski haline getirilmesi hedeflenmektedir.
- *Temel Güvenlik Gereksinimlerinin Belirlenmesi*: Ulusal siber güvenlik stratejisine katılan tüm paydaşlar, bilgi ve iletişim sistemlerinin güvenli ve sorunsuz çalışmasını sağlayan ve bir güvenlik olayının etkisini en aza indiren tüm teknik ve organizasyonel önlemleri almakla yükümlüdür. Bu tür önlemler, önleme önlemlerinin yanı sıra güvenlik olaylarının üstesinden gelmek için olanları da içermektedir.
- *Güvenlik Olaylarını Ele Alma*: Bir siber güvenlik olayı olması durumunda, ulusal stratejiye katılan paydaşların etkili bir şekilde tepki vermeye hazırlıklı olmaları gereklidir. Paydaşların işlemesi gereken olayların teknik ayrıntılarına ilişkin bilgi, analizleri ve gerekli bilginin yayılması, tüm katılımcıların kendilerini olayla başa çıkmak için daha iyi hazırlamalarına ve aynı zamanda güvenlik önlemleri ile ilgili düzeltici eylemlere devam etmelerine yardımcı olmaktadır. Bu şekilde, hazırlıklı olma ve güvenlik olaylarını yönetme ve daha sonra iyileşme yeteneği ulusal düzeyde artırılır.
- *Ulusal Hazırlık Egzersizleri*: Ulusal hazırlık alıştırmaları, katılımcı paydaşların hazırlıklılarını değerlendirmek ve sistem zayıflıklarını ve zayıflıklarını tespit etmek için önemli bir araçtır. Güvenlik olaylarının simülasyonu, paydaşların ilgili iyileştirmeler ve güncellemelerle ilerleyebilmeleri için, alınan ilgili güvenlik önlemlerinin ve taslak halindeki acil durum planlarının uygulanması yoluyla bunları gerçek olaylara benzer koşullarda ele alma fırsatı sunmaktadır. Ayrıca, bu tür tatbikatlar bilgi ve bilgi alışverişini ve katılımcı paydaşlar arasındaki işbirliğini geliştirirken, Yunanistan'da siber güvenlik seviyesini artırmaya yönelik işbirliği kültürünü güçlendirir.
- *Kullanıcı-Vatandaş Bilinci*: Siber güvenlikle ilgili tehditler ve güvenlik açıkları ve bunların sosyal etkileri konusunda farkındalık hayati önem taşımaktadır.
- *Güvenilir Bilgi Alışverişi Mekanizmaları*: Ulusal siber güvenlik stratejisine katılan özel paydaşlar ile kamu sektöründeki denetim organları arasında ve ulusal siber güvenlik kurumu ile belirtilen zorunlu bilgi alışverişi özel bir sistem ile yapılacaktır. Özel paydaşlar, işlettikleri bilgi ve iletişim sistemleri, uyguladıkları güvenlik

politikaları ve karşılaştıkları tehdit ve güvenlik olayları ile ilgili bilgi alışverişinde bulunmaya teşvik edilmektedir. Benzer şekilde, kamu sektörü paydaşları, istenen siber güvenlik düzeyini potansiyel olarak tehlikeye atabilecek şekilde toplanan bilgileri paylaşmaya teşvik edilmektedir.

- *Araştırma ve Geliştirme Programları ile Akademik Eğitim Programlarının Desteklenmesi*: Akademik topluluğun ulusal, AB veya diğer uluslararası araştırma ve geliştirme programlarına katılma çabası ve müfredatının ulusal siber güvenlik stratejisi ile ilgili konulara uyarlanması çabalarının devlet tarafından sağlanan önemli destek, siber güvenlik düzeyini güçlendirmek için önemli bir parametredir. Yunanistan'da, özellikle bunun sürekli gelişen en son teknolojiler ve uzmanlık bilgisi alanı olduğu dikkate alınmaktadır.
- *Uluslararası Düzeyde İşbirliği*: Siber uzay ve internetin küresel bir bilgi ortamı olduğu düşünüldüğünde, bilgi ve iletişim sistemlerinin tehditleri ve açıkları ile uğraşmak, ulusal düzeyde işbirliği gerektiren küresel bir çaba haline gelmiştir. Bu nedenle, Yunanistan'ın, ülkenin dış politikasının mevcut hedefleri ve uygulanmasına yönelik talimatlar bağlamında ve ilgili mevzuata uygun olarak, siber uzay güvenliği konusunda tüm uluslararası işbirliğine aktif olarak katılması önemlidir. Daha spesifik olarak, bu konuda benzer bir strateji benimseyen ve bu durumda seçimleri karşılık gelen Yunan seçimleriyle uyumlu olan ülkelerle sistematik işbirliği gereklidir.
- *Ulusal Stratejinin Değerlendirilmesi ve Revizyonu*: Ulusal siber güvenlik stratejisinin stratejik hedeflerinin uygulanması, stratejiyi değerlendirmek ve muhtemelen revize etmek amacıyla ulusal siber güvenlik otoritesi tarafından izlenecektir. Stratejinin değerlendirilmesi, niteliksel ve niceliksel verimlilik indekslerini kullanan ve uluslararası standartlar temelinde önceden belirlenmiş bir metodolojiye dayanmaktadır.

Yukarıda belirtilenlerin uygulanması, tüm çabanın başarısı için özellikle önemli görülen ancak aynı zamanda düşük olgunluk ve deneyim seviyesi göz önüne alındığında özellikle zor olan kamu ve özel sektör arasındaki işbirliğinin güçlendirilmesini gerektirir. Bununla birlikte, böyle bir işbirliğinin faydaları devlet için ve kamu idaresi için, vatandaşlar için ve sağlanan güvenlik hizmetlerinin seviyesi için ancak özel sektör için de (geniş bant hizmet sağlayıcıları, özel işletmeler) çok yönlü olacaktır (Yunanistan, 2017).

4.13. Portekiz'in Siber Güvenlik Eylem Planı

92/2019 sayılı Bakanlar Kurulu Kararı ile Portekiz'in Siber Güvenlik Eylem Planı kabul edilmiş ve yayımlanmıştır. Karar ile ağ ve bilgi sistemlerinin güvenliğini derinleştirmeyi ve siber uzayın tüm vatandaşlar tarafından ücretsiz, güvenli ve verimli kullanımını güçlendirmeyi amaçlayan ilk Ulusal Siber Uzay Güvenliği Stratejisini onaylanmıştır. Siber uzayın hızlı içsel gelişimi ve buna bağlı olarak tehditlerin, güvenlik açıklarının, süreçlerin ve altyapıların artan evrimi ve kullanımlarına dayalı ekonomik, sosyal ve kültürel modeller göz önüne alındığında, bu stratejinin bir dönem limiti içinde revize edileceği tanımlanmıştır.

Eylem planı 2019-2023 dönemi için hazırlanmıştır. Plan üç stratejik hedefe dayanmaktadır: (1) *dayanıklılığı en üst düzeye çıkarmak*, (2) *yeniliği teşvik etmek ve* (3) *kaynakları oluşturmak ve güvence altına almak*. Stratejik hedeflerin her biri ile ilişkili çıkarımlar ve ihtiyaçlar, siber uzaydaki ulusal stratejik potansiyeli güçlendirmeyi amaçlayan somut eylem hatları oluşturan altı müdahale eksenine çevrilmiş genel ve özel bir yönelim tanımlamamıza olanak tanımaktadır (Portekiz, 2019).

Portekiz'in demokratik hukukun üstünlüğünün temel değerlerini koruyan ve toplumun dijital evrimine karşılık gelen kurumların düzenli işleyişini sağlayan yenilikçi, kapsayıcı ve esnek eylem yoluyla daha güvenli ve daha müreffeh bir ülke olması planlanmaktadır. Eylem planı aşağıdakileri içerir (Portekiz, 2019);

1. Bu çözüme ekli ve ayrılmaz bir parçasını oluşturan Siber Uzay Güvenliği Ulusal Stratejisi 2019-2023'ü kapsamaktadır.
2. Bu kararın yürürlüğe girmesinden sonra 120 günlük süre içinde onaylanacak 2019-2023 Ulusal Siber Uzay Güvenliği Stratejisi için bir Eylem Planının hazırlanmasını belirlenecektir.
3. Ulusal Siber Güvenlik Otoritesi olarak Ulusal Siber Güvenlik Merkezi'ne, önceki paragrafta atıfta bulunulan eylem planının detaylandırılması, yürütülmesinin izlenmesi ve revizyonunun, siber uzay güvenliğinden sorumlu tüm kuruluşlarla eklemlenme ve yakın işbirliği içinde koordine edilmesi sağlanacaktır.
4. Ulusal Siber Güvenlik Merkezi koordinatörünün, siber güvenlikten sorumlu hükümet üyesi tarafından onaylanmadan önce 2019-2023 Ulusal Siber Uzay Güvenliği Stratejisi Eylem Planı konusunda Siber Uzay Güvenliği Üst Kurulu'na danışılmıştır.

5. Ulusal Siber Uzay Güvenliği Stratejisi 2019-2023 döneminin uygulanmasına yönelik taahhüdün, yetkili kamu kuruluşlarından temin edilebilen fonların varlığına bağlı olduğunu ifade edilmiştir.
6. Ulusal Siber Uzay Güvenliği Stratejisi 2019-2023 için Eylem Planının yıllık revizyonunu yapılacaktır.

Eylem planının ana hedefleri aşağıdaki gibidir (Portekiz, 2019):

- *Değerler, Tanımlar ve İlkeler*: Eylem planı, ulusal çıkarlara yönelik siber alanın korunmasını ve savunmasını garanti altına almak ve özgürlüğünü teşvik etmek için ağ ve bilgi sistemlerinin güvenliğini derinleştirme taahhüdüne dayanmaktadır. Tüm vatandaşlar, şirketler ve diğer kamu ve özel kuruluşlar için güvenli ve verimli kullanım alanı oluşturulacaktır.
- *Bağlamın Analizi*: 2015 yılında ilk Ulusal Siber Uzay Güvenliği Stratejisi onaylandığında, teknolojik yeniliklerin ortaya çıkması ve toplum üzerindeki etkisi değişmiştir. Bilgi ve iletişim teknolojilerine bağımlılığın giderek artma eğilimi ve sosyal kalkınmayı doğrudan etkileyen yeni fenomenlerin ortaya çıkması, bağlantılı toplumlarda, ağının ve bilgi sistemlerini geliştirmek isteyenler için önemli fırsatlar yaratmıştır. Portekiz toplumunun refahı için potansiyel olarak zararlı amaçlar tespit edilecek ve önlemler geliştirilecektir.
- *Vizyon*: Bu eylem planı, 2023 için aşağıdaki vizyonu belirlemektedir; "*Portekiz, demokratik hukukun üstünlüğünün temel değerlerini koruyan ve toplumun dijital evrimine karşılık gelen kurumların düzenli işleyişini sağlayan yenilikçi, kapsayıcı ve dirençli eylem yoluyla güvenli ve müreffeh bir ülke olacaktır.*"

Eylem planının stratejik hedefler aşağıdaki gibi belirlenmiştir (Portekiz, 2019):

Stratejik Hedef 1- Dayanıklılık en üst düzeye çıkarılacak: Toplum için gerekli olan ağ ve bilgi sistemlerini tehlikeye atabilecek veya bozulmasına neden olabilecek tehditlere karşı ulusal çıkarlar doğrultusunda siber uzayın güvenliğini korumak için dahil etme ve ağ oluşturmayı geliştirerek ulusal dijital dayanıklılığı güçlendirecek ve garanti altına alacaktır.
Stratejik Hedef 2- Yenilik teşvik edilecek: Siber uzayı ekonomik, sosyal ve kültürel gelişme ve refah için bir alan olarak onaylayarak ulusal yenilik kapasitesini teşvik edilecek ve geliştirilecektir.

Stratejik Hedef 3- Kaynaklar oluşturulacak ve garanti altına alınacak: Siber uzay güvenliği konusunda ulusal kapasiteyi oluşturmak ve sürdürmek için yeterli kaynakların tahsis edilmesini sağlamak ve garanti altına almak için katkıda bulunulacak. Stratejik hedeflerin her biri ile ilişkili çıkarımlar ve ihtiyaçlar, güvenliğini artırarak siber uzaydaki ulusal stratejik potansiyeli güçlendirmeyi amaçlayan somut eylem hatları oluşturan altı müdahale eksenine çevrilmiş genel ve özel bir yaklaşım tanımlamayı mümkün kılmaktadır. Bunlar (Portekiz, 2019);

- *Eksen 1- Siber Uzay Güvenlik Yapısı:* Siber uzay güvenliği zorluklarının karmaşıklığı ve kapsamı, güçlü ve çapraz bir liderlik ve yönetişim, çevik, hızlı ve etkili bir operasyonel koordinasyon, ulusal çıkarlara yanıt verme ve koruma kapasitesi ve hepsinden önemlisi, kaynaklar, bilgi ve yeterlilikler gibi değişkenliklerden etkilenmektedir.
- *Eksen 2- Önleme, eğitim ve farkındalık yaratma:* Önleme bağlamında, erken tehdit değerlendirmesinde bilgi paylaşımının kilit rolü korunmalıdır. Çeşitli yaygın tehditlere, tanımlanmamış, sürekli değişen sınırlara ve ulusal çıkarların siber uzayının güvenliğini dayatan gelişmelerle ilgili kalıcı belirsizlik, potansiyel ve devam eden tehditlerle ilişkilendirilebilecek göstergeleri zamanında tespit etmek ve bilmek için ulusal bir kapasite gerektirir.
- *Eksen 3- Siber uzayın korunması:* Siber uzayın güvenliği, ulusal güvenliğin ayrılmaz bir parçasıdır ve devletin düzenli işleyişi, ekonomik gelişme ve inovasyonun yanı sıra vatandaşların dijital pazara ve siber alana olan güveni için gereklidir.
- *Eksen 4- Tehditlere müdahale ve siber suçla mücadele:* Olay sonrası müdahale alanında, siber saldırıların özelliklerine göre ceza otoriteleri ve iç güvenlik sistemini oluşturan kuruluşlar, atıfları nedeniyle, kendilerine ait olanlar da dahil olmak üzere veya yazarlığa atfedilen veya cezai soruşturmanın kendisini destekleyen ulusal ve uluslararası işbirliğinden kaynaklanan alıkonan bilgiler müdahale edilecektir.
- *Eksen 5- Araştırma, geliştirme ve yenilik:* Siber güvenlik alanında teknolojik yetenekler inşa etmek, sürdürülebilir bir gelişme ve geleceğin ilgili gözlemi için bu stratejinin anahtarıdır. Sonuç olarak, kamu ve özel sektör, akademi ve endüstrinin bireysel ve kolektif kapasitelerine dayalı olarak, en son siber güvenlik süreçleri ve teknolojilerinin ulusal araştırma, geliştirme ve yenilik potansiyelini güçlendirmeyi, desteklemeyi ve teşvik etmeyi amaçlamaktadır.

- *Eksen 6- Ulusal ve uluslararası işbirliği:* Son derece birbirine bağlı ve birbirine bağımlı bir dünyada, siber uzay güvenliği, karşılıklı güvenin geliştirilmesine dayanan ulusal ve uluslararası müttefikler ve ortaklar arasında güçlü bir işbirliği gerektirir. Bu, tüm paydaşların katıldığı ağın dayanıklılığını artırmada kilit bir faktördür. Sonuç olarak, bu eylem planı, ister kamusal ister özel olsun, siber uzay güvenliğine katkıda bulunan alanlarda sorumluluk sahibi ulusal yapılar ve kuruluşlar arasında gelişmiş bir işbirliği görevi gerektirmektedir.

Bu strateji, Ulusal Siber Güvenlik Konseyi'nin yıllık incelemesine tabi olacaktır. Böyle bir değerlendirme, stratejik hedeflerin ve eylem planlarının ve bunların değişen koşullara uygunluğunun doğrulanmasını içerecektir. Öte yandan, siber uzayın hızlı içsel evrimi, bu eylem planının, koşullar gerektirdiğinde olağanüstü revizyon süreçlerine zarar vermeksizin, maksimum beş yıl içinde gerçekleşmesi gerektiği göz önünde bulundurularak, düzenli ve periyodik olarak revize edilmesini gerektirmektedir (Portekiz, 2019).

4.14. İspanya'nın Ulusal Siber Güvenlik Stratejisi

İspanya'nın 2019 yılı Ulusal Siber Güvenlik Stratejisi belgesi oldukça detaylı ve kapsamlıdır. Toplam beş ana bölümden oluşmaktadır. Strateji belgesinde beş ana hedef belirlenmiş ve hedeflere yönelik alt göstergeler oluşturulmuştur. Ulusal Siber Güvenlik Stratejisi 2019, Milli Güvenlik Konseyi tarafından onaylanmıştır. Sürece şu organlar katılmıştır; Dışişleri Bakanlığı, Avrupa Birliği ve İşbirliği; Adalet Bakanlığı; Savunma Bakanlığı; Hazine Bakanlığı; İçişleri Bakanlığı; Bayındırlık Bakanlığı; Eğitim ve Mesleki Eğitim Bakanlığı; Sanayi, Ticaret ve Turizm Bakanlığı; Cumhurbaşkanlığı, Parlamento İlişkileri ve Eşitlik Bakanlığı; Bölgesel Politika ve Kamu İşlevi Bakanlığı; Ekonomi ve İşletme Bakanlığı; Sağlık, Tüketim ve Sosyal Refah Bakanlığı; Bilim, Yenilik ve Üniversiteler Bakanlığı; Milli İstihbarat Merkezi; Ulusal Güvenlik Departmanı ve profesyonel dernekler, şirketler ve akademiden bir Uzmanlar Komitesidir (İspanya, 2019).

Dördüncü sanayi devrimi - dijital devrim - yıllarca, hala iyileşmeye başladığımız ekonomik krizler, sosyal ve politik ikincil etkilerle bir arada var olmuştur. Bu nedenle, dijital dünyanın sunduğu inkar edilemez fırsatlara ve ilerlemelere rağmen, vatandaşların çoğu, dijital teknolojik bozulma ile ilgili her şey hakkında endişeli ve belirsizidir. Bu algıyı değiştirme mücadelesinde, kamu idarelerinde öncelikli çabalardır (İspanya, 2019).

2019 yılı Ulusal Siber Güvenlik Stratejisi, siber güvenlik alanındaki 2017 Ulusal Güvenlik Strateji belgesinin devamıdır. Genel hedefleri, alanın özel hedefini ve bunlara ulaşmak için belirlenen eylem çizgilerini dikkate almaktadır. Belge beş bölüme ayrılmıştır. Birinci bölüm, "Ortak bir küresel alanın ötesinde Siberuzay" olup siber güvenlik alanının genel bir anlayışını, belgenin 2013'te onaylanmasından bu yana kaydedilen ilerlemeyi, 2019 Ulusal Siber Güvenlik Stratejisini oluşturmanın arkasındaki nedenleri ve onun temel özelliklerini sunmaktadır. "*Siber uzaydaki tehditler ve zorluklar*" başlıklı ikinci bölüm, herhangi bir saldırının etkisini artıran, yüksek teknolojiye sahip ve geniş bağlantılı ortak bir küresel alan olarak tanımlanmasından kaynaklanan siber uzaya yönelik ana tehditler ifade edilmiştir. Bu tehditleri ve zorlukları iki kategoride sınıflandırır: bir yandan siber uzay varlıklarına yönelik tehditler ve diğer yandan, her türlü kötü niyetli ve yasadışı faaliyeti gerçekleştirmek için siber alanı kullanan tehditler (İspanya, 2019).

"*Siber güvenlik için teklif, ilkeler ve hedefler*" başlıklı üçüncü bölüm, 2017 Ulusal Güvenlik Stratejisinin (Eylem birimi, Öngörü, Etkinlik ve Dayanıklılık) yönetim ilkelerini beş belirli hedefe uygulamıştır. Gelişiminden, yedi eylem çizgisi belirleyen ve her birini geliştirmek için tedbirleri belirleyen "*Eylem hatları ve önlemler*" başlıklı kısım dördüncü bölümde bahsedilmektedir. Bu eylem çizgilerinin amacı: siber uzaydan gelen tehditlerle savaşmak için becerileri güçlendirmek; İspanya için stratejik varlık güvenliğini ve dayanıklılığını garanti altına almak; vatandaşlar ve şirketler için siber güvenliği artırmak; siber suçları soruşturma ve kovuşturma, vatandaş güvenliğini garanti etme ve siber uzaydaki hak ve özgürlükleri koruma becerilerini güçlendirmek; vatandaşlar ve şirketler için siber güvenliği artırmak; İspanyol siber güvenlik endüstrisini desteklemek, yetenekleri teşvik etmek ve korumak, dijital özerkliği güçlendirmek; Uluslararası siber uzay güvenliğine katkıda bulunmak, ulusal çıkarları destekleyen açık, çoğul, güvenli ve güvenilir siber alanı teşvik etmek ve Kapsamlı Ulusal Güvenlik Kültür Planına katkıda bulunmak için bir siber güvenlik kültürü geliştirmek şeklindedir (İspanya, 2019).

"*Ulusal Güvenlik Sisteminde Siber Güvenlik*" başlıklı beşinci bölüm, siber güvenliğin organik mimarisini tanımlar. İspanya Başbakanı tarafından yönetilen yapı üç yetkiliye ayrılmıştır: Hükümetin Ulusal Güvenlik Delege Komisyonu olarak Ulusal Güvenlik Konseyi; Milli Güvenlik Konseyi'ni destekleyen ve Başbakan'ın siber güvenlik konusundaki Ulusal Güvenlik politikasını yönetmesine ve koordine etmesine yardımcı olan ve Kamu İdareleri arasında ve bunlar ile özel sektör arasında koordinasyonu, işbirliğini ve

işbirliğini teşvik eden Ulusal Siber Güvenlik Konseyi ve Özel Durum Komitesi Ulusal Güvenlik Departmanının desteğiyle, disiplinleri geçtiği için ya da büyüklüğü nedeniyle olağan mekanizmaların müdahale yeteneklerini aşabilecek herhangi bir alanda kriz durumu yönetimini destekleyecektir (İspanya, 2019).

Ulusal Siber Güvenlik Stratejisi hükümet tarafından sahiplenilmiş ve ulusal güvenliğin yönetim ilkelerine dayanmıştır. Bunlar aşağıdaki gibidir (İspanya, 2019);

1. *Eylem Birimi:* Siber güvenlik alanındaki bir olaya farklı devlet görevlilerinin dahil olabileceği herhangi bir müdahale, tutarlı olması, koordine edilmesi, hızlı ve etkili bir şekilde çözülmesi halinde güçlendirilecektir. Bu nitelikler, Devletin eylem biriminin dikkatli bir şekilde hazırlanması ve uygun şekilde organize edilmesiyle elde edilebilir.
2. *Öngörü:* Siber uzayın özel doğası ve ilgili oyuncular, özel sektörün de dahil olması gereken kriz durumlarında devlet eylemine rehberlik etmek için uzmanlaşmış kuruluşlarda öngörü mekanizmaları gerektirir. Beklenti, önleyici eylemlere ve tepkilere göre öncelik verir.
3. *Verimlilik:* Siber güvenlik, çok zorlu ihtiyaçlarla ilişkili, yüksek düzeyde teknoloji içeren yüksek değerli, çoklu teklif sistemlerinin kullanılmasını gerektirir ve geliştirme, satın alma ve işletmeden kaynaklanan yüksek maliyetler, ayrıca önceden planlama ihtiyacı ve bunu sürdürmenin yüksek karmaşıklığı ile mücadele anlamına gelmektedir. Ayrıca, mevcut ve gelecekteki senaryolar, kaynaklardan maksimum performans elde etmek için sosyal sorumluluğun yanı sıra, İspanya'nın siber güvenliğe ayrılmış kaynakların optimizasyonuna ve verimliliğine odaklanması, eylem biriminin önemini artırması, bilgi paylaşımı anlamına gelen ekonomik kemer sıkma politikasından etkilenmektedir.
4. *Dayanıklılık:* Esneklik, sistemler ve kritik altyapılar için temel bir özelliktir. Devlet, siber tehditlere karşı korumalarını artırarak, ulus için gerekli olduğu düşünülen unsurların mevcudiyetini sağlamalıdır. Siber tehdit faaliyetlerine veya siber uzayın yasa dışı kullanımına karşı bilgi ve iletişim ağları için gerekli olan güçlendirmeye özel olarak değinilmelidir.

2017 Ulusal Güvenlik Stratejisi doğrultusunda ve içinde bahsedilen siber güvenlik hedefini genişleten İspanya, siber uzayın güvenli ve güvenilir kullanımını garanti edecek, vatandaşların hak ve özgürlüklerini koruyacak ve sosyo-ekonomik ilerlemeyi

destekleyecektir. Strateji belgesinin genel hedef; *Yeni siber güvenlik zorlukları, daha entegre, kapsayıcı ve daha az teknik hale getirmek için uyarlamak anlamına gelmektedir.* Aşağıda hedef ve hedefe yönelik atılacak adımlar sunulmuştur (İspanya, 2019):

1. *Hedef: Kamu Sektörü ve Temel Hizmetler İçin Bilgi, İletişim Ağlarının, Sistemlerinin Güvenliğini ve Esnekliğini Artırmak.*
   a. Saldırı prosedürlerini ve kökenlerini belirleyebilmek için siber tehdit algılama ve analiz becerileri genişletilecek ve iyileştirilecek. Ayrıca daha etkili koruma, atıf ve savunma için gerekli istihbarat hazırlanacak.
   b. Mükemmeliyet merkezleri ve araştırma tesisleri siber tehditlerle mücadele etmek için birlikte çalışma konusunda teşvik edilecek.
   c. Siber güvenlik için en iyi uygulamaların ve standartların oluşturulması, yayılması ve uygulanması güçlendirilecek.
   d. Siber güvenlik sorumlulukları olan kuruluşların, şirketlerin ve toplumun teknik ve operasyonel koordinasyonu sağlanacak.
   e. Siber güvenlik olaylarına müdahale etmek için standartlar, prosedürler ve talimatlar geliştirilecek ve güncellenecek, böylece Ulusal Güvenlik Sistemine dahil olma sağlanacak.
   f. Siber savunma ve siber istihbarat yetenekleri güçlendirilecek.
   g. Şirketlerin bilgi alışverişi ve analizi için sektör tabanlı platformlara katılımı teşvik edilecek, sektör bazlı risk ölçülecek ve bunları düzenleyen yasal gerekliliklerin yanı sıra bunu azaltmak için eylemler önerilecek.
   h. İspanyol Bilgisayar Güvenliği Olay Müdahale Ekibi (Computer Security Incident Response Team/CSIRT) ağındaki gelişmeler güçlendirilecek ve desteklenecek.
   i. Sektör tabanlı siber güvenliği iyileştirmek için bildirim platformları, bilgi alışverişi ve koordinasyon için geliştirme konuları artırılacak.
   j. Ulusal Güvenlik çerçevesinde siber güvenlik alanı için kriz yönetimine odaklanan önleme, tespit, müdahale, normale dönüş ve değerlendirme için araçlar geliştirilecek.
   k. Kamu sektörü, özel sektör ve yetkili uluslararası kuruluşlar arasında siber kazalar, siber tehditler ve istihbarat hakkında bilgi alışverişi, koordinasyon, işbirliği ve bilgi alışverişinin sağlanması, önleme ve erken uyarı sistemleri teşvik edilecek.
   l. Müdahale yeteneklerini iyileştirmek için kamu sektöründe aktif siber savunma önlemleri yerleştirilecek.

2. *Hedef: Yasa Dışı veya Kötü Niyetli Kullanımı Engellemek İçin Siber Uzayın Güvenli ve Güvenilir Kullanımı Teşvik Edilecek.*
    a. Kamu sektörüne, temel hizmetlere ve stratejik şirketlere yönelik siber saldırılara karşı önleme, tespit, müdahale, kurtarma ve dayanıklılık yetenekleri genişletilecek ve güçlendirilecek.
    b. Kritik altyapı koruma standardının geliştirilmesini güçlendirerek bilgi ağları ve bunları destekleyen sistemler için güvenlik güçlendirilecek.
    c. Ulusal Güvenlik Çerçevesi'nin, Kritik Altyapı Koruma Sisteminin tam olarak uygulanmasını ve kritik altyapı koruma standardı ile temel hizmetlerin risk temelli bir öncelik odaklı olarak uyumu sağlanacak.
    d. Yetkinlikler dahilinde, ulusal siber güvenliği iyileştirmek için ulusal yapılarla işbirliği yapılacak ve koordine edilecek.
    e. Önleme, tespit ve müdahale becerileri geliştirilecek ve siber güvenlik operasyon merkezlerinin bölgesel ve yerel gelişimi artırılacak.
    f. Kamu idareleri tarafından da paylaşılan telekomünikasyon altyapı ve hizmetlerinin ve ortak yatay bilgi sistemlerinin uygulanması güçlendirilecek.
    g. Yetkili makamların güvenlik seviyelerini ve nasıl gelişebileceklerini belirlemelerine olanak tanıyan başlıca siber güvenlik değişkenleri için bir ölçüm sisteminin geliştirilmesi teşvik edilecek.
    h. Kamu ve özel sektörü, özellikle temel hizmet sunumunu etkilerken tedarik zinciri risk yönetimi taahhüt edilecek.
    i. Kamu sektörü sözleşme süreçlerinde ve temel hizmetlerde kullanılmak üzere nitelikli, sertifikalı ürün ve hizmetlerin katalogları geliştirilecek.
    j. Gizli bilgileri işleyen bilgi sistemleri için güvenlik yapıları ve gözetim kapasiteleri güçlendirilecek.
    k. Özellikle Ulusal Güvenliği, Kamu Yönetimini, temel hizmetleri ve aranan şirketleri etkileyen alanlarda siber uygulamaları ve siber güvenlik değerlendirmeleri teşvik edilecek.
    l. Tekil bilimsel-teknik altyapıların ve ar-ge referans merkezlerinin korunması sağlanacak.
3. *Hedef: İş ve Sosyal Ekosistem Ve Vatandaşlar Korunacak.*
    a. Hem suç türlerinin tanımlanması hem de doğru soruşturma önlemlerinin düzenlenmesi ile ilgili olarak siber suçlara etkili bir yanıt için yasal çerçeve güçlendirilecek.

b. Vatandaşların işbirliğini ve katılımı teşvik edilecek.
c. Soruşturma, ilişkilendirme ve kovuşturma becerilerini ve uygun olduğunda siber suçlara karşı cezai işlemleri güçlendirmek için eylemler geliştirilecek.
d. Cezai güvenlik olayları ile ilgili bilgilerin ceza yargılama yetkisinin yetkili kuruluşlara, özellikle de temel hizmet sunumunu ve kritik altyapıları etkileyen/etkileyebilecek olan transferler teşvik edilecek.
e. Yasal operatörler için, siber suçla mücadeleye yönelik yasal ve teknik çerçevenin daha iyi uygulanmasını sağlayan bilgi ve materyal kaynaklarına erişim olanakları geliştirilecek.
f. Siber suç soruşturma ve kovuşturma sorumluluklarına sahip personel arasında bilgi, deneyim ve bilgi alışverişi teşvik edilecek.
g. Hukukçuların ve devlet güvenlik güçlerinin insan ve malzeme kaynaklarına erişimi sağlanacak.
h. Bu alanda yetkinliğe sahip farklı kurumlar ve birimler arasında siber suçlar ve siber uzayın diğer yasa dışı kullanımları konusunda araştırma koordinasyonu güçlendirilecek.
i. Uluslararası hukuk ve polis işbirliği güçlendirilecek.

4. *Hedef: Siber Güvenliğe, İnsani ve Teknolojik Becerilerin Güçlendirilmesine Yönelik Kültür ve Bağlılık Desteklenecek.*
   a. Vatandaşlara ve özel sektöre, kaliteli ve erişimi kolay olan ve siber güvenlik iş sektörü hizmetlerine olan talep teşvik edilecek.
   b. KOBİ'lerde, mikro KOBİ'lerde ve serbest meslek sahipleri arasında siber güvenlik ile ilgili kamu politikaları açıklanacak, özellikle de dayanıklılığı geliştirilen adımlar atılacak.
   c. Yasal sisteme uygun olarak vatandaşın dijital hakları çerçevesinde kişisel verilerin gizliliğini ve korumasını garanti etmek için siber güvenlik teşvik edilecek.
   d. Özel sektör ve vatandaşlar için çevik, güvenli ihbar mekanizmaları oluşturulacak.
   e. Kamu ve özel aktörler arasında işbirliği teşvik edilecek, özellikle İnternet Hizmeti ve Dijital Hizmet Sağlayıcıların siber güvenliği iyileştirme taahhüdü desteklenecek.
   f. Siber güvenlik önlemlerine öncelik vermek ve toplumu uygun şekilde bilgilendirmek için hem vatandaşlar hem de şirketler için birikmiş riski ve nasıl değiştiğini ölçmek için mekanizmalar geliştirilecek.
   g. İş sektöründe, tanınmış siber güvenlik standartlarının uygulanması teşvik edilecek.

h. Güvenilir elektronik tanımlama sistemlerinin ve güvenilir elektronik hizmetlerin uygulanması artırılacak.
i. Kamu-özel sektör sinerjisini güçlendirmek ve oluşturmak için sivil toplum, bağımsız uzmanlar, özel sektör, akademi, dernekler, kar amacı gütmeyen kuruluşlar ve diğerlerinden temsilcilerin bir araya geldiği Ulusal Siber Güvenlik Forumu'nun kurulması sağlanacak.

5. *Hedef V: Uluslararası Siber Uzay Güvenliği Desteklenecek.*
   a. KOBİ'lerde, işletmelerde, üniversitelerde ve araştırma merkezlerinde dijital güvenlik ve siber güvenlikle ilgili Ar-Ge destek programları artırılacak.
   b. Özellikle mikro KOBİ'ler ve KOBİ'ler söz konusu olduğunda, yenilik, yatırım, uluslararasılaşma ve teknoloji transferini destekleyen tedbirler için teşvikler sağlayarak sanayi ve siber güvenlik hizmetleri sektörü yeniden canlandırılacak.
   c. Dijital özerkliği, fikri ve sınai mülkiyeti güçlendirmek için ulusal çıkar gereksinimlerini özellikle destekleyen herhangi bir siber güvenlik ürünleri, hizmetleri ve sistemleri tasarımdan itibaren güvenlik geliştirmek için ulusal faaliyetler artırılacak.
   d. Bilgi ve iletişim teknolojileri ürün ve hizmetlerinde standardizasyon faaliyetlerini ve siber güvenlik gereksinimleri teşvik edilecek.
   e. İş piyasasının ihtiyaçlarını karşılayan siber güvenlikte yetkinlik çerçeveleri güncellenecek veya uygun olduğunda geliştirilecek.
   f. Sürekli eğitimi, istihdam eğitimini ve üniversite eğitimini artırarak, mesleki yeterlilik ve sertifika sistemlerini teşvik ederek eğitim ve öğretim kurumları arasında işbirliği teşvik edilecek.
   g. Kamu sektörü iş tanımlarına profesyonel siber güvenlik profilleri dahil edilecek.
   h. Araştırma alanına özellikle dikkat ederek, siber güvenlik alanındaki yetenekler tespit edilecek.
   i. Siber güvenlik ve siber savunma alanında belirli Ar-Ge programları güçlendirilecek.

6. *Ek Hedef 1: Açık, Çoğul, Güvenli, Güvenilir Siber Alanı Teşvik Ederek ve Ulusal Çıkarları Destekleyerek Siber Uzay Güvenliğine Uluslararası Olarak Katkıda Bulunulacak.*
   a. İspanya'nın ait olduğu ve siber güvenliğin yetki alanının önemli bir parçası olduğu organizasyonlarda, konferanslarda ve bölgesel ve uluslararası forumlarda varlığı güçlendirilecek.

b. Birleşmiş Milletler alanında, sorumlu davranış kurallarının uygulanmasını sağlamak için fikir birliği arayışı teşvik edilecek.
c. Tek pazarın ilerlemesini ve sağlamlaştırılmasını teşvik eden güvenli bir Avrupa ekosistemi ve Avrupa Birliği ile NATO arasında tamamlayıcı yönler ve işbirliği arayışıyla Avrupa'nın güvenliği ve stratejik özerkliği teşvik edilecek.
d. Diğer ülkelerle siber tehditlerle savaşmaya, müzakereleri teşvik etmeye ve uluslararası anlaşmaları imzalamaya koordineli bir odak geliştirmek için ikili diyalog, işbirliği, bilgi ve deneyim alışverişi sistemleri ve erken uyarı cihazları teşvik edilecek.
e. Üçüncü taraf ülkelerde teknolojik becerilerin ve internet erişiminin geliştirilmesini teşvik ederek Sürdürülebilir Kalkınma Hedeflerine uyuma yardımcı olunacak.
f. Hibrit Tehditler konusunda daha fazla farkındalık geliştirmek için çevre ülkelerle birlikte çalışarak, ülkenin egemenliği ve bütünlüğü üzerindeki etki sınırlandırılacak.

7. *Ek Hedef 2: Siber Güvenlik Kültürü Geliştirilecek.*
   a. Vatandaşlar ve şirketler için farkındalık yaratma kampanyaları artırılacak.
   b. Ulusal siber güvenliğe ilişkin olarak toplumdan ortak sorumluluk ve yükümlülüklerde artışa neden olan eylemler güçlendirilecek.
   c. Siber güvenlikte dijital okuryazarlık için girişimleri ve planları güçlendirilecek.
   d. En iyi iş uygulaması olarak siber güvenlik kültürünün yayılması teşvik edilecek.
   e. Sahte haberleri ve dezenformasyonu saptamaya yardımcı olan doğru, yüksek kaliteli bilgilerden yana eleştirel bir ruh teşvik edilecek.
   f. Kuruluşların yöneticileri arasında farkındalık yaratılacak, böylece yöneticiler gerekli kaynakları serbest bırakabilirler ve kurumlarının gerektirdiği siber güvenlik projelerini teşvik edebilirler.
   g. Okullarda siber güvenlik konusunda tüm eğitim düzeylerine ve uzmanlık alanlarına uyarlanmış bilinçlendirme ve eğitim teşvik edilecek.
   h. Özellikle gençler arasında yurttaş kampanyalarına daha fazla erişim sağlamak için medya işbirliği ve katılımı araştırılacak.

Eylem planı, ulusal yönetişim modelinde daha fazla ilerlemeyi Avrupa politikalarıyla tamamlayan girişimleri güçlendirmeyi hedeflemektedir. Ulusal Güvenlik Sistemi içindeki siber güvenlik yapısı aşağıdaki bileşenlerden oluşmaktadır (İspanya, 2019):

- Milli Güvenlik Kurulu.
- Kriz durumlarında tüm Ulusal Güvenlik Sistemi için tek bir Özel Durum Komitesi.
- Ulusal Siber Güvenlik Konseyi
- Siber Güvenlik Daimi Komitesi.
- Ulusal Siber Güvenlik Forumu.
- Yetkili kamu makamları ve ulusal kurumlar.

2013 Ulusal Siber Güvenlik Stratejisinden edinilen deneyimler sayesinde, 2019 yılı eylem planında karşılaşılan değişen tehditler ve zorluklar daha detaylı olarak ele alınmıştır. Burada özellikle ilgili bir eylem olan, İspanya Merkezi Yönetimi Siber Güvenlik Operasyon Merkezi'nin kurulmasına odaklanılmıştır (İspanya, 2019).

4.15. Avusturya'nın Siber Güvenlik Stratejisi

Avusturya'nın strateji belgesi Avusturya Kritik Altyapı Koruması Programının ilkeleri tarafından yönlendirilmektedir. Ülke etkili dijital altyapıların, ülke vatandaşlarına enerji, su ve ulaşım gibi genel hizmetlerinin sağlanmasında ön koşul olarak kabul edilmektedir. Ülkenin karşı karşıya olduğu risk ve fırsatlar aşağıdaki gibi özetlenebilir (Avusturya, 2013):

Riskler genel olarak siber uzay, devlet, ekonomi, bilim ve toplum için hayati bir faaliyet alanı haline geldiğinden bahsedilerek insanların güvenliğinin bir dizi risk ve tehdide maruz kalmakta olduğu ifade edilmiştir. Siber suç, kimlik sahtekarlığı, siber saldırılar veya internetin aşırılık yanlısı amaçlarla kötüye kullanılması, etkilenen tüm paydaşların karşı karşıya olduğu ciddi yeni zorluklardır. Ulusal ve uluslararası düzeyde hükümet ve sivil toplum kuruluşlarının geniş işbirliğini ile söz konusu risklere karşı önlem alınmalıdır (Avusturya, 2013).

Rapordaki fırsatlar ise siber dünyanın gelişmekte olduğu ifade edilerek aşağıdaki değişkenler sıralanmıştır (Avusturya, 2013);

- *Bilgi ve iletişim alanı:* Siber alan, farklı veri ve bilgi kaynakları kümelerinin yayılmasını ve iletilmesini mümkün kılmaktadır.
- *Hızlı bir şekilde siber uzay büyüyor:* Dünya çapında her dakika yaklaşık 204 milyon e-posta gönderiliyor, iki milyondan fazla Google araması yapılıyor, Facebook'ta altı

milyon kez oturum açılıyor ve 70'ten fazla yeni alan kaydediliyor. Bu gelişmeler ile geleceğin daha hızlı olacağı öngörülüyor.

- *Sosyal etkileşim alanı:* Siber alan, insanlar tarafından sosyalleşmek için kullanılan genel bir alandır. Bugün dünya çapında iki milyardan fazla internet kullanıcısı vardır. Bu sosyal yakınlık sadece ülke içi değil ülkeler arasındaki sosyal iletişimi artırmaktadır.
- *Ekonomik ve ticari alan:* Siber uzay, nispeten kısa bir süre içinde stratejik öneme sahip bir pazar yeri haline gelmiştir. Tahminlere göre, küresel e-ticaret hacmi son iki yılda neredeyse ikiye katlanmaktadır. Bu süreç ülke içindeki ve ülkeler arasındaki ticareti canlandırmaktadır.
- *Politik katılım alanı:* Siber alanın, hükümet ve toplum arasındaki ilişki üzerinde etkisi vardır. Devlet, e-devlet aracılığıyla vatandaşlara ulaşarak devlet hizmetlerine kolaylaştırılmış erişim sunmaktadır. Dijital etkileşim biçimleri, siyasi katılım ve siyasi ifade için yeni fırsatlar yaratmaktadır. Bu hedefe ulaşmanın ön koşulu hem sanal alanda hem de çevrimdışı ortamda tüm insan haklarını garanti altına almaktır.
- *Kontrol alanı:* Siber alanın bir kontrol alanı olarak rolü, bilgi alanı olarak işleviyle yakından bağlantılıdır. Bu kontrol alanını kullanarak ulaşım, ekonomi, sanayi, sağlık ve eğitim sektörlerinin tüm altyapılarını izlemek, işletmek ve sürdürmek pratik olarak mümkündür. Tahminlere göre, 2020 yılına kadar 50 milyara kadar cihaz birbiriyle iletişim kurabilecektir (*nesnelerin interneti*). Bu nedenle, söz konusu iletişimin güvenliğini sağlamak çok daha önemli olacaktır.

Avusturya strateji belgesinde birtakım prensipler belirlemiştir. Ülke kapsamlı entegre ve proaktif dayanışmaya dayalı bir siber güvenlik politikası uygulamayı planlamaktadır. Politikaların güvenilirlik, bütünlük, zorunlu uygulama, özgünlük, kullanılabilirlik ve ayrıca gizlilik ve veri koruma temeline uyulması amaçlanmıştır. Temel prensipler ise; uygulanabilir, hukuk kuralına bağlılık, hizmette yerellik, öz düzenleme ve orantılılık olarak belirlenmiştir (Avusturya, 2013).

Ülke stratejik belge kapsamında birçok stratejik hedef belirlemiştir. Avusturya dijital bir toplum olarak gelişmeye devam ederken, açık bir toplumun temel değerleriyle uyumluluğun sağlanması hayati önem taşıdığını ifade etmiştir. Dinamik bir sanal alan, e-devlet ve e-ticaret çerçevesinde sosyal refahı ve ekonomik faydaları kolaylaştırmaktadır. Bunun yanı sıra, bilgi alışverişi ile birlikte sosyal ve politik katılım stratejik belgenin temel görevi olarak

görülmektedir. Avusturya, Siber Güvenlik Stratejisi çerçevesinde aşağıdaki stratejik hedefleri takip etmektedir (Avusturya, 2013):

- Veri alışverişinin kullanılabilirliği, güvenilirliği ve gizliliği ile verilerin kendilerinin bütünlüğü yalnızca güvenli, esnek ve güvenilir bir siber alanda garanti edilecektir.
- Yetkili federal idarelerin ulusal yaklaşımına dayalı olarak Avusturya, bilgi ve iletişim teknolojileri altyapılarının güvenli ve tehditlere karşı dayanıklı olmasını sağlayacaktır.
- Yasal hedef olan "*siber güvenlik*" Avusturya makamları tarafından (hükümet dışı ortaklarla işbirliği içinde) siyasi-stratejik kontrol, tanıma ve müdahale, ayrıca etkilerin sınırlandırılması ve restorasyon alanında etkili ve orantılı önlemler alınarak korunacaktır.
- Avusturya, bir dizi bilinçlendirme önlemi alarak bir "*siber güvenlik kültürünü*" inşa edecektir.
- Siber güvenlik konusunda ulusal bir diyalog çerçevesinde, mevcut işbirliği güçlendirilecek ve yeni girişimler bilgi, yetenek ve kapasite geliştirilecek desteklenecek ve birbirleriyle ilişkilendirilecektir.
- Avusturya, özellikle bilgi alışverişinde bulunarak, uluslararası stratejiler oluşturarak, gönüllü planlar ve yasal olarak bağlayıcı düzenlemeler geliştirerek, ceza davalarını düzenleyerek, uluslararası tatbikatlar oluşturarak ve işbirliği projeleri yürüterek, Avrupa ve küresel düzeyde uluslararası işbirliğinde aktif bir rol oynayacaktır.
- Avusturya'nın e-devleti siber olarak güvenli hale getirmeyi hedeflemektedir. Avusturya Federal Cumhuriyeti'nin, federal eyaletlerin, şehirlerin ve belediyelerin güvenlik önlemleri güçlendirilecektir.
- Tüm Avusturya özel şirketleri, kendi uygulamalarının bütünlüğünü, müşterilerinin kimliğini ve mahremiyetini koruyacaktır.
- Avusturya hükümeti, halkının siber alandaki bireysel sorumluluğunun farkında olması için çalışacaktır. Tüm vatandaşlar, çevrim içi faaliyetlerinin yeterli şekilde korunmasının sağlanması, elektronik kimlik doğrulama ve imza için gerekli yeteneklere sahip olunması amacıyla eğitim faaliyetleri düzenlenecektir.

Ülke 7 adet ana hedef belirlemiştir. Her hedefin altında ise alt hedefler yer almakta olup toplam 15 adet alt hedef belirlenmiştir. Eylem planındaki ana hedefleri ve alt hedefleri aşağıda sıralamak mümkündür (Avusturya, 2013):

Eylem 1- Yapılar ve Süreçler: Siber uzay içinde, siber güvenliği sağlamak için ayrı ayrı çalışan çok sayıda yapı ve paydaş vardır. Plan kapsamında, kamu ve özel sektörün ilgili tüm paydaşlarını dahil ederek hem siyasi-stratejik düzeyde hem de operasyonel düzeyde genel koordinasyonu sağlayacak süreç ve yapıların tanımlanması hedeflenmiştir. Amaç özelindeki önlemler aşağıdadır:

1) Siber Güvenlik Yönlendirme Grubunun Kurulması: Siber Güvenlik Yönlendirme Grubu, Avusturya Bakanlar Kurulu'nun 11 Mayıs 2012 tarihli kararına dayanılarak kurulmuştur.

2) Operasyonel düzeyde koordinasyon için bir yapı oluşturmak:

a. Mevcut operasyonel yapıların üzerine inşa edilen ve bunlardan faydalanan bir koordinasyon yapısı oluşturulacaktır.
b. Operasyonel Koordinasyon Yapısı çerçevesinde gerçekleştirilen görevler, bakanlıklar ile iş ve araştırma sektörlerinin yapıları dahil edilerek Federal İçişleri Bakanlığı tarafından koordine edilecektir.

3) Siber Kriz Yönetiminin Kurulması:

c. Avusturya'nın Siber Kriz Yönetimi, eyaletin temsilcilerinden ve kritik altyapıların operatörlerinden oluşturulacaktır.
d. Kriz yönetimi ve süreklilik planları, kamu kurumları ve kritik altyapı işletmecileri ile işbirliği içinde sektöre özel ve sektörler arası siber tehditler için risk analizleri bazında düzenli olarak hazırlanacak ve güncellenecektir.
e. Siber Kriz Yönetiminin yanı sıra kriz ve devamlılık planlarını test etmek için düzenli siber tatbikatlar yapılacaktır.

4) Mevcut siber yapıların güçlendirilmesi:

f. Devlet Bilgisayar Acil Müdahale Ekibi (GovCERT)'nin rolü geliştirilecek ve güçlendirilecektir.
g. Siber suçlardan kaçınmak, önlemek ve bu alandaki operasyonel uluslararası işbirliğini kolaylaştırmak için Federal İçişleri Bakanlığı Siber Suçlar Yetkinlik Merkezinin rolü güçlendirilecektir.
h. Siber saldırıların önlenmesine yönelik operasyonel yeteneklerin temeli olarak, Askeri Bilgisayar Acil Müdahale Ekibi (MilCERT), kendi ağlarını korumak ve Siber Güvenlik Araştırmasını daha da geliştirmek için güçlendirilecektir.
i. Avusturya Bilgisayar Acil Müdahale (CERT) Derneği genişletilecek ve diğer derneklerle ulusal işbirliğini kolaylaştırmak için güçlendirilecektir.

Eylem 2- Yönetişim: Amaç, devletin ve devlet dışı aktörlerin siber alandaki rolünü, sorumluluklarını, yetkilerini tanımlamak ve tüm aktörler arasında işbirliği için yeterli çerçeve koşulları oluşturmaktır. Amaç özelindeki önlemler aşağıdadır:

5) Modern düzenleyici çerçevenin oluşturulması:

a. Siber Güvenlik Yönlendirme Grubu'nun himayesi altında, Avusturya'da siber güvenliğin güvence altına alınması için ek bir yasal dayanak, düzenleyici önlemler ve gönüllü öz taahhüt (davranış kuralları) oluşturma ihtiyacını analiz eden kapsamlı bir rapor hazırlanacak ve federal hükümete sunulacaktır.
b. Devlet dışı aktörlerin görevlerinin tanımlanmasında teşvikler ve yaptırımlar arasında bir denge sağlanacaktır.

6) Asgari standartların tanımlanması: İlgili tüm paydaşların etkileşimine dayalı olarak, etkili önlemeyi sağlamak ve mevcut gereksinimlere ilişkin ortak bir anlayışa ulaşmak için minimum güvenlik standartları tanımlanacaktır.

7) Siber güvenlik hakkında yıllık rapor hazırlanması: Siber Güvenlik Yönlendirme Grubu, "*Avusturya'da Siber Güvenlik*" yıllık raporunu hazırlayacaktır.

Eylem 3- Hükümet, Özel Sektör ve Toplum Arasında İşbirliği: Kamu idarelerinin, özel sektörün ve nüfusun birçok görev ve sorumluluğu bilgi ve iletişim teknolojilerine dayanmaktadır. Bu nedenle, kamu idareleri, özel sektör ve vatandaşlar arasında mevcut kapasite ve süreçleri işbirliği yoluyla güçlendirmek ve yeni fırsatlar yaratmak önemlidir. Amaç kapsamındaki önlemler aşağıdadır:

8) Siber Güvenlik Platformunun Kurulması:

a. Avusturya Siber Güvenlik Platformu, kamu idaresinin, özel sektörün ve akademinin tüm paydaşları ile devam eden iletişimi kolaylaştırmak için bir kamu özel ortaklığı olarak kurulması planlanmıştır. Tüm paydaşlar eşit düzeyde katılım sağlayacaktır.
b. Kritik altyapıların ve diğer sektörlerin özel operatörleriyle işbirliği, Avusturya'nın siber güvenliği için çok önemli görülmüştür.
c. Siber Güvenlik Platformuna katılan ortaklar arasında bilinçlendirme, eğitim, araştırma ve geliştirme gibi konularda kapsamlı işbirliği başlatılacaktır.
d. Siber güvenlik konularına dahil olan tüm ortakların zorlukları ve eylem fırsatlarını karşılıklı olarak anlamasını desteklemek için, devlet, özel ve akademik kuruluşlar arasında uzman alışverişi yoğunlaştırılmalıdır.

9) KOBİ'lere yönelik desteğin güçlendirilmesi: KOBİ'lerin farkındalığını artırmak ve onları tehlikeli durumlara hazırlamak için siber güvenlik konusunda öncelikli programlar başlatılacaktır.

10) Siber Güvenlik İletişim Stratejisinin Hazırlanması: Kamu yönetimi, özel sektör, akademi ve toplumdaki paydaşlar arasındaki iletişimi optimize etmek amacıyla, devlet kurumları tarafından kurulan veya planlanan tüm web sitelerinin bir Siber Güvenlik İletişim Stratejisi çerçevesinde koordine edilmesi sağlanacaktır.

Eylem 4- Kritik Altyapıların Korunması: Günümüzde neredeyse tüm altyapılar, operasyonların mümkün olduğunca sorunsuz, güvenilir, sürekli olmasını garanti etmesi beklenmektedir. Bu nedenle, bu bilgi sistemlerinin tehditlere karşı dayanıklılığını artırmak en önemli öncelik olarak belirlenmiştir. Kritik Altyapı Koruması için Avusturya Programı kapsamında, kritik altyapıları çalıştıran işletmeler kapsamlı güvenlik mimarilerini uygulamaya teşvik edilecektir. Amaç özelindeki öneri aşağıdadır:

11) Kritik altyapıların dayanıklılığının artırılması:

a. Kritik altyapı operatörleri, ulusal siber kriz yönetiminin tüm süreçlerine dahil edilecektir. Bu stratejik işletmeler, kapsamlı bir güvenlik mimarisi (risk ve kriz yönetimi) kurulması, ortaya çıkan tehditlere göre sistemlerin güncellenmesi ve bir siber güvenlik sorumlusu atanması için kullanılacaktır.
b. Kritik altyapı operatörlerinin ciddi siber olayları bildirme görevi olmalıdır. İlgili paydaşlarla kapsamlı istişarelerden sonra uygun yasal dayanak oluşturulacaktır.
c. Kritik altyapıların korunması için mevcut düzenlemeler, yeni siber zorlukları karşılamaya devam etmelerini ve gerekirse değiştirmelerini sağlamak için sürekli olarak gözden geçirilecektir.

Eylem 5- Farkındalık Yaratma ve Eğitim: Tüm hedef grupları duyarlı hale getirerek, siber güvenliğe yönelik gerekli farkındalık, kişisel ilgi ve gösterilen özen artırılacaktır. Okullarda ve diğer eğitim tesislerinde siber güvenlik ve medya yeterliliği alanında eğitim yoğunlaştırılacaktır. Amaç kapsamındaki önlemler aşağıdadır:

12) Siber güvenlik kültürünün güçlendirilmesi:

d. Farkındalık artırma girişimleri, mevcut programlar dikkate alınarak ortak bir yaklaşım temelinde geliştirilir, koordine edilir ve uygulanır. Bu bağlamda siber güvenliği farklı açılardan incelemek, ilgili tehlikeleri vurgulamak, olası etki ve zararlara dikkat çekmek ve güvenlik önlemleri için önerilerde bulunmak önemlidir. Bu amaçtan yola çıkılarak projeler geliştirilecektir.

e. Farklı hedef gruplara daha derinlemesine özelleştirilmiş tavsiyelere erişim sağlamak için, mevcut danışmanlık programları daha da güçlendirilecek ve genişletilecektir.
f. Bir web platformu biçiminde Bilgi ve İletişim Güvenliği İnternet Portalı kurulacaktır.
g. Siber suç önleme programları daha da geliştirilecektir.

13) Siber güvenlik ve medya yeterliliğini tüm eğitim ve öğretim seviyelerine dahil edilmesi:

h. Okul müfredatına bilgi ve iletişim teknolojileri, siber güvenlik ve medya yeterliliğinin daha güçlü entegrasyonu için bu hedefler her tür okulun müfredatının bir parçası haline getirilecektir.
i. Bilgi iletişim teknolojilerinin yeterliliği, pedagojik üniversitelerin ve diğer pedagojik kurumların yükseköğretim düzeyindeki eğitim programlarında yer alacaktır.
j. Kamu sektöründe siber güvenliğin geliştirilmesinden sorumlu uzmanların eğitimi, ulusal ve uluslararası eğitim tesisleri ile işbirliği içinde yoğunlaştırılacaktır.
k. Kritik altyapı operatörlerinin sistem yöneticileri, siber olayları tanımalarını, söz konusu sistemlerindeki anormallikleri tespit etmelerini ve bunları siber güvenlik sorumlularına rapor etmelerini sağlamak için siber güvenlik eğitimi almaları zorunlu tutulacaktır.

Eylem 6- Araştırma ve Geliştirme: Siber güvenliği sağlamak için, en son araştırma ve geliştirme sonuçlarına dayalı olması gereken teknik uzmanlık gereklidir. Bu amaçla, uygulamalı siber araştırmaların yanı sıra güvenlik araştırma programlarında siber güvenlik konuları giderek daha fazla dikkate alınmalıdır. AB güvenlik araştırma programlarında aktif tematik liderliğe ulaşmak için ülke, çalışmalar yapmayı hedeflemektedir. Amaç kapsamındaki önlemler aşağıdadır:

14) Avusturya'nın siber güvenlik alanındaki araştırmalarını güçlendirmek için;

a. Ulusal ve AB güvenlik araştırma programları çerçevesinde, siber güvenlik temel araştırma öncelikleri arasında olacaktır. Ortak projelerde, kamu yönetimi, özel sektör ve akademi ilgili paydaşlar, Avusturya'nın siber güvenlik standartlarını geliştirmek için kavramsal çerçeveyi ve teknolojik araçları geliştirecekler.
b. Avusturya, AB güvenlik araştırma programlarında aktif bir tematik liderlik için çaba gösterecektir. Avusturya, uluslararası araştırma programlarına önemli olduğunu düşündüğü temalara katkıda bulunacaktır.

Eylem 7- Uluslararası İşbirliği: Küresel ağ oluşturma ve uluslararası işbirliği eylem planının temel amacıdır. Siber uzayda güvenlik, yalnızca ulusal ve uluslararası düzeyde koordineli bir politika karışımı ile sağlanabilir. Avusturya bu nedenle aktif bir "*siber dış politika*" yürütecek ve koordineli ve hedefli bir yaklaşıma dayalı olarak AB, BM, AGİT, Avrupa Konseyi, OECD ve NATO ortaklıkları çerçevesinde çıkarlarını sürdürecektir. Amaç kapsamındaki önlemler aşağıdadır:

15) Avrupa'da ve dünya çapında siber güvenlik konusunda etkili işbirliği:
   c. Avusturya, AB Siber Güvenlik Stratejisinin geliştirilmesine ve uygulanmasına önemli bir katkı sağlayacaktır.
   d. Yetkili bakanlıklar, Avrupa Konseyi Siber Suçlar Sözleşmesini uygulamak ve ondan tam anlamıyla yararlanmak için gerekli önlemleri alacaklardır.
   e. Avusturya, uluslararası düzeyde ücretsiz interneti savunmaktadır.
   f. Avusturya, NATO Barış için Ortaklık çerçevesinde başlatılan ikili işbirliğine devam edecek ve AGİT'te somut güven ve güvenlik artırıcı önlemler listesinin hazırlanmasını aktif olarak destekleyecektir.
   g. Avusturya, uluslararası siber uygulamaların planlanması ve uygulanmasına aktif olarak katılacaktır.
   h. Siber güvenlikle ilgili dış politika önlemleri, Federal Avrupa ve Uluslararası İlişkiler Bakanlığı tarafından koordine edilecektir.

Yukarıdaki hedeflerin federal hükümet tarafından kabul edilmesinden sonraki üç ay içinde Avusturya Siber Güvenlik Stratejisinde belirtilen yatay önlemleri uygulamak için bir Uygulama Planı geliştirilmesi ön görülmüştür. Yetkili organlar ve sorumlu tutulan birimler, söz konusu hedefleri önlemleri kendi yetkileri dahilinde uygulamaktan sorumlu tutulmuştur. Eylem planındaki önlemlerinin uygulanması, Siber Güvenlik Yönlendirme Grubu tarafından koordine edilecek, hedeflere dayalı olarak, yetkili bakanlıklar kendi sorumluluk alanları için alt stratejiler geliştireceklerdir. Siber Güvenlik Yönlendirme Grubunda temsil edilen bakanlıkların, her iki yılda bir federal hükümete bir Uygulama Raporu sunulması öngörülmüştür. Böylece belirlenen hedeflere ne kadar ulaşıldığı tespit edilebilmesi amaçlanmıştır. Stratejik temellerin, devlet dışı ortaklarla işbirliği içinde daha da geliştirilmesi hedeflenmiştir (Avusturya, 2013).

4.16. Finlandiya'nın Siber Güvenlik Stratejisi

Finlandiya'nın 2013 yayınlanan Siber Güvenlik Stratejisi kapsamlı farklı değişkenleri dikkate alan bir yapıdadır. Toplam dört bölüm ve bir ek bölümden oluşmaktadır. Giriş kısmında ülke ve dünya için değerlendirmeler ve tespitler yer almaktadır. Toplumun güvenliğini sağlamak, hükümet yetkililerinin temel görevidir ve toplumun hayati işlevleri her durumda güvence altına alınmalıdır. Bir bilgi toplumu olarak Finlandiya, bilgi ağlarına ve sistemlerine güvenir ve sonuç olarak, onların işleyişini etkileyen sorunlara karşı savunmasızdır. Bu birbirine bağımlı, çok amaçlı elektronik veri işleme ortamı için uluslararası bir terim siber alan olarak tanımlanmıştır (Finlandiya, 2013).

Düzgün bir çalışma ortamı, Finlandiya'nın uluslararası yatırımcılar için çekiciliğini de artırmaktadır. Bunlara ek olarak, siber güvenliğin kendisi de yeni ve güçlenen bir iş alanıdır. Artan iş fırsatlarına ve vergi gelirine ek olarak, toplum tahakkuk eden bu iş sektöründen pek çok şekilde yararlanmaktadır. Ulusal siber güvenlik, Fin şirketlerinin başarısıyla bağlantılıdır. Bu Strateji, siber alana yönelik tehditlere yanıt vermede kullanılan ve işleyişini sağlayan temel hedefleri ve yönergeleri tanımlamaktadır. Finlandiya, Siber Güvenlik Stratejisinin yönergelerini ve gerekli önlemleri izleyerek siber alandaki kasıtlı veya kasıtsız rahatsızlıkları yönetebilir ve bunlara yanıt verebilir ve bunlardan kurtulabilir (Finlandiya, 2013).

Küçük, yetenekli ve işbirlikçi bir ülke olarak Finlandiya, siber güvenlik alanında öncü konumuna yükselme konusunda avantajlara sahiptir. Güvene ve sektörler arası işbirliğine dayanan geniş bir bilgi tabanına ve güçlü bir uzmanlığa, uzun bir yakın kamu-özel işbirliği geleneğine sahiptir. Finlandiya'nın siber güvenliğinin vizyonu aşağıdaki gibidir (Finlandiya, 2013):

- Finlandiya hayati işlevlerini her durumda siber tehditlere karşı koruyabilir.
- Vatandaşlar, yetkililer ve işletmeler güvenli bir siber alanı ve siber güvenlik önlemlerinden kaynaklanan yeterliliği hem ulusal hem de uluslararası düzeyde etkin bir şekilde kullanabilir.
- 2016 yılına kadar Finlandiya, siber tehditlere hazırlıklı olma ve bu tehditlerin neden olduğu sorunların yönetilmesinde küresel bir öncü olacaktır.

Siber alanda meydana gelen değişiklikler hızlıdır ve etkilerini tahmin etmek zordur. Bilgi teknolojisi için Yazılım Geliştirme Yaşam Döngüsü kısadır ve aynı eğilim farklı siber saldırı ve kötü amaçlı yazılım türleri için de geçerlidir. Siber tehditlere hazırlıklı olma ve siber savunma, hem bireysel hem de toplu olarak toplumdaki tüm taraflardan giderek daha hızlı, şeffaf ve daha iyi koordine edilmiş eylemler gerektirir. Finlandiya'nın siber güvenlik yönetimi için ulusal yaklaşım aşağıdaki ilkeler üzerine inşa edilmiştir (Finlandiya, 2013).

1. Bakanlıklara verilen görevlere ilişkin konular hükümetin görev alanına girmektedir. Her bakanlık kendi sektöründe siber güvenlikle ilgili konuları hazırlamaktan ve idari konuların uygun şekilde düzenlenmesinden sorumludur.
2. Siber güvenlik, toplumun kapsamlı güvenliğinin önemli bir parçası olduğundan, uygulanmasına yönelik yaklaşım, *Toplum için Güvenlik Stratejisinde* belirlenen ilke ve prosedürleri izler.
3. Siber güvenlik, tüm toplumun bilgi güvenliği düzenlemelerine dayanır. Çeşitli işbirlikçi düzenlemeler ve tatbikatlar, bunların uygulanmasını ilerletir ve destekler.
4. Siber güvenliğin uygulanmasına yönelik yaklaşım, verimli ve geniş kapsamlı bilgi toplamaya, analiz ve toplama sistemine, ortak ve paylaşılan durum farkındalığına, hazırlıklı olma konusunda ulusal ve uluslararası işbirliğine dayanmaktadır.
5. Siber güvenlik düzenlemeleri, tüzükler ve mutabık kalınan işbirliğine uygun olarak yetkililer, işletmeler ve kuruluşlar arasındaki görev dağılımını takip eder.
6. Siber güvenlik, işlevsel ve teknik gereksinimlerini karşılayacak şekilde inşa edilmektedir. Ulusal eyleme ek olarak, uluslararası işbirliğine ve uluslararası Ar-Ge ve tatbikatlara katılım için girdiler yapılmaktadır.
7. Dünya'nın siber güvenlik alanında önde gelen ülkelerinden biri olabilmesi için siber araştırma ve geliştirmenin yanı sıra eğitim, istihdam ve ürün geliştirmeye büyük ölçüde yatırım yapacaktır.
8. Siber güvenliğin gelişmesini sağlamak için Finlandiya, iş faaliyetlerini ve bu alandaki gelişimlerini desteklemek için uygun mevzuat ve teşvikleri destekleyecektir. Stratejik yönergelere uygun olarak ulusal bir siber strateji geliştirilecek ve ulusal siber güvenlik vizyonunun gerçekleşmesi için gerekli adımları atacaktır. Ayrı olarak hazırlanan bir eylem planı, ulusal siber güvenlik hedeflerinin gerçekleştirilmesini sağlayan önlemleri ana hatlarıyla belirtecektir. Uygulama programı, farklı aktörlerin ve idari şubelerin planlarının yanı sıra planlardan kaynaklanan sektörler arası önlemleri içerecektir.

Stratejik yönergelerin uygulanması, Fin güvenlik topluluğunun bir önceliği olarak kabul edilen kamu-özel sektör işbirliğini güçlendirecektir. Böyle bir işbirliği tüm topluma en iyi şekilde hizmet edebilir ve hayati işlevlerini yerine getiren aktörleri destekleyebilir. Amaç, günlük yaşamda ve rahatsızlıklar sırasında farklı işlevlerin kesintisiz ve güvenli akışını sağlamaktır. Eylem planı kapsamındaki hedefler aşağıdaki gibi sıralanabilir (Finlandiya, 2013):

1. Ulusal siber güvenliği ve siber savunmayı geliştirmek amacıyla yetkililer ve diğer aktörler arasında verimli bir işbirliği modeli oluşturulacak.
2. Toplumun hayati işlevlerinin güvenliğini sağlamaya katılan kilit aktörler arasında kapsamlı siber güvenlik durumu farkındalığı geliştirilecek.
3. İş dünyasının süreklilik yönetiminin bir parçası olarak herhangi bir hayati işlevi tehlikeye atan siber tehditleri ve rahatsızlıklar tespit edilecek. Bunlardan kurtulma konusunda toplumun hayati işlevleri için kritik olan işletmelerin ve kuruluşların yeteneklerini korunacaktır.
4. Polisin siber suçları ortaya çıkaracak, çözecek ya da önlemeye yetecek kapasiteye sahip olduğundan emin olunacak.
5. Finlandiya Savunma Kuvvetleri, yasal görevleri için kapsamlı bir siber savunma yeteneği oluşturacaktır.
6. Uluslararası kuruluşların faaliyetlerine ve siber güvenlik için kritik öneme sahip işbirlikçi forumlara aktif ve verimli katılım yoluyla ulusal siber güvenlik güçlendirilecektir.
7. Tüm toplumsal aktörlerin siber uzmanlığı ve farkındalığı geliştirilecektir.
8. Ulusal mevzuat aracılığıyla etkili siber güvenlik önlemlerinin uygulanması için ön koşullar oluşturulacak.
9. İş dünyasındaki yetkililere ve aktörlere siber güvenlikle ilgili görevleri, hizmet modelleri ve ortak siber güvenlik yönetimi standartları belirlenecek.
10. Stratejinin uygulanması ve tamamlanması izlenecektir.

4.17. İsveç'in Ulusal Siber Güvenlik Stratejisi

İsveç Ulusal Siber Güvenlik Stratejisi 2016-2017 dönemi için hazırlanmış ve yayımlanmıştır. Üç ana bölümden oluşan stratejik belge literatür ve uygulama alanlarına odaklanmıştır. Stratejik belgenin ana içeriği İsveç'te siber güvenliğin geliştirilmesine büyük

ihtiyaç olmasıdır. Bu ulusal siber güvenlik stratejisi, hükümetin kapsamlı önceliklerinin bir ifadesidir ve İsveç'in bölgedeki devam eden geliştirme çalışmaları için bir platform oluşturması amaçlanmıştır. Stratejinin temel amacı, toplumdaki tüm paydaşların siber güvenlik konusunda etkin bir şekilde çalışması için uzun vadeli koşulların oluşturulmasına yardımcı olmak ve toplum genelinde farkındalık ve bilgi düzeyini yükseltmektir. Strateji aracılığıyla hükümet, siber güvenliğin artırılması için toplumda halihazırda var olan çabaları ve katılımı desteklemek istemektedir. Dolayısıyla strateji, toplumun tamamını, yani merkezi hükümet yetkililerini, belediyeleri, il meclislerini, şirketleri, kuruluşları ve özel şahısları kapsamaktadır (İsveç, 2016).

Dijital dönüşüm, temelde toplumun her bölümünü etkileyen küresel bir fenomendir. Bize hem büyük fırsatlar hem de riskler sunmaktadır. Dijital dönüşümün doğasında bulunan riskleri nasıl yönettiğimiz hem refahımızı hem de güvenliğimizi sürdürme ve geliştirme becerimiz üzerinde önemli bir etkiye sahiptir. Günümüzde siber güvenlik tüm toplumu ilgilendirmektedir. Etkili ve güvenli bir bilgi yönetimi sağlamak istiyorsak, herkesin siber güvenlik sorunları için sorumluluk alması gerekmektedir (İsveç, 2016).

Toplumun siber güvenliğine yönelik talepler hızla artmaktadır. Yeni teknoloji kullanımındaki bu gelişme, değişiklikler ve yeni yenilikler, tehditlerin tespit edilmesini, risklerin değerlendirilmesini ve bağımlılıkların araştırılmasını zorlaştırmaktadır. Dijital dönüşüm, çağımızın en büyük değişikliklerinden biridir. Bilgi ve iletişim teknolojisinin hızlı gelişimi geleceğimiz üzerinde büyük etkiye sahiptir. İsveç, teknolojik gelişimin ön saflarında yer almaktadır. Fiber ağların kullanımının artması ve daha büyük mobil kapsama alanı, elektronik iletişim ağlarına yapılan yatırımları temsil etmektedir (İsveç, 2016).

Toplumun çeşitli politika alanlarının hedefleri doğrultusunda işlemesini ve gelişmesini sağlamak için siber güvenlik çalışmaları gereklidir. Dijital dönüşüm, toplumdaki tüm faaliyetlerin artan bir oranının ağlara, bilgi sistemlerine ve dolayısıyla siber güvenliğe bağlı olarak değişen derecelerde olduğu anlamına gelmektedir. Siber güvenlik stratejisi, İsveç'in güvenliğine yönelik hedeflere dayanmaktadır: nüfusun yaşamlarını ve sağlığını korumak, toplumun işleyişi ve demokrasisi, hukukun üstünlüğü, insan hakları ve özgürlükleri gibi temel değerleri sürdürme kapasitesidir (İsveç, 2016).

Ulusal güvenlik stratejisi, İsveç'in ulusal çıkarlarımızı aktif olarak koruyacağını ve bilgi teknolojisi alanında bulunan tehditler ve riskler de dahil olmak üzere, zarar görme riskiyle karşı karşıya olduklarında onları savunacağını belirtmektedir. Dijital strateji, İsveç'in dijital toplumda güvenli bir şekilde yer almak, sorumluluk almak ve güven inşa etmek için en iyi koşulları sağlayacağını belirtmektedir (İsveç, 2016).

Açık demokratik toplum, bilgileri işlerken istenen gizlilik, bütünlük ve erişilebilirliği sürdürme becerisine bağlıdır. Bu hem bilginin kendisinin hem de bu bilgiyi depolamak ve aktarmak için kullanılan sistemlerin korunması gerektiği anlamına gelmektedir. Siber güvenlik çalışmaları, toplumsal işlevlerin kalitesini ve etkinliğini korumak için gerekli bir faaliyet ve dijital dönüşümün fırsatlarından yararlanabilmenin ön şartıdır. Bu tür fırsatlar, gelişmiş dijital kamu hizmetlerinden bağlantılı ve otomatik araçlara, fabrikalara kadar her şeyi içerir. Nihayetinde siber güvenlik, demokrasi, insan hakları ve özgürlükler gibi temel toplumsal değerleri ve hedefleri korumayı içermektedir (İsveç, 2016).

Bilgi teknolojisi alanındaki tehdit ve risklerin ölçeği, özel şahıslar için daha az kapsamlı risklerden, toplumun işleyişinin hayati kısımlarına karşı iyi planlanmış ve hassas saldırılara kadar uzanmaktadır. Yazılım, donanımda veya işletim sistemlerinde çeşitli kesintiler yaygındır. Yangın, sel, kopmuş yer altı kabloları gibi harici fiziksel olaylar da tehdit senaryosunun bir parçasıdır.

Güvenlik açıklarını azaltmak ve İsveç'in bilgi ve iletişim teknolojileri politikasının hedeflerini desteklemek için, hükümetin değerlendirmesi, toplumun siber güvenlik çalışmalarının her şeyden önce geldiğinin göstergesidir. Bu amaçlar aşağıdaki gibidir (İsveç, 2016):

- Siber güvenlik çalışmalarında sistematik ve kapsamlı bir yaklaşım sağlamak,
- Ağ, ürün ve sistem güvenliğini artırmak,
- Siber saldırıları ve diğer bilgi ve iletişim teknolojileri olaylarını önleme, algılama ve yönetme becerisinin geliştirilmesi,
- Siber suçları önleme ve bunlarla mücadele olasılığını artırmak,
- Bilgiyi artırmak ve uzmanlığı teşvik etmek,
- Uluslararası işbirliğini geliştirmek.

Eylem planındaki ana hedefler ve alt amaçlar aşağıdaki gibidir (İsveç, 2016):

Siber Güvenlik Çalışmalarında Sistematik ve Kapsamlı Bir Yaklaşımın Güvence Altına Alınması: Bu hedef kapsamındaki alt gereklilikler aşağıdaki gibidir:

1. *Sistematik siber güvenlik çalışmaları:*
   a. Merkezi hükümet yetkilileri, belediyeler, il meclisleri, şirketler ve diğer kuruluşlar tehdit ve riskler hakkında bilgi sahibi olmalı, siber güvenliklerinin sorumluluğunu üstlenmeli ve sistematik siber güvenlik çalışmaları yürütmelidir.
   b. Sistematik siber güvenlik çalışmalarını desteklemek için ulusal bir model olmalıdır. Yapılacak faaliyetler;
      - ✓ Yönetişiminin netliğini artırılacak ve yetkililer nezdinde tatmin edici siber güvenlik çalışmalarının önemi vurgulanacak.
      - ✓ Sistematik siber güvenlik çalışmaları için ulusal bir modelin geliştirilmesi yoluyla, toplumdaki farklı paydaşların sistematik siber güvenlik çalışmaları yürütmesi ve tehdit, risk, güvenlik gibi önlemlerin değerlendirmelerinin yapabilmesi için koşulların iyileştirilmesi.
2. *İşbirliği ve bilgi paylaşımı:*
   a. İşbirliği ve siber güvenlik bilgi paylaşımı geliştirilecektir. Yapılacak faaliyetler;
      - ✓ Siber güvenlik alanında belirli görevleri olan yetkililer arasındaki işbirliği geliştirilecek.
      - ✓ Kamu ve özel sektör paydaşları arasında uygun bilgi paylaşımı ve işbirliği sağlanacak.
3. *Siber güvenlik alanında denetim:*
   a. Toplumun siber güvenliğini artıracak koşullar yaratmak için uygun denetim mekanizması sağlanmalıdır. Yapılacak faaliyetler;
      - ✓ Koruyucu güvenlik mevzuatının, kısmen yeterli bir yaptırım sistemi ve etkili bir denetim yoluyla, siber güvenlik alanındaki koruyucu güvenlik konusundaki değişen talepleri daha etkin bir şekilde karşılaması sağlanacak.
      - ✓ Eylem planının etkili bir şekilde uygulanması sağlanacak ve belirlenen sektörlerdeki belirli operatörler için kritik altyapıdaki ağ ve bilgi sistemlerinin güvenliğinin yeterli bir şekilde yönlendirilmesi ve denetlenmesi sağlanacak.
      - ✓ Toplum genelinde siber güvenliğin denetimini geliştirmek için daha fazla önlem alınması ihtiyacı izlenecek.

Ağ, Ürün ve Sistem Güvenliğini Geliştirmek: Bu hedef kapsamındaki alt gereklilikler aşağıdaki gibidir:

1. *Elektronik iletişim için güvenli altyapı oluşturma:*
    1. Elektronik iletişim ağları etkili, güvenli ve sağlam olmalı ve kullanıcılarının ihtiyaçlarını karşılamalıdır.
    2. İsveç'teki elektronik iletişim, ülke sınırları dışındaki işlevlerden bağımsız olarak sağlanacaktır.
    3. Denetim makamının yeterli önlemleri alabilme ihtiyacı karşılanmalıdır. Yapılacak faaliyetler;
        - ✓ Elektronik iletişim ağlarının diğer ülkelerdeki işlevlerden bağımsız olarak çalışabilecek şekilde kurulması sağlanacak,
        - ✓ Kamu düzeni, güvenlik, sağlık ve savunma alanlarındaki paydaşların modern, güvenli ve sağlam iletişim çözümlerine erişimi sağlanacak,
        - ✓ Ağların, ürünlerin ve sistemlerin tedariki ile ilgili olarak yetkililerin uzmanlığı artırılacak ve yetkililerin satın alımlarda güvenlik hususlarının dikkate alınmasını garanti etmesi sağlanacak,
        - ✓ Elektronik iletişim sektöründe yüksek düzeyde ağ ve siber güvenlik sağlamak için koşullar iyileştirilecek.
2. *Güvenli veri şifreleme sistemleri:*
    1. Bilgi ve iletişim teknolojileri ile iletişim çözümleri için güvenli veri şifreleme sistemlerine erişim, toplumun ihtiyaçlarını karşılamak içindir. Yapılacak faaliyetler;
        - ✓ Güvenli veri şifreleme sistemleri için ulusal bir strateji ve eylem planı uygulanacak.
3. *Endüstriyel bilgi ve kontrol sistemlerinde güvenlik:*
    1. Endüstriyel bilgi ve kontrol sistemlerinde güvenlik artacaktır. Yapılacak faaliyetler;
        - ✓ Endüstriyel bilgi ve kontrol sistemlerini içeren kritik altyapıya sahip olan veya onunla çalışan şirket ve yetkililerin siber güvenliği artırma çabalarında destek almaları sağlanacak.
        - ✓ Endüstriyel bilgi ve kontrol sistemlerinin önemli işlevlere sahip olduğu mühendislik ve işletme gibi sektörlerde faaliyet gösteren şirketlerin siber güvenlik çabalarını iyileştirmek için gelişmiş koşullar alması sağlanacak.

Siber Saldırılar, Diğer Bilgi ve İletişim Teknolojisi Olaylarını Önleme, Algılama ve Yönetme Becerisinin Geliştirilmesi: Bu hedef kapsamındaki alt gereklilikler aşağıdaki gibidir:

1. *Sistemin becerisinin geliştirilmesi:*
   a. Toplumdaki siber saldırıları ve diğer bilgi ve iletişim teknolojisi olaylarını önleme, tespit etme ve yönetme kapasitesi geliştirilecektir.
   b. İlgili paydaşlar, siber saldırıları ve diğer ciddi bilgi ve iletişim teknolojisi olaylarını yönetmek için koordineli eylemde bulunabilmelidir.
   c. İsveç'teki güvenlik açısından en hassas faaliyetler, siber uzaydaki nitelikli rakiplerin saldırılarını karşılama ve yönetme konusunda güçlendirilmiş bir askeri kabiliyete sahip gelişmiş bir siber savunma olacaktır. Yapılacak faaliyetler;
      - ✓ Bir siber saldırı veya diğer ciddi bir bilgi ve iletişim teknolojisi olayı durumunda yetkililer arasında koordineli planlama sağlanacak,
      - ✓ Sürekli izlemeye ihtiyaç duyan ve belirli koruma ihtiyaçları olan faaliyetlerin bir sensör sistemine veya algılama ve uyarı sistemine erişimi sağlanacak,
      - ✓ İsveç Silahlı Kuvvetlerinin siber uzaydaki nitelikli saldırganlara karşı İsveç'i savunma kabiliyetini geliştirmesini de içeren, hem askeri hem de sivil faaliyetler için siber saldırıları önleme, tespit etme ve yönetme kabiliyetine sahip etkili ve sorunsuz bir siber savunmanın sürekli geliştirilmesini ve güçlendirilmesi sağlanacak.

Siber Suçları Önleme ve Bunlarla Mücadele Olasılığını Artırmak: Bu hedef kapsamındaki alt gereklilikler aşağıdaki gibidir:

1. *Kolluk kuvvetleri, siber suçla etkili ve uygun bir şekilde mücadele etmek için hazırlıklı ve beceriye sahip olmalıdır.*
2. *Siber suçları önleme çalışmaları geliştirilecektir.* Yapılacak faaliyetler;
   - ✓ Siber suçla etkili bir şekilde mücadele etmesine izin verecek şekilde mevzuat uyarlanacak,
   - ✓ Kolluk kuvvetlerine, kişisel mahremiyetin ve hukuki kesinliğin korunmasına atıfta bulunarak, bilgi edinme kabiliyetlerini sürdürmeleri için koşullar sağlanacak,
   - ✓ Kolluk kuvvetlerinin siber suçları etkili bir şekilde önlemek ve bunlarla mücadele etmek için yeterli bir organizasyon ve yeterli kaynakları garanti etmesi sağlanacak,
   - ✓ Kolluk kuvvetlerinin siber suçları önlemek ve bunlarla mücadele etmek, uzmanlık ve çalışma yöntemleri geliştirmek için sistematik olarak çalışması sağlanacak,
   - ✓ Kolluk kuvvetleri dışındaki makamların siber suçları önleme çalışmalarına nasıl katkıda bulunabilecekleri konusunda farkındalığı ve bilgileri artırılacak,
   - ✓ İsveç'teki yasal işlemleri artırmak için siber suçlara karşı uluslararası işbirliği güçlendirilecek.

Bilgiyi Artırmak ve Uzmanlığı Teşvik Etmek: Bu hedef kapsamındaki alt gereklilikler aşağıdaki gibidir:

1. *Güvenlik açıklarının ve önlem ihtiyaçlarının haritalanması:*
   a. En acil güvenlik açıkları ve güvenlik önlemleri için ihtiyaçlar konusunda toplumun bir bütün olarak bilgisi artacaktır.
   b. Bireysel dijital teknoloji kullanıcılarının en acil güvenlik açıkları ve güvenlik önlemleri için ihtiyaçlar konusundaki bilgileri artacaktır. Yapılacak faaliyetler;
      - ✓ İlgili makamların, toplumdaki güvenlik açıklarının ve uygun güvenlik önlemlerinin haritalanması, araştırılması, uygulama ve destekleme çalışmalarını geliştirmeleri sağlanacak,
      - ✓ İnsanların güvenlik açıkları hakkındaki bilgilerini ve herkesin kendini korumak için alabileceği uygun güvenlik önlemleri artırılacak.
2. *Yükseköğretim, araştırma ve geliştirme faaliyetlerinin desteklenmesi:*
   a. İsveç'te siber güvenlik, bilgi ve iletişim teknolojileri ile telekomünikasyon güvenliği alanlarında yüksek kalitede yüksek eğitim, araştırma ve geliştirme yapılacaktır. Yapılacak faaliyetler;
      - ✓ Siber güvenlik alanında kullanımı ve yeniliği artırmak için yükseköğretim kurumları, endüstriyel araştırma enstitüleri, özel ve kamu sektörü arasındaki ortaklıklar geliştirilecek,
      - ✓ Tüm stratejik inovasyon ortaklık programlarında siber güvenliği hesaba alınacak.
3. *Eğitim faaliyetleri:*
   a. İsveç'in ciddi bilgi ve iletişim teknolojileri olaylarının sonuçlarını yönetme kabiliyetini artırmak için hem sektörler arası hem de teknik siber güvenlik eğitimi düzenli olarak gerçekleştirilecektir. Yapılacak faaliyetler;
      - ✓ Kuruluşlar arasındaki politikaları, planları, prosedürleri, ekipmanı ve anlaşmaları doğrulamak,
      - ✓ Personeli rolleri ve sorumlulukları konusunda eğitmek,
      - ✓ Kuruluşlar arasındaki koordinasyonu ve iletişimi geliştirmek,
      - ✓ Kaynak eksikliklerinin belirlenmesi ve
      - ✓ Hem bireysel hem de organizasyonel seviyelerde iyileştirme fırsatları belirlenecek.

Uluslararası İşbirliğini Geliştirmek: Bu hedef kapsamındaki alt gereklilikler aşağıdaki gibidir:

1. *Dış ve güvenlik politikası:*
    a. Özgürlük ve insan haklarına saygı ile karakterize edilen küresel, erişilebilir, açık ve sağlam internet hedefinin bir parçası olarak siber güvenlik konusunda uluslararası işbirliği geliştirilecektir. Yapılacak faaliyetler;
        - ✓ İsveç'in ilgili uluslararası süreçlerde (BM, AB, AGİT dahil ve NATO ile ortaklık dahil) ve benzer fikirlere sahip ülkelerle (İskandinav bölgesinde, çevre bölgede, AB içinde ve küresel ölçekte) bir paydaş olarak genel eylemler geliştirilecektir,
        - ✓ İnternetin parçalanmasına ve küresel akışların kısıtlanmasına yönelik eğilimlere karşı koyulacaktır,
        - ✓ İnternetin devlet tarafından yönetimine karşı koymak ve devlet dışı aktörlerin rolleri ve sorumlulukları korunacak,
        - ✓ Tehditleri ve açıkları yönetmek için siber güvenlik ve siber savunma konusunda uluslararası işbirliği geliştirilecek,
        - ✓ Uluslararası hukukun uygulanması ve çatışmaların önlenmesi konusunda uluslararası işbirliğini geliştirilecek,
        - ✓ İnsan haklarını ve küresel gelişimi desteklemek için açık, özgür ve güvenli bir internet teşvik edilecek.
2. *Ticaret ve ekonomik işbirliği:*
    a. Siber güvenlik, yenilikçiliği, rekabetçiliği ve toplumsal gelişimi desteklemek için serbest akışları koruma hırsının bir parçası olarak desteklenmelidir. Yapılacak faaliyetler;
        - ✓ İsveç'in, AB içindeki dijital liderliğini sürdürmek, dijital pazarı tamamlayarak ve gelecekteki konulardaki tartışmalarda itici bir güç olarak dijital gündemi ileriye taşınacak,
        - ✓ AB'nin aktif ve saldırgan bir şekilde dijital korumacılığa karşı koymasını ve aynı zamanda veri koruma ve ulusal güvenlik gibi meşru kamu çıkarlarına saygı göstermesi sağlanacak.

Hükümet bu eylem planındaki amacı, İsveç'in uzun vadeli siber güvenlik çabaları için açık bir platform oluşturmaktır. Strateji, ihtiyaç duyulduğunda, hedeflere ulaşılması için ilgili makamlara özel komisyonlar ve diğer yönlendirme önlemleri tarafından takip edilecektir. Teknoloji ve tehditlerin gelişimi, siber güvenlik alanının hızlı bir şekilde değiştiği ve geliştiği anlamına gelmektedir. Hükümetin amacı, stratejiyi yeni hükümlere ve İsveç hukukunda uygulanmasının diğer sonuçlarına uyarlamak için güncellemektir (İsveç, 2016).

4.18. Güney Kıbrıs'ın Siber Güvenlik Stratejisi

Güney Kıbrıs Cumhuriyeti'nin Siber Güvenlik Stratejisi belgesi dört bölümden oluşmaktadır. Bilgi, iletişim teknolojileri ve sistemleri, günümüzde sosyal ve ekonomik kalkınmanın en önemli itici güçlerinden biri olmakla birlikte, şüphesiz herhangi bir ülkede işlevsel ve sosyal yapıların işleyişi için de gerekli araçlardır. Bunun bir sonucu olarak, bilgilerin iletilmesi, işlenmesi ve depolanması sırasında gizlilik, bütünlük ve erişilebilirlik ilkelerinin korunması olarak tanımlanan bu teknolojilerin kullanımlarında güvenlik sunmaları için hayati bir önem taşımaktadır. Bu ilkeler, ekonominin değerli sektöründe sürekli gelişme ve büyüme için bir ön koşul olarak kabul edilen bilgi sistemleri ve elektronik hizmetlerde güvenin inşasına yol açar. Ağ ve bilgi güvenliği, daha genel olarak siber güvenlik, yukarıdaki ilkeleri sürdürmek için çalışır (Güney Kıbrıs, 2012).

Bu Strateji Belgesi, Güney Kıbrıs Cumhuriyeti'nde, kesintiye uğraması veya yok edilmesi hayati toplumsal işlevler üzerinde ciddi sonuçlar doğuracak kritik bilgi altyapılarının korunmasına yönelik belirli hususlar ve eylemlerle güvenli bir elektronik ortam oluşturmayı amaçlamaktadır. Bu Stratejinin geliştirilmesi ve hazırlanması, geçerli bir stratejinin birden fazla güvenlik düzeyi sunması gerektiğini kabul ederek, siber uzaydaki tehditlere yanıt vermek için bütünsel bir yaklaşım izlemiştir. Bu strateji belgesi, aşağıdaki alanlarda yukarıda tartışılan hedeflere ulaşmak için belirlenmiş bir dizi eylemi içermektedir (Güney Kıbrıs, 2012):

- Organizasyon yapıları,
- Yasal çerçeve,
- Kamu ve özel sektör arasında işbirliği,
- Kritik bilgi altyapılarının tanımlanması,
- Tehdit alanı analizi,
- Ulusal siber güvenlik çerçevesi,
- Olay yanıtı,
- Ulusal ve uluslararası siber tatbikatlar,
- Yetenek geliştirme,
- Farkındalık,
- Dış kuruluşlar ve uluslararası çalışma grupları ile işbirliği,
- Kritik bilgi altyapıları için ulusal acil durum planının geliştirilmesi,

- Karşılıklı bağımlılıkların modellenmesi ve analizi.

Bu belge ayrıca, alınacak önlemleri ve her bir eylem için ayrıntılı planlama ve maliyetlendirme, ulusal siber güvenliğin önceliklendirilmesi ve planlanması gibi takip edilmesi gereken sonraki adımları da analiz etmektedir. Programı ve takip edecek strateji eylemlerinin sonuçlarının değerlendirilmesini kapsamaktadır. Siber uzayda ortaya çıkan (ve görünmeye devam edecek) yeni tehditlerin yanı sıra değerlendirme sürecinin sonuçları dikkate alınarak, Güney Kıbrıs Cumhuriyeti'nin Siber Güvenlik Stratejisinin düzenli olarak gözden geçirileceğine dikkat çekmektedir. Bilgi ve iletişim teknolojisi dünyasında "güvenlik" genellikle üç ilkenin korunmasına atıfta bulunmaktadır (Güney Kıbrıs, 2012):

- Bilgilerin gizliliği, yani bilgilere yalnızca yetkili kişilerin erişmesine izin vermek,
- Bilgilerin bütünlüğü, yani bilgilerin herhangi bir istenmeyen değişiklik veya tahribattan korunması,
- Bilgi veya sistemlerin erişilebilirliği, yani bir sistemin talep edildiğinde hizmet ve/veya bilgi sağlayabilmesi için.

Yukarıdaki ilkelerin korunması, aşağıdakilerle ilgili olarak ağ ve bilgi güvenliğini mümkün olan en yüksek derecede sağlamayı amaçlamaktadır (Güney Kıbrıs, 2012):

- Geçiş halindeki bilgilerin/verilerin korunması,
- İşleme sırasında bilgi/verilerin korunması,
- Depolamadaki bilgilerin/verilerin korunması.

Hükümet tarafından sunulan bilgi sistemleri, iletişim ve diğer elektronik hizmetlere güven inşa etmek için altyapı, sistem ve bilgi korumasının ötesine geçerek, yukarıda açıklanan ilkelere göre yüksek düzeyde güvenliğin korunması gereklidir (Güney Kıbrıs, 2012).

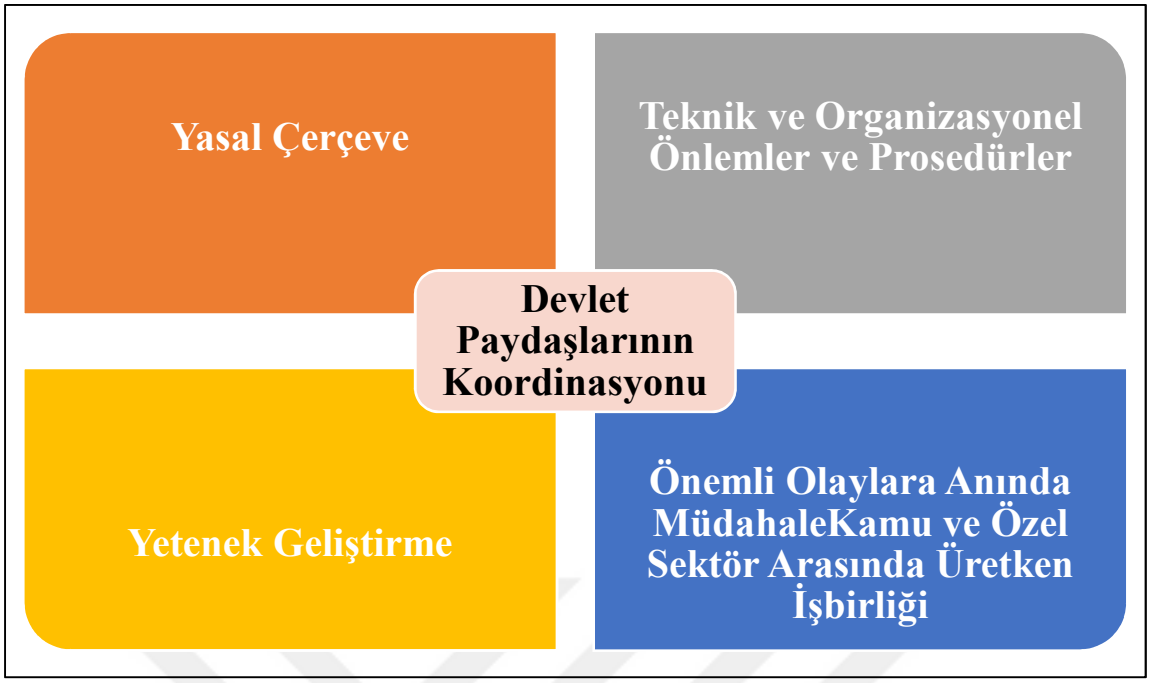
Kritik Bilgi Altyapıları açısından Güney Kıbrıs'ın son yıllarda bilgi altyapıları büyük ölçüde artmış ve ortalama bir vatandaşın hayatının neredeyse her alanına girmiştir. Güney Kıbrıs Cumhuriyeti Siber Güvenlik Stratejisinin vizyonu, bilgi ve iletişim teknolojilerinin her kullanıcının yararına gerekli güvenlik seviyelerinde işletilmesidir. Eylem planının amaçları ve hedefleri aşağıda sunulmuştur (Güney Kıbrıs, 2012):

- Güney Kıbrıs'ta güvenli ve emniyetli bir elektronik iş ortamının geliştirilmesi ve korunması,
- Bilgi toplumu için koşulların geliştirilmesi için "*Dijital Kıbrıs*" strateji programında belirlenen hükümet hedeflerinin desteklenmesi,
- Vatandaşlar ve kuruluşlar / işletmeler adına, bilgi ve verilerin aktarım, işleme ve depolama sırasında korunması da dahil olmak üzere e-devlet hizmetlerinde güvenin geliştirilmesi,
- Güney Kıbrıs Cumhuriyeti'nde çocuklar dahil tüm vatandaşları için güvenli bir elektronik ortamın oluşturulması,
- Siber uzaydaki tehditlerin etkilerinin azaltılması ve acil durumlara etkili müdahale,
- Güney Kıbrıs Cumhuriyeti'ndeki kritik altyapıların korunması için gelecekte koordine edilmiş bir ulusal müdahale planının desteklenmesi.

Bu belgenin yapısı ve içeriği aşağıdaki yol gösterici ilkelere dayanmaktadır (Güney Kıbrıs, 2012):

- Her bir hükümet paydaşının yetkilerini dikkate alarak, tüm yetkili makamlar arasında bir işbirliği çerçevesinde strateji ve politika geliştirilmesi,
- Siber uzaydaki tehditlerle yüzleşmek için bütünsel bir yaklaşımın geliştirilmesi,
- Geçerli bir stratejinin birden fazla güvenlik seviyesi sunması gerektiğinin kabul edilmesi (katmanlı güvenlik, derinlemesine savunma vb.),
- Stratejinin uygulanmasının tüm aşamalarında açık süreçlerin kullanılması ve
- Strateji iradesi ile iddialı hedeflerin belirlenmesi, Güney Kıbrıs'ta elektronik güvenlik seviyelerinin iyileştirilmesine somut bir şekilde katkıda bulunma eylemleri.

Güney Kıbrıs Cumhuriyeti'nin daha önce bahsedilen tehditlere stratejik tepkisi, kritik bilgi altyapılarının optimum düzeyde korunması için belirlenmiş bir dizi öncelik alanına bölünebilir. Aşağıdaki şekilde gösterildiği üzere Kıbrıs Cumhuriyeti'nin ihtiyaçları ile ilgili olarak öncelik verilen alanlar şunlardır (Güney Kıbrıs, 2012):



Şekil 4.18. Güney Kıbrıs Cumhuriyeti siber güvenlik stratejisinin öncelikleri

Ağ ve bilgi güvenliği alanı çok geniş ve karmaşık bir konudur ve bir dizi paydaşı içerir. Her yetkili veya ilgili makamın kendi sorumluluk alanları vardır ve bu farklılıkları sürdürmek önemlidir (Güney Kıbrıs, 2012).

- Eylem 1- Aşama A- Elektronik Haberleşme ve Posta Düzenleme Komiseri Ofisi (Office of the Commissioner of Electronic Communications and Postal Regulation/OCECPR) ile kamu otoriteleri arasında işbirliği ve bilgi alışverişi çerçevesinin oluşturulması. Böylece OCECPR, ülkenin siber güvenlik ve kritik bilgi altyapılarının korunması alanındaki stratejik müdahalesini etkin bir şekilde koordine edecek bir konumda olacaktır.
- Eylem 2- Aşama A- OCECPR, uygun zamanda ve diğer yetkili makamlarla işbirliği içinde, Güney Kıbrıs Cumhuriyeti'nin çabalarını tam olarak koordine edecek bir konumda olması, yeniden düzenlenmesi için yeni politikaya ilişkin bir rapor geliştirecektir. Tüm eylemlerin optimum şekilde uygulanması ve denetlenmesi, günümüzde siber uzayda yaygın olan tehditlere ve gelecekte ortaya çıkması muhtemel tehditlere etkili yanıt verilmesi için kullanılır.
- Eylem 3- Aşama A/B- Strateji Eylemlerini uygulamak için (gerektiği şekilde) kamu ve özel sektör temsilcileriyle çalışma gruplarının oluşturulması.

- Güney Kıbrıs Cumhuriyeti'ndeki mevzuat, ağ ve bilgi güvenliğinin yanı sıra siber suç (ve diğer elektronik suçlar) ile ilgili çok sayıda alanı kapsamaktadır. Ancak, yine de Güney Kıbrıs'taki tüm ilgili yasaların belirlenmesi, gerektiğinde güncellenmesi ve ayrıca bu Stratejinin tüm hükümlerini kapsayacak şekilde yeni birincil ve ikincil mevzuatın oluşturulmasının teşvik edilmesi gerekli görülmektedir.
- Eylem 4- Aşama B- Siber Güvenlik Stratejisinin hükümlerini tam olarak desteklemek için uygun bir yasal çerçevenin oluşturulması. Yetkili makamların tüm ilgili yasaları, herhangi bir mevcut ihtiyaç için değerlendirilmelidir.
- Eylem 5- Aşama A/B- Güney Kıbrıs Cumhuriyeti'nde elektronik güvenlik seviyelerinin iyileştirilmesine olumlu bir şekilde katkıda bulunabilecek grupların ve paydaşların belirlenmesi için özel sektörün kapsamlı araştırması ve eşzamanlı olarak yakın işbirliğine dayalı ilişkiler geliştirmek.
- Eylem 6- Aşama B- Güney Kıbrıs Cumhuriyeti'nde kritik bilgi altyapısının korunması alanında dinamik bir PPP (Kamu-Özel Ortaklığı) oluşturma olasılığı araştırılacak ve uluslararası forumlara katılım yoluyla uluslararası kuruluşlarla aktif işbirliğini teşvik edilecek. Bu belgede vurgulanan ve açıklandığı üzere kritik bilgi altyapılarının korunması ihtiyacı, kötü niyetli eylemlerin veya doğal afetlerin altyapı üzerindeki olumsuz etkilerini ve olası yıkıcı sonuçlarını, Güney Kıbrıs Cumhuriyeti içinde ulusal düzeyde en aza indirmek için gereklidir. Her paydaş (elektronik iletişim şirketleri, devlet daireleri ve hizmetleri, güvenlik güçleri, silahlı kuvvetler, hastaneler, finans kurumları, enerji ve su sağlayıcıları, vb.) altyapılarını hayati derecede önemli olarak görecek ve ideal durum, istisnasız Güney Kıbrıs Cumhuriyeti'ndeki tüm bilgi altyapılarını kapsayacaktır.
- Eylem 7- Aşama A- Hem kamu hem de özel sektörün katkılarıyla, Güney Kıbrıs Cumhuriyeti'ndeki kritik bilgi altyapılarının, korunmalarına yönelik faaliyetleri ve eylemleri daha iyi hedeflemek için tanımlanması ve değerlendirilmesi.
- Güney Kıbrıs'ta ortaya çıkan ve gelecekte artabilecek özel tehdit karışımlarına ilişkin mevcut bilgilerin sınırlı olduğunu belirtmek önemlidir. Bilgi altyapılarının korunması yalnızca genel önlemlerle (bir dereceye kadar) sağlanabilir, ancak siber uzaydaki tehditlere stratejik tepki, Güney Kıbrıs'ta fiilen mevcut ve belirgin olan ana tehditler bilinir hale gelirse büyük ölçüde iyileştirilecektir.

- Eylem 8- Aşama B- Güney Kıbrıs'ta yayınlanan siber uzaydaki mevcut tehditleri ve saldırıları kaydetmenin yanı sıra Avrupa ve uluslararası alanda ortaya çıkan yeni tehditleri izlemek için kapsamlı anket düzenlenmesi.

Güney Kıbrıs Cumhuriyeti'ndeki tüm kritik bilgi altyapılarında kabul edilebilir bir güvenlik düzeyine ulaşmanın en kolay ve en etkili yöntemi, kritik bilgi altyapılarının korunması ve bilgi güvencesi için temel olarak kullanılacak bir Ulusal Siber Güvenlik Çerçevesi geliştirmektir. Bu çerçeve, uluslararası güvenlik standartlarına dayalı olarak geliştirilmeli ve aşağıdakileri (diğerleri arasında) içermelidir:

- Yönetişim ve risk yönetimi
- Güvenlik açığı değerlendirmesi
- Düzenli sızma testi
- Fiziksel alanların, donanımın ve yazılımın yönetimi
- Uygun personel yetkilendirmesi
- Fiziksel güvenlik ve çevre yönetimi
- Olay yönetimi için Computer Emergency Response Teams (CERT) kullanılması
- Devam eden olayları tespit etmek amacıyla kötü niyetli saldırılar için elektronik iletişimin sürekli izlenmesi.

- Eylem 9- Aşama B- Güney Kıbrıs Cumhuriyeti'ndeki kritik bilgi altyapılarının yanı sıra devlet daireleri ve hizmetlerinin korunmasını teşvik edecek bir Ulusal Siber Güvenlik Çerçevesinin Geliştirilmesi.
- Kıbrıs'taki Bilgisayar Acil Durum Müdahale Ekiplerinin tam işlevselliğini sağlamak, bu Stratejinin ayrılmaz ve hayati bir parçasıdır. Ayrıca bir ulus olarak taahhütlerimizi yerine getirmenin bir parçasıdır.
- Eylem 10- Aşama A- Hükümetlerin CERT/CSIRT operasyonu için acil öncelik ile Bilgisayar Acil Durum Müdahale Ekiplerinin (CERT'ler/CSIRT'ler) tam işlevselliği sağlanacaktır. İlgili Avrupa çalışma gruplarına katılımlarını sağlamak için gerekli sertifikalar ve üyelikler alınacaktır.
- Eylem 11- Aşama B- OCECPR tarafından, CERT'ler/CSIRT'ler ile işbirliği içinde, faaliyetlerini genişletme veya özel sektörün ve iş dünyasının ihtiyaçlarını karşılamak için değerlendirmesi.

Hem kamu hem de özel sektörde hükümet ve farklı paydaşlar arasındaki önemli işbirliği ihtiyacı artmıştır. Bu işbirliğinin ve özellikle bağlantılı güvenin geliştirilmesi son derece önemlidir.

- Eylem 12- Aşama A- Giderek gerçekçi senaryolar ile düzenli ulusal siber güvenlik uygulamalarının planlanması ve organizasyonu ve ayrıca pan-Avrupa ve diğer uluslararası siber alıştırmalara aktif katılım.

Bu nedenle, hükümet aşağıdaki eylemler yoluyla elektronik güvenlik alanında uygun personel eğitimini destekleyecektir:

- Uygun (ve mevcut) eğitim programları ve sertifikalarının belirlenmesi,
- Bu tür programların hükümet içinde benimsenmesini teşvik etmek,
- Gerekli uzmanlık bilgisi ile uygun iş gücünün oluşturulması,
- Elektronik güvenlikle ilgili iş tanımlarına ilgili sertifika ve deneyimlerin dahil edilmesi,
- Elektronik güvenlik konularının müfredatlarına ve ilgili araştırma programlarının enstitüsüne dahil edilmesi yoluyla, ağ ve bilgi güvenliği alanındaki Kıbrıs yüksek öğretim kurumlarındaki faaliyetleri desteklemek.

- Eylem 13- Aşama B- Bu Stratejinin hükümlerini orta ve uzun vadede üst düzeyde uygulamak için gerekli teknik bilgi ve sertifikalara sahip olacak uygun insan kaynaklarının geliştirilmesi ve bu beceri ve sertifikaların dahil edilmesi ilgili pozisyonlar için iş tanımlarına uyumlaştırılması.

Siber güvenliğe yönelik potansiyel tehditlerin boyutları, ağa bağlı herhangi bir bilgisayarın siber uzaya bir giriş noktası veya kötü niyetli ve/veya zararlı unsurlar olarak hizmet verebileceği göz önüne alındığında, bu sorunun tüm bilgi altyapısı kullanıcılarını ilgilendirdiğini açıkça göstermektedir. Güney Kıbrıs Cumhuriyeti, siber güvenlik konuları için aşağıdakileri içeren bir Ulusal Farkındalık Programını teşvik edecektir:

- Kişisel verilerin korunmasına, siber alandaki etik davranışa ve korumaya odaklanarak, vatandaşlar için güvenli İnternet kullanımı ile ilgili olarak harici kaynak materyallerinin yanı sıra bilgi materyalinin oluşturulması,

- Bu bilgilendirici materyalin birden fazla medya aracılığıyla dağıtımı, örn. televizyon, radyo, SMS, web siteleri, broşürler / kitapçıklar, konferanslar vb.
- Çalışan profesyoneller için küçük süreli eğitim seminerlerinin geliştirilmesi,
- Hassas ve/veya sınıflandırılmış bilgiler içeren bilgi ve iletişim teknolojileri sistemlerinin devlet kullanıcıları için özel eğitim seminerlerinin geliştirilmesi,
- Tüm devlet dairelerinde ve hizmetlerinde ve ayrıca özel işletmelerde pozitif bir güvenlik kültürünün geliştirilmesinin teşvik edilmesi.

- Eylem 14- Aşama B- Devlet çalışanlarından devlet vatandaşlarına kadar elektronik sistemlerin tüm kullanıcılarını kapsayan, siber güvenlik konuları için kapsamlı bir Ulusal Farkındalık Programının geliştirilmesi.

Güney Kıbrıs Cumhuriyeti'nde siber uzayın güvenliğini sağlamaktan sorumlu ana organın diğer paydaşlarla işbirliği sadece bir seçim değil, gerekli hedeflere ve sonuçlara ulaşmak için kesinlikle gerekli hale geldi. Siber uzaydaki sorunlar ve tehditler tek başına tek bir ülke tarafından tam anlamıyla hafifletilemez. Bu nedenle, Avrupa düzeyinde devletlerarasında yapıcı işbirliği gereklidir.

- Eylem 15- Aşama A- Güney Kıbrıs Cumhuriyeti, temsili ve ilgili çalışma gruplarına ve forumlarına aktif katkıları yoluyla, Avrupa Birliği üye devletlerinin geri kalanıyla yapıcı işbirliğini geliştirmeye devam edecektir. Bu işbirliği, tüm Avrupa'da siber güvenlik seviyesini iyileştirmek için Birlik düzeyindeki eylemleri ve faaliyetleri destekleyecektir.

Ulusal Acil Durum Planının oluşturulması ve geliştirilmesi, Güney Kıbrıs Cumhuriyeti'ndeki kritik bilgi altyapılarının belirlenmesi ile birlikte gerçekleştirilecek ve aşağıdaki faaliyetleri içerecektir:

- Kritik altyapıların kategorilerinin ve hiyerarşilerinin, bilgi ve iletişim hizmetlerinin işletilmesine katkılarına göre belirlenmesi,
- Olası hasar veya yıkımın etkilerini en aza indirmek için bu altyapının her bir parçası için gerekli koruma seviyesinin belirlenmesi (örneğin fazlalık, alternatif yollar, fiziksel güvenlik vb.),

- Potansiyel olarak kritik altyapıların izlenmesine yönelik erken uyarı sistemleri ve süreçlerinin geliştirilmesi,
- Ana ağlardan bağımsız ve mümkünse tamamen alternatif iletişim araçları (örneğin kablolu, mobil ve uydu ağları) kullanarak acil durum iletişim ağlarının oluşturulması (veya halihazırda mevcut olanların iyileştirilmesi),
- Olası bir krizin üstesinden gelmek ve aralarında yapıcı işbirliğini sağlamak için kritik bilgi altyapısı operatörleri arasında kapsamlı iletişim ve yönetim süreçlerinin geliştirilmesi,
- Diğer ülkelere bağlı olan veya diğer ülkelerdeki bilgi altyapılarını etkileyebilecek hizmetler sunan tüm kritik bilgi altyapılarının belirlenmesi,
- Bu kaynak metin hakkında daha fazla bilgi elde edilmesi,
- İlgili departmanlar ve hizmetler arasında yararlı veya gerekli görüldüğünde ekipman ve altyapı açısından mevcut kaynakların belirlenmesi ve acil durumlarda birbirlerinin kaynak ve hizmetlerini kapsayacak sinerji yaratılması.

- Eylem 16- Aşama A- Büyük ölçekli bir krizin Güney Kıbrıs Cumhuriyeti'ndeki kritik bilgi altyapılarının operasyonlarını önemli ölçüde etkilemesi durumunda alınacak önlemleri ve ayrıntılı süreçleri içerecek bir Ulusal Acil Durum Planının geliştirilmesi, tam restorasyona kadar operasyonlarını kabul edilebilir seviyede sürdürmek.

Başarılı bir şekilde tamamlanması için her birinin kendine özgü ve ayrı hedefleri olmasına rağmen, açıklanan eylemler arasındaki karşılıklı bağımlılıklara ve etkileşimlere özel bir vurgu yapmaktadır.

- Eylem 17- Aşama A/B- Bu Stratejinin uygulanması için var olan karşılıklı bağımlılıkların belirlenmesi ve incelenmesi. Bu karşılıklı bağımlılıklar başlangıçta eylemlerin kendileri, devletin yetkili makamları arasındaki ilişkiler ve kritik altyapı operatörleri ile tedarikçileri, müşterileri ve personeli arasındaki ilişkilerde mevcut olarak tanımlanacaktır. Bu karşılıklı bağımlılıklar ilgili tüm paydaşlar tarafından tanınmalı ve kabul edilmelidir.

Münferit eylemlerin ayrıntılı değerlendirmesi ve analizi bağlamında, uygulanabilir olduğu noktaya kadar, her bir eylemin uygulanmasının maliyeti ve belirli bütçe kalemlerinin gerekli olacağı zaman dilimleri belirlenecektir. Bu maliyetlendirme süreci, yetkili makamlarla

işbirliği içinde gerçekleştirilecek ve maliyetlendirmenin olabildiğince gerçekçi olabilmesi için, her bir eylemin ve uygulamanın kapsamının önemi her zaman göz önünde bulundurulacaktır.

4.19. Çekya'nın Ulusal Siber Güvenlik Stratejisi

Çek Cumhuriyeti'nin 2015- 2020 Dönemi Ulusal Siber Güvenlik Stratejisi Belgesi dokuz ana bölümden oluşmaktadır. İnsan eylemleri ve faaliyetleri, fiziksel çevreden siber uzaya giderek daha fazla hareket etmektedir. Bilgi ve iletişim teknolojileri, son on yılda, iletişimi, paylaşımı, bilgi ve hizmetlere erişimi önemli ölçüde kolaylaştırarak hayatımızın neredeyse her alanını değiştirmiştir. Bu gerçekten yola çıkan Çekya Ulusal Güvenlik Kurumu 2011 yılından bu yana siber güvenlik alanında koordinatör ve ulusal otorite olarak faaliyet göstermektedir. Kamu sektörü ile toplumun geri kalanı arasında derin karşılıklı güven ve işbirliği olmadan siber güvenlik sağlanamaz. Aşağıda strateji belgesinin vizyonları yer almaktadır (Çekya, 2015):

- Çekya, sorunsuz işleyen bir bilgi toplumu için siber uzay içinde yeni koşullar yaratacaktır.
- Çekya, siber güvenlik uzmanlığının ve en yeni siber tehditlere direnme yeteneklerinin sürekli olarak geliştirilmesini hedefleyecektir. Aynı zamanda devlet güvenlik güçlerinin önleme ve erken uyarı kapasitelerini destekleyecek ve geliştirecektir.
- Çekya, modern bir Orta Avrupa ülkesi ve AB, NATO, BM ve diğer uluslararası kuruluşların aktif bir üyesi olarak lider bir rol oynamayı amaçlayacaktır.
- Çekya, siber saldırıları önleme ve çözme konusunda uluslararası ortaklarını aktif olarak destekleyecek, uluslararası örgütlere üyelik ve NATO içindeki toplu savunmadan doğan taahhütlerini yerine getirecek ve diğer devletlerin güvenliğini teşvik edecektir.
- Çekya, uluslararası kuruluşlara üyeliği yoluyla, Orta Avrupa ülkeleri arasında siber güvenliği, savunma işbirliğini ve diyaloğu aktif olarak teşvik edecektir.
- Çekya, kritik bilgi altyapısının yalnızca tek tek unsurlarını etkin bir şekilde güvence altına almakla kalmayacak, aynı zamanda nüfus tarafından kullanılan ağların ve siber uzayın genel güvenliğini de sağlayacaktır. Bunlar ülkenin ekonomik ve sosyal çıkarları için çok önemlidir.

- Çekya, özellikle kritik bilgi altyapısında yer alan endüstriyel kontrol sistemlerinin güvenliğini sağlamaya odaklanacak ve birkaç yıl içinde edinilen uzmanlık ve bilgi sayesinde bu alanda önde gelen ülkelerden biri haline gelecektir.
- Çekya, güven oluşturmaya ve verimli bir işbirliği modeli geliştirmeye çalışırken, aynı zamanda diğer siber güvenlik ekipleri için bir şemsiye otorite olarak işlev görecek ve bunların oluşturulmasını ve geliştirilmesini teşvik edecektir.
- Çekya, bilgi ve iletişim teknolojilerinin güvenliği ile ilgili araştırma ve geliştirme faaliyetlerinde özel sektör ve akademi ile işbirliği yapacaktır.
- Çekya, maksimum siber uzay güvenliğini sağlamak için çaba gösterecektir. Buna paralel olarak, yüksek teknolojilerin üretimini, araştırmasını, geliştirilmesini ve uygulanmasını destekleyecektir. Böylelikle rekabet gücünü artırmak ve işlevsel bir bilgi altyapısının bulunduğu yerel ve uluslararası yatırımlar için en uygun koşulları yaratmak amacıyla Çekya'daki teknolojik gelişmeye katkıda bulunacaktır.
- Çekya, vatandaşları ve özel sektör konuları arasında farkındalık yaratarak bilgi toplumu kültürünün gelişmesini teşvik edecektir. Bilgi toplumu hizmetlerine ve sorumlu davranış ve bilgi teknolojilerinin kullanımına ilişkin bilgilere ücretsiz erişime sahip olacaklardır. Vatandaşlar, yaşam kalitelerini ve devlete olan güvenlerini olumsuz etkileyebilecek siber saldırıların kötü niyetli etkilerinden korunacaktır.

Strateji belgesinde Çekya dört adet temel prensip belirlemiştir. Bu prensipler; (a) temel insan hak ve özgürlüklerinin ve demokratik hukukun üstünlüğü ilkelerinin korunması, (b) yetki ikamesi ve işbirliği ilkelerine dayalı siber güvenliğe kapsamlı yaklaşım, (c) kamu ve özel sektör ile sivil toplum arasında güven oluşturma ve işbirliği ve (d) siber güvenlik kapasitesi oluşturma şeklindedir. 2015- 2020 Dönemi Ulusal Siber Güvenlik Stratejisi Belgesinde ülkenin karşı karşıya olduğu on dokuz adet engel veya zorluk tespit edilmiştir. Söz konusu zorluklar özetle aşağıdaki gibidir (Çekya, 2015):

1. *Potansiyel bir test alanı:* Çekya, diğer ülkeler tarafından da kullanılan gelişmiş güvenlik teknolojilerini kullanan bir ülkedir.
2. *Halkın devlete olan güveninin eksikliği:* Kamuoyunun siber güvenliğini sağlayan kuruluşlar olarak devletlere ve onların güvenlik yapılarına olan güveni son zamanlarda önemli ölçüde azalmıştır.
3. *İnternet, bilgi ve iletişim teknolojileri kullanıcılarının sayısının artması ve teknoloji arızalarının kritikliğinin artması:* Kamu ve özel sektörün artan bilgi ve iletişim

teknolojileri bağımlılığı ile birlikte artan sayıda internet kullanıcısı bu tür teknolojilerin potansiyelinin artan bir kritikliğini taşımaktadır.

4. *Mobil cihaz kullanıcılarının sayısıyla birlikte artan mobil kötü amaçlı yazılım miktarı:* Çok az akıllı telefon ve tablet kullanıcısı, en azından temel güvenlik araçlarını (ör. antivirüs yazılımı) kullanır.
5. *Bir donanımda arka kapıdan olası bilgi hırsızlığı:* Artan sayıda teknoloji kullanıcısı ve sağlayıcı, donanıma bilinçli olarak yerleştirilmiş "arka kapılar" riskini taşımaktadır.
6. *Nesnelerin interneti:* Çevrimiçi cihazların sayısı artarken, çoğu kullanıcı gerekli dijital hijyeni, yani çevrimiçi olarak nasıl davranılacağını ve kullandıkları cihazları nasıl koruyacaklarını görmezden geliyor.
7. *IPv4'ten IPv6'ya geçişle ilgili güvenlik riskleri:* IPv4'ten IPv6 protokolüne gerekli geçiş, yeni siber güvenlik risklerini beraberinde getirir.
8. *Kamu yönetiminin elektronik hale getirilmesiyle ilgili güvenlik riskleri (e-devlet):* Çekya'da kamu yönetiminin devam eden dijitalleşmesi, işleyişini ve halkla ilişkisini iyileştirmeyi amaçlamaktadır.
9. *Küçük ve orta ölçekli işletmelerin yetersiz güvenliği:* Küçük ve orta ölçekli işletmelerde bilgi altyapısının korunması ve güvenli bilgi işlemenin en iyi uygulamaları ve yöntemleri hakkında farkındalık yaratma ve böylece siber saldırılarla başa çıkmalarına yardımcı olma ihtiyacı giderek artmaktadır.
10. *Büyük veri, yeni veri depolama ortamları:* Verilerin, özellikle kamu yararına olanların korunması ve güvenliği Çekya için çok önemlidir.
11. *Sağlık sektöründe endüstriyel kontrol sistemlerinin ve bilgi sistemlerinin korunması:* Siber saldırılar, odaklarını doğrudan finansal faydadan endüstriyel siber casusluğa, siber vandalizme ve güvenlik açıklarının belirlenmesine kaydırmaktadır.
12. *Akıllı şebekeler:* Çekya'nın enerji dağıtım ağının geliştirilmesi potansiyel bir sonraki adımı oluşturmaktadır.
13. *Devletin savunma güçlerinin artan bilgi ve iletişim sektörü bağımlılığı:* Bu teknolojilerin güvenlik açıkları ve siber saldırı da dahil olmak üzere kesintiye uğrama veya imha tehlikesi, kuvvetlerin temel savunma yetenekleri NATO ve AB üyeliğinden kaynaklanan taahhütlerin yerine getirilmesi üzerinde olumsuz etki riskini artırmaktadır.
14. *Giderek daha karmaşık hale gelen kötü amaçlı yazılım:* Kötü amaçlı yazılımların ve saldırganların giderek artan karmaşıklığı, saldırı kaynağı izleme seçeneklerini, yani tersine mühendislik ve adli analiz (geri izleme) seçeneklerini önemli ölçüde sınırlar.

15. *Bot ağları ve DDoS / DoS saldırıları:* Çok yaygın DDoS / DoS saldırıları için kullanılan bot ağları sağlamlık, dayanıklılık ve gizlilik kazanıyor.
16. *Siber suçta artış:* İnternetin açık ve anonim doğası nedeniyle, hassas bilgilerin ticareti, erişilebilirlik ve hatta suç faaliyetlerinin ücretsiz satın alınması olasılıkları artmaya devam ediyor. Tüm bunlar, hassas bir şekilde hedeflenmiş ve aynı zamanda toplu ve geniş yüzey saldırıları izin verir.
17. *Çevrimiçi sosyal ağların kullanımıyla ilgili tehditler ve riskler:* Artan sayıda sosyal ağ kullanıcısı, hem gerçek hem de tüzel kişileri hedef alan özel veri hırsızlığı ve hatta dijital kimlik hırsızlığı riskinin artmasına neden olur.
18. *Son kullanıcıların düşük dijital okuryazarlığı:* Hem kamu sektöründe hem de özel sektörde önemli sayıda internet kullanıcısı, yaygın bilgisayar saldırı yöntemleri (özellikle kimlik avı, sahte e-mağazalar vb.) hakkında temel bilgilerden yoksundur.
19. *Siber güvenlik uzmanlarının eksikliği ve müfredat reformuna duyulan ihtiyaç:* Siber güvenlik alanındaki mevcut Çek eğitim modeli, mevcut ihtiyaçları ve eğilimleri karşılamıyor.

Yukarıdaki zorluklar ülkenin düzeltilmesini amaçladığı konular kapsamındadır. Söz konusu konular oldukça geniş kapsamlı ve farklı alanları içermektedir. Genel olarak ülkeler mevcut eksikliklerini veya zayıf yönlerini kamuoyuna açıklamazlar. Ancak Çekya kendi eksikliklerini planda açıklamıştır. Eylem Planındaki hedefler özetle aşağıdaki gibidir (Çekya, 2015):

<u>Ana Hedef A. Siber Güvenliğin Sağlanmasında İlgili Tüm Yapıların, Süreçlerin ve İşbirliğinin Etkinliğinin Sağlanması ve İyileştirilmesi</u>

a. Ulusal düzeyde siber güvenlik aktörleri arasında etkili bir işbirliği modeli geliştirmek ve mevcut yapılarını ve süreçlerini güçlendirmek.
b. Bir işbirliği formatı belirleyecek, bir iletişim matrisi, bir prosedür protokolü içerecek ve her bir aktörün rolünü tanımlayacak bir ulusal olay ele alma prosedürü geliştirmek.
c. Eyalet düzeyinde bir risk değerlendirme metodolojisi geliştirmek.
d. Çekya'nın siber güvenlikle ilgili diğer departmanlarla koordine edilecek siber güvenlik konularında harici pozisyonlarına tutarlı bir yaklaşım sürdürmek.
e. Ulusal stratejik ve güvenlik belgelerini hazırlarken veya incelerken siber tehditlerin sürekli gelişimini uygun bir şekilde yansıtmak.

Ana Hedef B. Aktif Uluslararası İşbirliği

a. AB, NATO, BM, AGİT, Uluslararası Telekomünikasyon Birliği ve diğer uluslararası kuruluşların forumlarında, programlarında ve girişimlerinde yer alan uluslararası tartışmalara aktif olarak katılmak.
b. Orta Avrupa bölgesinde siber güvenliği ve devletlerarası diyaloğu teşvik etmek.
c. Diğer devletlerle ikili işbirliği kurmak ve derinleştirmek.
d. Uluslararası tatbikatlara katılmak ve düzenlemek.
e. Uluslararası eğitimlere katılmak ve düzenlemek.
f. Etkin bir işbirliği modelinin oluşturulmasına ve uluslararası düzeyde, uluslararası kuruluşlar ve akademik çevrede güven oluşturmaya katılmak.
g. Resmi ve gayri resmi yapılar içinde, yasal düzenlemeler ve siber alandaki davranış, açık bir internetin korunması,insan hakları ve özgürlükleri konusunda uluslararası bir fikir birliğinin geliştirilmesine katkıda bulunmak.

Ana Hedef C. Ulusal Kritik Alt Yapıların Korunması

a. Açıkça tanımlanmış bir protokole dayalı olarak güvenliğinin sürekli analizini ve kontrolünü takip etmek.
b. Çekya'da yeni ekiplerin oluşturulmasını desteklemek.
c. Siber ağlarının direncini, bütünlüğünü ve güvenilirliğini sürekli olarak geliştirmek.
d. Çekya'daki tehditleri ve riskleri sürekli olarak analiz etmek ve izlemek.
e. Devlet ile siber güvenlik konuları arasında bilgiyi verimli bir şekilde paylaşmak.
f. Personeline sürekli eğitim ve öğretim sağlarken, Ulusal Siber Güvenlik Merkezi'nin teknolojik kapasitelerini ve yeteneklerini artırmaya devam etmek.
g. Devlet tarafından kurulacak ve yönetilecek bir kritik altyapı veri depolama ortamını kapsamlı ve güvenilir bir şekilde güvence altına almak.
h. Kritik altyapı sistemlerine yönelik sızma testi ilkelerine dayalı olarak, devlet tarafından kullanılan bilgi sistemleri ve ağlarındaki hataları ve güvenlik açıklarını düzenli olarak test etmek ve tespit etmek.
i. Siber saldırılara aktif şekilde karşı koymak (bastırma) için teknolojik ve organizasyonel ön koşulları sürekli olarak geliştirmek.
j. Aktif siber savunma ve siber saldırılara karşı önlemler için ulusal kapasiteleri artırmak.
k. Siber güvenlik ve siber savunmada aktif karşı önlem soruları ve genel olarak siber güvenliğe saldırgan yaklaşım konusunda uzmanlaşmış uzmanlar yetiştirmek.

l. Siber Güvenlik Yasası uyarınca ilan edilen siber olağanüstü halden 110/1998 Coll., Çek Cumhuriyeti Güvenlik Hakkında Anayasa Yasası'nda tanımlanan eyaletlere geçiş için bir prosedür geliştirmek.

Ana Hedef D. Özel Sektörle İşbirliği

a. Özel sektör ile işbirliğine devam etmek ve kamu kurumlarının siber güvenlik alanındaki faaliyetleri hakkında genel farkındalığı artırmak.
b. Özel sektörle işbirliği içinde, güvenlik normları oluşturmak, işbirliğini standartlaştırmak.
c. Tüm Çek şirketlerinin rekabet gücünü desteklemek ve yatırımlarını korumak için bilgi paylaşımı, araştırma ve geliştirme için güvenilir bir ortam sunan ve güvenli bir bilgi altyapısı sağlayan özel sektörle işbirliği içinde bir siber uzay sağlamak.
d. Eğitim vermek ve özel sektörün siber güvenlik bilincini artırmak.
e. Tehditlere, olaylara ve yakın tehlikelere ilişkin bilgi paylaşımı için ulusal bir platform/sistem oluşturulması da dahil olmak üzere özel sektör ve devlet arasında güven oluşturmak.

Ana Hedef E. Araştırma ve Geliştirme / Tüketici Güveni

a. Siber güvenlikle ilgili ulusal ve Avrupa araştırma projelerine ve faaliyetlerine katılmak.
b. Ulusal Siber Güvenlik Kurumu (National Security Authority/NSA)'nu siber güvenlik araştırmaları için ana irtibat noktası olarak belirlemek.
c. Maksimum koruma ve şeffaflıklarını sağlamak için özel sektör ve akademi ile devlet tarafından kullanılan teknolojilerin geliştirilmesi ve uygulanması konusunda işbirliği yapmak.
d. Araştırma projeleri (birincil ve deneysel araştırmalar dahil) ve teknik disiplinler, sosyal bilimlerdeki faaliyetler konusunda özel sektör ve akademik çevrelerle ulusal, Avrupa ve uluslararası, transatlantik düzeylerde işbirliği yapmak.
e. Araştırma ve geliştirmeyi ulusal bir öncelik haline getirmek ve böylece bu alandaki yatırımları aktif olarak teşvik etmek.

Ana Hedef F. Eğitim, Bilinçlendirme ve Bilgi Toplumu Geliştirme

a. Destek inisiyatifleri, farkındalık kampanyaları, kamu konferansları vb. organize ederek ilk ve ortaokul öğrencilerinin ve son kullanıcıların siber güvenlik bilincini ve okuryazarlığını artırmak.
b. Mevcut ilk ve orta öğretim müfredatını modernize etmek ve siber güvenlik uzmanları yetiştirmek için tasarlanmış yeni üniversite eğitim programlarını desteklemek.
c. Siber güvenlik ve siber suç alanında yer alan kamu idaresi personeline ilgili eğitim ve öğretim sağlamak.

Ana Hedef G. Siber Suç Soruşturması ve Kovuşturması İçin Çek Polisinin Yeteneklerini Artırmak

a. Bireysel siber suç polis departmanlarının personelini güçlendirmek.
b. Uzman polis departmanlarının teknolojik donanımını modernize etmek.
c. İlgili ulusal birimler ve diğer güvenlik güçleri arasında siber suç alanı için doğrudan ve hızlı işbirliği bağlantıları kurmak.
d. Siber suç alanında bilgi paylaşımı ve eğitimde uluslararası işbirliğini desteklemek.
e. Polis uzmanlarına mesleki eğitim ve öğretim sağlamak.
f. Çek Polisinin siber suç kovuşturma kapasitesini geliştirmek için çok disiplinli bir akademik ortam yaratmak.

Ana Hedef H. Siber Güvenlik Mevzuatının Oluşturulması ve Uygulanmasına Katılım

a. Sistemik yaklaşıma dayalı ve mevcut mevzuatı dikkate alan anlaşılır, etkili ve yeterli bir siber güvenlik mevzuatı oluşturmak.
b. Avrupa ve uluslararası yönetmeliklerin oluşturulması ve uygulanmasına aktif olarak katılmak.
c. Siber güvenlik mevzuatının etkinliğini ve ilgili teknik disiplinler ve sosyal bilimlerdeki en son bulgulara uygunluğunu sürekli olarak değerlendirmek, güvenli bir bilgi toplumunun mevcut gereksinimlerini yansıtmak için bu mevzuatı düzenli olarak güncellemek ve değiştirmek.
d. Yargının (yani savcılar veya hakimler) siber güvenlikle ilgili eğitimini desteklemek.

Çekya stratejinin ana hedeflerine dayalı olarak ve dahil olan tüm paydaşlarla koordinasyon içinde, hedeflerin gerçekleştirilmesi ve denetlenmesi için belirli adımları ve sorumlulukları belirlenmiştir. NSA ve Ulusal Siber Güvenlik Merkezi (National Cyber Security

Centre/NCSC) ülkenin uzman departmanı olarak, diğer paydaşlarla işbirliği içinde, bireysel hedeflere ulaşma seviyelerini sürekli olarak izleyecek, tartışacak ve değerlendirecektir. Eylem Planının yerine getirilmesine ilişkin bilgilerin ekleneceği yıllık rapor hazırlanması öngörülmüştür (Çekya, 2015).

4.20. Estonya'nın Siber Güvenlik Stratejisi

Estonya Cumhuriyeti Siber Güvenlik Stratejisi 2019-2022 dönemini kapsayacak şekilde hazırlanmıştır. Belge yedi ana bölümden oluşmakta olup hedefler kısmı 4 ana başlıkta incelenmiştir. Giriş kısmında bir takım tespitlere ve değerlendirmelere yer verilmiştir. Ülke eylem planlarında sürekliliğe sahiptir. 2019-2022 dönemi siber güvenlik stratejisi, Estonya'nın üçüncü ulusal siber güvenlik stratejisi belgesidir. Uzun vadeli vizyonu, hedefleri, öncelikli eylem alanlarını, etki alanı için rolleri ve görevleri tanımlayarak faaliyet planlaması ve kaynak tahsisi için temel oluşturmaktadır. Strateji, önceki iki strateji döneminde (2008-2013 ve 2014-2017) öğrenilen derslere dayanmaktadır (Estonya, 2019).

Strateji belgesi, Estonya'da katkıda bulunan tüm paydaşları içerir: kamu sektörü (hem sivil hem de savunma), temel hizmet sağlayıcıları, sektörel girişimciler ve akademi. Günümüzde siber güvenlik evrensel olarak devletin, ekonominin, iç ve dış güvenliğin işleyişinin ayrılmaz bir parçası olarak kabul edilmektedir. Hızlanan, çeşitlenen ve büyük ölçüde öngörülemeyen dijitalleşme, risk tanımlama ve yönetimi için büyük zorluklar ortaya çıkarmaktadır. Bunların yanı sıra, bugün Estonya toplumu, mevcut siber tehditlerle başa çıkmak için yeterince hazırlıklı değildir. Hem özel sektör hem de kamu sektörü, özellikle liderlik düzeyinde, büyük ölçüde risklerden ve ihtiyaçlardan habersizdir. Siber güvenlik stratejisinin vizyonu ve temel ilkeleri Estonya, en dirençli dijital toplum üzerine oturtulmuştur. Estonya, bu vizyonu dört temel ilkeyi takip ederek sürdürmektedir (Estonya, 2019):

- Temel hak ve özgürlüklerin korunması ve geliştirilmesinin fiziksel ortamda olduğu kadar siber uzayda da önemli olduğu düşünülmektedir.
- Siber güvenliği, Estonya'nın sosyoekonomik büyümesinin temeli olarak hızlı dijital gelişiminin kolaylaştırıcısı ve güçlendiricisi olarak görülmektedir.
- Kriptografik çözümlerin güvenlik sağlama açısından, dijital ekosistemin temeli olduğu için Estonya için benzersiz bir öneme sahip olduğunu ifade etmiştir.

- Şeffaflığın ve halkın güveninin dijital toplum için temel olduğu düşünülmektedir. Bu nedenle, açık iletişim ilkesine bağlı kalınması taahhüt edilmiştir.

Stratejik hedefler vizyonunu uygulamak için dört stratejik hedefe odaklanmaktadır. İlgili stratejik hedefler kapsamında Estonya'nın güçlü yönleri sırasıyla açıklanmıştır. Ülkenin öncelikli faaliyetleri aşağıdaki gibidir (Estonya, 2019):

- Yeni hizmetlerin ve veri tabanlarının geliştirilmesi, tasarım gereği güvenlik ve mahremiyet ilkeleri izlenecektir.
- Estonya bilgi ve ağ güvenliğinin ulusal organizasyonunda risk temelli bir yaklaşıma yönelecek, uluslararası kabul görmüş en iyi standartları ve uygulamaları takip edecektir.
- Devlet, tüm paydaşlarla işbirliği içinde, kapsamlı bir durum tablosuna sahip olacaktır. Bunun için, otomatik ağ izinsiz giriş izlemeyi artıracak ve özel ağlar için ağ izleme hizmeti sunacaktır.
- Temel hizmetlerin güvenliği sağlanacaktır. Bu amaçla, dijital karşılıklı bağımlılıkları, sınır ötesi bağımlılıkları sistematik olarak yönetileceği ve en kritik veri tabanları ile bilgi sistemlerini destekleyen güvenlik testlerinin yapılacağı ifade edilmiştir.
- Siber güvenlik, siber uzay ile ilgilenen tüm aktörlerin ortak sorumluluğu olarak kabul edilmektedir.

Ülkenin siber güvenlik kapsamındaki koruduğu değer ve sistemler aşağıda sunulmuştur (Estonya, 2019):

- Devletin sahip olduğu kaynaklarla daha fazlasını yapmak için yeteneklerin geliştirmek amaçlanmıştır.
- Siber güvenlik, ulusal savunmaya yönelik kapsamlı yaklaşıma sürekli olarak dahil edilecektir. Bunu yapmak için, siber güvenliği ulusal güvenlik planlama belgelerine (ulusal savunma geliştirme planı ve ulusal savunma faaliyet planı) daha da entegre edilecek ve hayati hizmet sağlayıcıları, üst düzey siyasi liderlik ve ulusal savunma örgütleriyle düzenli olarak ortak tatbikatlar yapılacaktır.
- Aktif ve uyumlu bir siber güvenlik topluluğu oluşturulacaktır. Bunu yapmak için, teknik bilgi akışları sunulacak, ortak tatbikatlar düzenlenecek, özel sektörü ve

akademik yeterliliği sağlam yasal taslak hazırlama ve stratejik planlama süreçlerine dahil edilecektir.

- Savunma Kuvvetlerinin Siber Komutanlığını daha da geliştirmeye devam edilecektir. Siber saldırı kabiliyetini geliştirerek ve zorunlu askerlik hizmetini tamamlamak için piyade yerine "siber zorunlu askerliği" teşvik ederek siber operasyonlar için kapasite geliştirilecektir.
- Siber suçla mücadeleye yönelik tedbirler uygulanacaktır. Bunu yapmak için, kurumlar arası işbirliği ve bilgi alışverişi için bir çerçeve oluşturacak, veri kaydedenler eğitilecek ve uluslararası uzmanlar arasında doğrudan temaslar teşvik edilecektir.
- Kritik veri tabanlarının iletişim güvenliğini sağlanacaktır. Bunu yapmak için, devlet iletişim konsepti uygulanacak ve kritik veri tabanlarının Estonya dışında bulunan veri elçiliklerine yansıtılması sağlanılacaktır.
- Uluslararası stratejik ortaklar ve müttefikler ile günlük pratik işbirliği güçlendirilecektir.
- Siber güvenliği yoğunlaştırılmış bilgi teknolojileri çalışmalarının bir parçası olarak görerek ve uzmanların eğitimi söz konusu olduğunda üniversiteler için beklentileri belirleyerek, gelecekte bilgi teknolojileri uzmanlarının tedarik edilmesini sağlanacaktır.
- Devlet, akademi ve özel sektörün kilit ortakları arasında etkili işbirliğini desteklenecektir. Bu amaçla hem yurt içi hem de uluslararası işbirliğini kolaylaştıran bir küme başlatılacaktır.
- İnovasyonu, ürün geliştirmeyi destekleyerek ve pazarlama faaliyetleri için diplomatik destek güçlendirilecektir. Ekonomik bir sektör olarak siber güvenliğin büyümesini desteklenecektir.
- Siber sektör için bir araştırma ve geliştirme planı ve üniversiteler ve şirketler tarafından gerçekleştirilen Ar-Ge çalışmalarını yönlendirmek, şirketlerin destek tedbirlerine önemli içerik vermek ve eğitim projeleri ve bursları finanse etmek için bir koordinasyon mekanizması oluşturulacaktır.
- Gelecekteki eğilimleri ve riskleri analiz ederek, yeni zorluklara ve tehditlere hızlı bir şekilde yanıt verme yeteneği sağlanacaktır.
- Ortak ülkelerde rekabetçi ve sürdürülebilir siber yeteneği teşvik ederek, Estonya'nın deneyimini AB ve uluslararası projeler aracılığıyla üçüncü ülkelere açıklayacaktır.

Yukarıdaki hedef ve vizyona ulaşmak için, Estonya tüm seviyelerde aşağıdaki değişkenlere ihtiyaç duyduğunu ifade etmiştir (Estonya, 2019):

- Yeterli yetkinlik, insan kaynakları ve finansman;
- Siber güvenliğin tüm alanlara ve temel planlama süreçlerine entegrasyonu;
- Projelerin karmaşıklığının idaresi ve
- Hem yasal hem de kamu idaresi önlemleri yoluyla devlet ve özel sektör için bürokrasinin en aza indirilmesi.

Estonya'da siber güvenliğin mevcut durumu; siber güvenliği etkileyen trendler, ülkelerin faaliyet gösterdikleri ve faaliyetlerini planlarken ilerlemeleri gereken ortamı şekillendirir yaklaşımından yola çıkılarak analiz edilmiştir. Bunlar, Estonya'nın etkilemek için çok sınırlı olasılıklara sahip olduğu ancak dikkate alınması gereken eğilimler olarak değerlendirilmiştir. Siber güvenliği etkileyen trendler ve gelişmeler aşağıdaki gibi sıralanmıştır (Estonya, 2019):

- Teknolojinin yaygınlaşması, artan dijital bağımlılık ve yeni teknolojilerin ortaya çıkışı;
- Büyüyen, değişen ve hizmet temelli siber suç;
- Karmaşık (jeopolitik) bir güvenlik durumu;
- Sınırlı teknolojik özerklik;
- Siber güvenlik tartışmasının küreselleşmesi;
- Piyasa katılımcıları için her zamankinden daha kapsamlı bir yasal ortam;
- İnternet özgürlüğünün getirdiği zorluklar

Estonya'nın güçlü yönü ise ülkenin stratejik hedeflerini gerçekleştirmesine ve zorluklara etkili çözümler bulmasına olanak sağlayacaktır. Aşağıda, siber sektördeki en büyük etkiye ve potansiyele sahip olan Estonya'nın en güçlü beş gücü listelenmiştir (Estonya, 2019):

- Estonya'nın dijital toplumu için güvenli temel mimari;
- Test edilmiş bir olgunluk seviyesi;
- Daha küçük bir ülkeye özgü verimlilik ve esneklik;
- Estonya'nın uluslararası etkisi ve
- Son kullanıcılar arasında yüksek güven

Estonya siber güvenliğini sağlamaya yönelik temel zorluklar, karşılaştırılabilir ülkelerle karşılaşanlardan önemli ölçüde farklı değildir. Estonya, dünyanın dijital olarak en bağımlı ülkelerinden biridir ve bu nedenle siber tehditlerin potansiyel etkileri, diğer birçok ülkeye göre çok daha önemlidir. Aşağıda, stratejinin hazırlanması sırasında belirlenen, alanın optimum işleyişini, gelişimini engelleyen ve bu noktaya uygulanan standartlaştırılmış çözümlerin düzeltmediği yedi en öncelikli sorun ve zorluk listelenmiştir (Estonya, 2019):

- Uzmanlık için sınırlı yetenek;
- Bütünsel liderlik eksikliği;
- Siber tehditlerin etkilerinin yetersiz anlaşılması, olaylar ve çapraz bağımlılıklar;
- Yetersiz farkındalık ve düşük sahiplenme duygusu;
- Yeni uzmanların yetersiz eğitimi de dahil olmak üzere uzman eksikliği;
- Sektörde az sayıda başarılı firma, yetersiz Ar-Ge hacmi ve
- Estonya'nın güvenilir ve değerli bir uluslararası ortak olarak itibarını sürdürmektir.

Aşağıda Estonya Cumhuriyeti Siber Güvenlik Stratejisi 2019-2022 dönemi eylem planında belirlenen ana hedefler ve alt amaçlar açıklanmıştır (Estonya, 2019):

Ana Hedef 1: Sürdürülebilir Bir Dijital Toplum

1. *Hedef 1:* Estonya, güçlü teknolojik dayanıklılığa ve krizle başa çıkmaya hazır, sürdürülebilir bir dijital toplumdur. Hedef, maddeye üç aktivite ile ulaşılması öngörülmüştür:
   a. *Faaliyet Alanı 1.1:* Teknolojik dayanıklılığın daha etkin hale getirilmesi
      - Devlet bilgi sistemi mimarisinde bilgi güvenliği ve veri koruma ilkelerine bağlılık sürecektir.
      - Temel güvenlik gereksinimlerinin geniş tabanlı uygulaması sağlanacaktır.
      - Devlet kurumları arasında güvenli veri alışverişi sağlanacaktır.
      - Estonya devletinin işleyişi için gerekli kritik veri tabanlarının güvenliği sağlanacaktır.
      - Yeni nesil teknolojilerle ilgili risklerin sistematik değerlendirmesi yapılacak ve süreç yönetilecektir.
   b. *Faaliyet Alanı 1.2*: Olayların ve krizlerin önlenmesi, bunlara hazırlıklı olma ve yönetilmesi

- Siber tehditlerin erken tespiti ve önlenmesi için yeteneğin güçlendirilmesi sağlanacaktır.
- Siber güvenliği, ulusal savunma planlaması ve krizlerle başa çıkmaya hazır olma ile bütünleştirilecektir.

c. *Faaliyet Alanı 1.3:* Sektörün bütünsel yönetimi ve uyumlu bir topluluğu şekillendirme
   - Siber güvenlik sektörünün bütünsel yönetimi ve yeteneklerin birleştirilmesi sağlanacaktır.
   - Birleşik bir siber güvenlik topluluğunu şekillendirmek ve tutarlı bir şekilde kapsayıcı bir planlama süreci hazırlanacaktır.

Ana Hedef 2: Siber Güvenlik Sektörü, Araştırma ve Geliştirme

2. *Hedef 2:* Estonya, siber güvenlik sektöründe devlet için önemli olan temel yeterlilikleri kapsayan güçlü, yenilikçi, araştırmaya dayalı, küresel olarak rekabetçi bir girişim ve Ar-Ge'ye sahiptir. Hedef, maddeye bir aktivite ile ulaşılması öngörülmüştür:
   a. *Faaliyet alanı 2.1:* Siber güvenlik Ar-Ge'sini ve araştırmaya dayalı işletmeyi desteklemek ve teşvik etmek.
   b. Özel sektör, devlet ve akademi arasındaki verimli işbirliğinin güçlendirilmesi sağlanacaktır.
   c. Devlet için öncelikli odak alanlarını tanımlayan ülke çapında bir siber güvenlik Ar-Ge planı hazırlanacaktır.
   d. İnovasyon üretimi ve ihracat potansiyeli için destek verilecektir.
   e. Start-up'ların başlaması ve gelişmesine elverişli bir ortam sağlanacaktır.

Ana Hedef 3: Lider Uluslararası Katılımcı

3. *Hedef 3:* Estonya, uluslararası arenada güvenilir ve güçlü bir ortaktır. Hedef, maddeye iki aktivite ile ulaşılması öngörülmüştür:
   a. *Faaliyet Alanı 3.1:* Stratejik yabancı ortaklarla işbirliğini daha etkin hale getirme
      - Estonya, siber konularda yeterince temsil edilmeli ve yetkinliğe sahip olmalıdır.
      - Estonya dış temsilcilikleri, AB, NATO ve BM'de uluslararası hukuku şekillendirme süreçlerine pozisyonları için lobi yapılacaktır.
      - Estonya, kilit ortaklarla ikili işbirliği formatları geliştirecek ve düzenli olarak ortak tatbikat yapacaktır.

- Estonya, uluslararası savunma işbirliğinde yer alır ve siber istikrarın artırılmasına katkıda bulunacaktır.

b. *Faaliyet Alanı 3.2:* Sürdürülebilir siber yeteneğin uluslararası tanıtımı

- Estonya, rekabetçi ve sürdürülebilirliğin sağlanmasına öncü bir katkı sağlayacaktır.
- Avrupa Birliği siber yardım ağı oluşturmada yer alacaktır.

Ana Hedef 4: Siber Okuryazar Bir Toplum

4. *Hedef 4:* Bir toplum olarak Estonya, siber okuryazar ve gelecek alanında uzman arzı garanti etmeyi hedeflemektedir. Hedef, maddeye iki aktivite ile ulaşılması öngörülmüştür:

a. *Faaliyet Alanı 4.1:* Vatandaşların, devletin ve özel sektörün siber bilincini artırma

- Kamuoyunu bilinçlendirmeye yönelik faaliyetler yürütülecektir.
- Öğrenci ve öğretmenlerin bilgi ve becerileri sistematik olarak ölçülecektir.
- Genel eğitim okulu ve meslek okulu öğretmenleri için siber güvenlik alanında bir eğitim kaynağı sağlanacaktır.
- Devlet kurumları ve yerel yönetimlerde siber farkındalığı artırmak için sistematik, ülke çapında bir platform geliştirilecektir.
- Eyaletin orta ve üst düzey yetkililerinin bilgi ve becerileri güçlendirilecektir.

b. *Faaliyet Alanı 4.2:* Devlet ve özel sektör talebine karşılık gelen yetenek gelişimi

- Genel eğitim okullarında siber savunma çalışmaları geliştirilecek ve yetenekli gençlerin potansiyelinin artırılması için çaba gösterilecektir.
- Siber savunma uzmanları için işgücü ihtiyaçlarına sistematik bir genel bakış oluşturulacaktır.
- Siber savunma, iç güvenlik alanlarında ve sürekli eğitim alanında uzmanların kalitesi sağlanacaktır.
- Estonya'nın uluslararası siber hukuk yeterliliğini geliştirilecektir.

4.21. Macaristan'ın Ulusal Siber Güvenlik Stratejisi

Macaristan Ulusal Siber Güvenlik Stratejisi 30 Haziran 2013 tarihinde yürürlüğe girmiştir. Hükümet, Macaristan'ın Ulusal Siber Güvenlik Stratejisinde tanımlanan görevlerin uygulanmasına yönelik bir çalışma ve eylem planı hazırlaması için Macaristan Başbakanlık

Bürosunun başındaki devlet sekreteri talimatıyla hazırlanmıştır. Eylem planı Başbakan Viktor Orbán tarafından imzalanmıştır (Macaristan, 2013).

Strateji belgesi, Macaristan Anayasasında yer alan temel değerleri, özellikle özgürlük, güvenlik, hukukun üstünlüğü, uluslararası ve Avrupa işbirliğini güvenlik ve ekonomi politikası dahilinde ayrı bir alanda karşılamaktadır. Avrupa Komisyonu ve Avrupa Birliği Ortak Dış ve Güvenlik Politikası Yüksek Temsilcisi tarafından 7 Şubat 2013 tarihli "*Avrupa Birliği'nin Siber Güvenlik Stratejisi: Açık, Güvenli ve Güvenli Bir Siber Uzay"* direktife uyumlu hareket edileceği ifade edilmiştir (Macaristan, 2013).

Siber uzay, küresel olarak birbirine bağlı, merkezi olmayan ve sürekli büyüyen elektronik bilgi sistemlerinin birleşik fenomeni, bu sistemlerin içinde ve bunlar aracılığıyla veri ve bilgi biçiminde ortaya çıkan toplumsal, ekonomik süreçler anlamına gelmektedir. Siber uzayda ortaya çıkan tehditlerin artan sayısı ve çeşitli kaynakları ile bunların sonuçlarının artan büyüklük sırası, kamuya açık ve kamuya açık olmayan kullanıcıların sayısının ve verimliliğinin son on yılda yasa dışı olarak edinim için siber uzay kullanan hızlı bir şekilde arttığını göstermektedir. Bu strateji belgesinin temel hedeflerinden biri, teknolojik ilerlemeden kaynaklanan yeni siber güvenlik zorluklarını öngörülebilir gelecekte esnek bir şekilde adapte ederek yönetebilecek siyasi ve profesyonel karar alma düzeyinde farkındalık ve kapasite oluşturmaktır (Macaristan, 2013).

Siber güvenlik, siber uzaydaki riskleri yönetmek için politik, yasal, ekonomik, eğitici, bilinçlendirme ve teknik önlemlerin sürekli ve planlı olarak alınmasıdır. Macaristan'ın egemenliğinin korunması da ulusal çıkar meselesidir. Macar siber uzayının hukukun üstünlüğüne dayalı özgür, demokratik ve güvenli bir şekilde işleyişi temel bir değer ve çıkar olarak kabul edilmektedir. Macaristan'da, siber uzayın özgürlüğü ve güvenliği, hükümet, akademi, iş sektörü ve sivil toplum arasındaki ortak sorumlulukları temelinde yakın işbirliği ve koordineli faaliyetler yoluyla sağlanabilir (Macaristan, 2013).

Macaristan ile aynı değerler kümesini paylaşan küresel siber uzayın tüm kamu ve özel aktörleri ile güvene dayalı işbirliğini kurmayı ve sürdürmeyi amaçlamaktadır. Macaristan müttefikleri ve uluslararası ilişkiler aracılığıyla küresel siber uzayın özgür ve güvenli kullanımını garanti altına almak için çaba gösterecektir. Özellikle AB ve NATO, AGİT, Birleşmiş Milletler, Avrupa Konseyi ve ülkenin üye olduğu diğer uluslararası kuruluşlar ile

ilişkiler geliştirilecektir. Bu stratejiler kapsamındaki eylem planındaki hedefler aşağıdaki gibi özetlenebilir (Macaristan, 2013):

- Bireylerin ve toplulukların özgürlüğe, korkusuzluğa dayalı iletişim, kişisel verilerin korunmasını garanti altına alarak sosyal gelişim ve entegrasyonu sağlamasına,
- İş sektörünün verimli ve yenilikçi iş çözümleri geliştirmesi,
- Gelecek nesiller için değer temelli öğrenmeyi ve sağlam bir zihinsel gelişimle sonuçlanan zarar görmeden deneyimlerin toplanmasını sağlamak,
- Elektronik kamu idaresi için, kamu hizmetlerinin yenilikçi ve son teknoloji gelişimini teşvik etmek.

Siber uzayın ücretsiz ve güvenli bir şekilde kullanılması için Macaristan, ulusal güvenlik, etkin kriz yönetimi ve kullanıcı korumasının çıkarlarını uyumlu hale getirerek karşılanması gereken aşağıdaki hedefleri belirlemiştir (Macaristan, 2013):

- Herhangi bir kötü niyetli siber aktivite, tehdit, saldırı veya acil durum ile kazara bilgi sızıntısını önleme, tespit etme, yönetme (mücadele etme), müdahale etme ve kurtarma konusunda etkin yeteneklere sahip olmak,
- Ulusal veri varlıkları için yeterli koruma sağlamak, kritik altyapılarının siber uzay ile bağlantılı kısımlarının operasyonel güvenliğini sağlamak ve bir uzlaşma durumunda hızlı, verimli bir azaltma ve kurtarma kabiliyetine sahip olmak, bir devlet sırasında da kullanılabilir acil durum oluşturma,
- Uluslararası güvenlik sertifikasyon standartlarına uygunluğa özel önem vererek, Macaristan siber uzayının güvenli çalışması için gerekli BİT ve iletişim ürün ve hizmetlerinin kalitesinin uluslararası en iyi uygulamaların gereksinimlerini karşılamasını sağlamak,
- Eğitim, öğretim ve araştırma ve geliştirme kalitesinin uluslararası en iyi uygulamaların gerekliliklerini karşılamasını sağlamak, böylece dünya standartlarında bir ulusal bilgi havuzunun oluşturulmasına katkıda bulunmak,
- Çocuklar ve gelecek nesiller için güvenli bir siber alanın kurulmasının uluslararası en iyi uygulamaların gerekliliklerini karşılamasını sağlamak.

Siber uzayın özel yapısından kaynaklanan, ulus için stratejik bir meydan okuma oluşturan bir dizi güvenlik riski ve tehdidi dikkate alınmalıdır. Siber güvenlik seviyesini korumak,

iyileştirmek ve hedeflere ulaşmak için mevcut araçlar ve görevlerin yerine getirilmesinden etkilenen alanlar aşağıdaki gibi özetlenebilir (Macaristan, 2013):

- *Hükümet koordinasyonu.* Öncelikle, her devlet kurumu siber uzayın ücretsiz ve güvenli kullanımı için kendi sorumluluğunu üstlenir. Bununla birlikte, bu alanın karmaşıklığından dolayı, bu sorumluluklar, hükümetin siber uzayın özgür ve güvenli kullanımına ilişkin amacını ancak açık ve verimli bir hükümet koordinasyonu yoluyla karşılayabilir. Bu nedenle, hükümetin ve sektörel kaynakların koordineli ve yoğun kullanımı için zorunlu bir adım olan başbakanlık aracılığıyla merkezi yönetim koordinasyonu güçlendirilecektir.
- *İşbirliği.* Hedefleri ve siber güvenlik çıkarlarını karşılamak için geliştirilmiş işbirliği ve verimli bilgi paylaşımına ihtiyaç vardır. Bu amaçla, iş dünyası ve akademi temsilcilerinin hükümetin karar alma süreçlerinin hazırlanmasına katılımını sağlayan, bu forumların üyelerinin siber güvenlik faaliyetlerinin geliştirilmesi ve sürekli iyileştirilmesine yönelik öneriler veya görüşler öne sürmelerine olanak tanıyan operasyonel işbirliği forumlarının oluşturulması gerekmektedir.
- *Uzmanlaşmış kurumlar.* Siber güvenlik görevleri, yalnızca birbirleriyle değil, aynı zamanda veri koruma ve sınıflandırılmış bilgilerin korunmasından sorumlu diğer yetkililerle de işbirliği yaparak belirli becerilere ve yetkilere sahip kuruluşlara atanmalıdır. Bu görevler, ulusal güvenlik, savunma, kolluk kuvvetleri, afet yönetimi, kritik altyapı korumasından sorumlu kuruluşları ve elektronik bilgi güvenliğinden sorumlu yetkilileri etkilemek olarak sıralanabilir.
- *Yasal düzenlemeler.* Karmaşık bir mevzuata ek olarak, ortak sorumluluğa dayalı siber güvenliğin verimli bir şekilde çalışması için yeterli temel ve düzenleme sağlamak için sivil toplum, iş sektörü ve akademi aktörleri ile işbirliği anlaşmaları yapmak gereklidir.
- *Uluslararası işbirliği projeleri.* Macaristan, AB ve NATO içindeki siber savunma girişimleri ve işbirliği projelerinin yanı sıra BM ve AGİT'in siber güvenlik işbirliği projelerindeki rolünü geliştirmeyi amaçlamaktadır.
- *Farkındalık.* Macaristan uluslararası siber güvenlik forumlarının düzenlenmesinde lider olmak istemektedir. Uzman kurumları ve sivil toplum, iş sektörü ve akademi aktörleri ile işbirliği yoluyla, siber alanın güvenli kullanımına ve farkındalığın artırılmasına yönelik faaliyetleri ve ayrıca bireysel kullanıcılar arasında farkındalık yaratmaya özel odaklanarak, pratik siber güvenlik becerilerini teşvik eden girişimler desteklenecektir.

- *Eğitim, araştırma ve geliştirme.* Macaristan, ilk, orta ve yüksek öğrenimin bilgi teknolojisi müfredatında, hükümet görevlileri için eğitim kurslarında ve mesleki eğitim kurslarında siber güvenliğin bir alan olarak entegre edilmesine özellikle dikkat edecektir. Macaristan, siber güvenlik araştırma ve geliştirmesinde olağanüstü ve uluslararası kabul görmüş sonuçlar elde eden ve siber güvenlik mükemmellik merkezlerinin kurulmasına yardımcı olan üniversite ve bilimsel araştırma merkezleriyle stratejik işbirliğine yatırım yapacaktır.
- *Çocukların koruması.* Macaristan, siber güvenliğin temel bir unsuru olarak çocukların sağlıklı gelişimine izin veren bir ortamın yaratılması ve sürdürülmesini kabul etmektedir ve bunu etkilenen tüm alanlarda bir öncelik olarak ele alır ve aynı zamanda Daha İyi İnternet için Avrupa Stratejisi'nin hedeflerine ulaşmayı planlamaktadır.
- *İş aktörlerinin motivasyonu.* Macaristan, bilgi teknolojisi ve iletişimde kamu ihaleleri için siber güvenlik gereksinimlerini belirlerken, ekipman üreticilerini ve hizmet sağlayıcılarını, uluslararası sertifika standartlarına uyuma özel önem vererek, mümkün olan en yüksek siber güvenlik düzeyini oluşturmak için teklif vermeye teşvik etmeyi amaçlamaktadır. Ayrıca Macaristan, siber güvenliğin iyileştirilmesi için teşvik edici önlemler geliştirmek için iş aktörleriyle işbirliği yapmak istemektedir.

Ulusal Siber Güvenlik Stratejisi Eylem Planını uygulamak için mevcut veya ek hükümet araçları aşağıdaki gibidir (Macaristan, 2013):

- Macaristan siber uzayının güvenliğinden sorumlu devlet kuruluşlarının envanterinin tutulması ve koordinasyonu, verimli işbirliğinin kurulması;
- Macar siber uzayının güvenliğinden sorumlu sivil toplum, iş dünyası ve akademik kuruluşların incelenmesi, kurumsal işbirliğinin kurulması;
- Kritik bilgi altyapılarının ve kritik varlıkların ve ayrıca ulusal veri varlıklarının envanterinin tutulması ve bunların korunmasının sağlanması;
- Devlet kurumlarının işletilmesinde uzmanlaşma;
- Düzenleyici bir ortamın sağlanması;
- Siyasi, operasyonel ve düzenleyici düzeylerde uluslararası ve bölgesel işbirliğine katılım;
- Araştırma ve geliştirme, eğitim ve bilinçlendirme için bir destek çerçevesinin oluşturulması;

- İş motivasyon sistemlerinin kurulması;
- Siber güvenlik unsurlarının devlet kontrolü altındaki teknik gelişmelerle ve hükümetin bilgi sistemlerinin geliştirilmesi ve işletilmesi ile ilgili görevlere entegre edilmesi.

Mevcut araçların güçlendirilmesi, daha verimli kullanılması ve bunların ulusal güvenlik açısından daha etkili pratik uygulamaları, hükümet içi ve hükümet dışı işbirliği için bir sistemin kurulmasını ve işletilmesi ülkenin ana hedeflerdendir (Macaristan, 2013).

4.22. Letonya'nın Siber Güvenlik Stratejisi

Letonya'nın Siber Güvenlik Stratejisi 2014-2018 dönemi için hazırlanmış ve onaylanmıştır. 7 ana bölümden oluşan strateji belgesi kapsamlı ve detaylı bir şekilde hazırlanmıştır. Letonya Devleti idaresi, toplumu ve ekonomisi tarafından sağlanan fırsatlara ve hizmetlere bağlı bir yapıdadır. Letonya'nın Sürdürülebilir Kalkınma Stratejisi, modern ve yenilikçi bir toplumun daha fazla gelişmesinin teşvik edilmesini, yeni fikirler ve yüksek teknolojinin Letonya'nın ekonomik kalkınması ve küresel rekabet gücü için bir varlık olarak kullanılmasını tanımlamaktadır (Letonya, 2014).

BİT'in toplumda, devlet idaresinde ve ekonomide artan kullanımından dolayı, yasadışı kullanımı, hasarı, felç veya yıkımı, devlet ve kamu güvenliği, kamu düzeni ve ekonomik faaliyet için tehditlerin yanı sıra daha fazla gelişmenin engellenmesine neden olabilir. Siber alandaki güvensizlik, BİT kullanımının güvenilirliğini etkileyebilir ve böylece modern ve yenilikçi bir toplumun gelişmesini engelleyebilir. Siyasi, sosyal veya ekonomik açıdan hassas gelişmeler sırasında, büyük siber saldırılar Letonya'ya yönelik olabilmektedir. Eylem planı, başta AB ve NATO olmak üzere uluslararası kuruluşların belgeleri doğrultusunda geliştirilmiştir. Siber güvenlik politikasının amacı, devlet ve toplum için gerekli olan hizmetlerin güvenli, güvenilir ve sürekli tedarikini sağlayan güvenli ve güvenilir bir siber alan oluşturulmasıdır. Politikanın amaçları ve temel ilkeleri aşağıdaki gibidir (Letonya, 2014):

- *Gelişim:* Siber uzayda hızla gelişen tehditlere karşı korunmak, yalnızca BİT sektöründeki ve güvenlik uzmanlığındaki becerileri sürekli ve sistematik olarak geliştirerek ve iyileştirerek mümkündür.

- *İşbirliği:* Ülkelerin coğrafi sınırları veya kurumların idari sınırları tarafından kısıtlanmayan siber alandaki tehditlere karşı etkili koruma, ancak hem ulusal hem de uluslararası düzeyde işbirliği ile mümkündür.
- *Sorumluluk:* Siber alandaki riskleri etkin bir şekilde azaltmak. Ancak bireyler, devlet kurumları ve özel işletmeler de dahil olmak üzere siber uzayda yer alan tüm tarafların faaliyetlerinin veya hareketsizliklerinin kendi güvenlikleri üzerindeki etkileri hakkında bilgilendirilmesi ve bunların farkında olması halinde mümkündür.
- *Açıklık:* Siber güvenlik politikası, bir bireyin haklarına ve temel özgürlüklerine saygı gösterirken bilgi ve iletişim teknolojisinin erişilebilirliğini kolaylaştırarak, özgürlük, mahremiyet ve güvenlik arasında bir denge arayarak ve iyi uygulamaları teşvik ederek uygulanmalıdır.

Modern toplum, BİT'ni hem doğrudan bilgi edinerek hem de işleyerek ve kendini ifade etmek için yeni ve yaygın olarak erişilebilir araçlar yaratarak daha kapsamlı bir şekilde kullanmaktadır. Letonya'da ikamet edenlerin toplam %75,8'i interneti kullanırken, %70,3'ü interneti en az önce bir kere kullanmaktadır. BİT'nin yaygın kullanımı, toplumun günlük rutinini değiştirmiş fiziksel, dijital eylemlerin birleştiği bir sanal ortam yaratılmıştır. Ayrıca, BİT araçlarının kullanımı bir bireyin haklarını ve temel özgürlüklerini kısıtlayabilir veya özel hayatın gizliliği ve kişisel verilerin korunması hakkını ihlal edebilir. BİT yardımıyla topluma zarar verildiğinde vakaların sayısını azaltmak için, siber alanı ve hizmetlerini koruyacak bir dizi kapsamlı önlem geliştirmek önemlidir. Eylem planı, beş öncelikli hedef alanı belirler (Letonya, 2014):

- Siber Güvenliğin Yönetişimi ve Kaynakları.
- Siber Uzayda Hukukun Üstünlüğü ve Siber Suçun Azaltılması.
- Kriz Yönetimi.
- Kaçınma, Eğitim ve Araştırma.
- Uluslararası İşbirliği.

Eylem planında ana hedefler ve ana hedeflere yönelik eylemler aşağıdaki gibidir (Letonya, 2014):

Eylem 1: Siber Güvenliğin Yönetişimi ve Kaynakları

1. *Ulusal Siber Güvenlik:* Ulusal siber güvenlik, bilgi güvenliğinin sağlanmasının gerekli olduğu üç boyutta (altyapı, hizmetler ve süreçler) incelenmelidir. Şu anda, siber güvenlik yönetişimi, önde gelen kurumların (ilgili otoriteye göre) siber güvenliğin stratejisini, metodolojisini ve koordinasyonunu idare etme işlevini yerine getirmeye çalışmaktadır. Ana hedef kapsamındaki eylemler şu şekildedir:
   a. Kamu, sivil toplum ve özel sektör temsilcilerinin işbirliği ile Ulusal BT Güvenlik Konseyi çerçevesinde ulusal siber güvenlik politikasının koordineli geliştirilmesi, uygulanması ve değerlendirilmesi iyileştirilecek.
   b. Girişimciler arasında güncel siber güvenlik tehditleri, sorunları, çözümleri, iyi uygulamalar ve bunların uygulamaları hakkında bilgi alışverişini teşvik ederek bir bilgi alışverişi ortamı (platformu) oluşturulacak.
   c. Ulusal siber güvenliğe yönelik risklerin değerlendirmesi sağlanacak.
   d. İş ortamında BİT güvenliği hakkında anlayış yaratarak ve lider işverenler için düzenli eğitimler düzenleyerek kamu ve özel sektörde iyi güvenlik yönetimi standartları ve uygulamaları teşvik edilecek.
   e. Elektronik iletişim operatörleri için güvenlik gereksinimlerinin uygulanması ve izlenmesine yönelik mekanizmalar iyileştirilecek.
   f. BT güvenlik olaylarını gözlemleme, analiz etme ve önleme ve bilgi alışverişi konusunda NATO ve AB ortaklarıyla işbirliği yapma becerisi geliştirilecek.
   g. Merkezi güvenlik testleri gerçekleştirmek için kaynaklar ve yeterlilikler geliştirilecek.
2. *Devlete Ait Bilgi ve İletişim Teknolojileri:* Ulusal düzeyde siber güvenlik, şu anda kısmen Devlet Bilgi Sistemleri Yasası ile düzenlenen Eyalet BİT yönetişim sistemi ile yakından bağlantılıdır. Daha sonraki gelişimi, Devlet BİT yönetiminin örgütsel modeli konseptinde özetlenmiştir. Gerekli görevlerin yerine getirilmesi, daha yüksek derecede uzmanlık ve daha yüksek mesleki yeterliliklere sahip daha iyi motive edilmiş insan kaynaklarını çekecek ve böylece Devlet BİT güvenliğinin genel düzeyini artıracak, homojen, daha paylaşılan, profesyonelce ve rasyonel olarak sürdürülen bir Devlet BİT altyapısına ulaşmaya izin verecektir. Ana hedef kapsamındaki eylemler şu şekildedir:
   a. Birleşik BİT mimarisinin geliştirilmesini ve yönetim süreçlerinin, standartlarının ve kılavuzlarının geliştirilmesini veya iyileştirilmesini sağlayan Devlet BİT yönetiminin kavramsal organizasyon modelinde belirtilen iyileştirilmiş yönetim önlemlerinin uygulanmasına devam edilecek.

b. Bir risk analizine ve güvenlik yönetimi için uygun şekilde farklılaştırılmış gereksinim çerçevesine dayalı bir sistem sınıflandırmasını sağlayan Devlet BİT hükümlerinin birleşik bir yönetimi için yasal bir düzen geliştirilecek.
c. Devlet idaresinin idari personeli ve BİT güvenlik yönetiminde yer alan personel için eğitim programları düzenleyerek ICT Çözümleri ve altyapısı sahiplerinin anlayışı ve bilgisi geliştirilecek.
d. BİT güvenlik yönetiminin denetiminin etkinliğini, güvenlik yönetimi önlemlerini uygulamamanın sorumluluğunu, cezalarını ve ayrıca güvenlik yöneticilerinin çalışmaları için asgari gereksinimler belirlenecek.
e. Bağımsız kuruluşlar tarafından gerçekleştirilen Devlet BİT Çözümleri ve altyapısının olağanüstü denetimleri ve güvenlik testleri düzenlenecek.
f. Kurumların, bilgi güvenliği önlemlerinin uygulanması hakkında ortak bir yetkili makama rapor vereceği prosedür geliştirilecek.
g. Belediye BİT kaynaklarının güvenlik yönetimini iyileştirmek için Letonya Yerel ve Bölgesel Yönetimler Birliği, Belediyeler ve Kurumlar arasındaki işbirliği geliştirilecek.

3. *Kritik Altyapılar:* Kritik altyapının bütünlüğünü, erişilebilirliğini ve gizliliğini sağlamak için devlet ve toplum için esas olan temel işlevlerin yerine getirilmesi için kritik bilgi teknolojisi altyapısı oluşturulmuştur. Ana hedef kapsamındaki eylemler şu şekildedir:
   a. Olaylar, kritik altyapının korunması ve kritik altyapı sahipleri ve devlet güvenlik kurumları arasında risklerin önlenmesi ile ilgili bilgi ve deneyim alışverişi iyileştirilecek.
   b. Ulusal, bölgesel ve uluslararası düzeyde ve Ulusal Silahlı Kuvvetlerin Siber Savunma Birimi (NAF) ile işbirliği içinde kriz eğitimi ve güvenlik ihlali testleri düzenlenecek.
   c. Güvenlik personelinin kapasitesini, bilgisini ve karşılıklı işbirliğini iyileştirmenin yanı sıra güvenliğin otomatik sağlanması ve kontrolü için teknik araçlar geliştirilecek.
4. *İnsan Kaynakları:* Devlet ve belediye kurumlarındaki durum, iyi maaşlı ve yüksek vasıflı çalışanlara ve modern teknik kaynaklara sahip kurumlardan - çoğu durumda - yetersiz vasıflara sahip çalışanların bulunduğu kurumlara kadar insan ve malzeme kaynaklarındaki önemli farklılıklar ile karakterize edilmektedir. Bu, Devlet idaresinde bilgi güvenliği yönetimi alanında mevzuat tarafından belirlenen yükümlülüklerin

eşitsiz düzeyde yerine getirilmesini yaratmaktadır. Bu yüzden insan kaynaklarının kalitesinin artırılması gerekmektedir. Ana hedef kapsamındaki eylemler şu şekildedir:

a. Siber güvenlik hakkında bilgi ve beceriler için gereksinimleri dahil ederek BİT ile ilgili mevcut mesleki standartlar değerlendirilecek ve yükseltilecek.
b. Siber güvenlikten sorumlu uzmanların mesleki yeterlilikleri tanımlanacak, artırılacak ve değerlendirilecek.
c. Çalışma programlarına siber güvenlik uzmanlığını dahil ederek yüksek öğretim kurumlarının katkısı teşvik edilecek.
d. Siber güvenlik uzmanlarının talebi, arzı, ücretleri ve eğitim kurumları tarafından hazırlanan uzmanların istihdam düzeyi hakkında bir işgücü piyasası analizi yapılacak.
e. Öğretim kadrosunun siber güvenlik alanındaki yeterlilikleri geliştirilecek ve metodolojik materyallerin hazırlanması desteklenecek.

Eylem 2: Siber Alanda Hukukun Üstünlüğü ve Siber Suçun Azaltılması: Siber uzayda hukukun üstünlüğü, hem fiziksel hem de sanal ortamda yasa ve düzenlemelerin gözlemlenmesini sağlayan eşdeğerlik ilkesine dayanmaktadır. Devlet, uygulama alanlarına bakılmaksızın, herhangi bir kimsenin Anayasa tarafından belirlenen temel hak ve özgürlüklerini ve evrensel haklar ilkelerinin gözetilmesini sağlamakla yükümlüdür. Sağlanan teknolojik olanaklar, siber alandaki cezai suçların artmasını desteklemiştir. Ana hedef kapsamındaki eylemler şu şekildedir:

a. Letonya İdari İhlal Kanunu ve Ceza Kanununu uygulamak için bir temel olarak BİT sektöründeki kanunları ve düzenlemeleri değerlendirilecek ve bu temeli, ceza hukuku aracılığıyla ve ilgili olarak bireylerin çıkarlarının etkili bir şekilde korunmasını sağlamak için geliştirilecektir.
b. Mevcut durumu ve otomatik veri işleme sistemlerine yönelik bilgi sistemlerinin güvenliğine veya işleyişine zarar vermesi nedeniyle ceza öngören mevzuatta gerekli değişiklikler değerlendirilecek.
c. Letonca dilinde bilgi güvenliği, siber güvenlik ile ilgili terminoloji geliştirilecek ve yasal düzenlemelerde kullanımı uyumlu hale getirilecek.
d. Yasama kanunlarında belirtilen siber güvenlik alanındaki yükümlülüklerin denetimi değerlendirilecek ve iyileştirilecek.

e. Uluslararası eğilimler doğrultusunda yeni BİT suçlarının tespiti ve sınırlandırılmasının yasal dayanağının iyileştirilmesine ilişkin tartışmalar ve fikir alışverişi kolaylaştırılacak.
f. Mevcut kaynakları, prosedürleri, işbirliği mekanizmalarını ve bunların etkinliklerini değerlendirip iyileştirerek siber suçlarla mücadele edilecek ve soruşturulacak.
g. Polis, savcılık ve mahkeme sisteminde siber alandaki cezai suçları (istatistikler) listelemek için birleşik bir mekanizma geliştirilecek.

Eylem 3: Kriz Durumunda Harekete Geçme Hazırlığı ve Kapasitesi: Letonya'da ulusal siber güvenlik kabiliyetlerini sağlayan kurumlar kurulmuştur. Artan tehdit durumunda eylem planları geliştirilmiş ve düzenli olarak güncellenmektedir. İçişleri Bakanlığı ile farklı kriz durumlarının çözümü için işbirliği yapılmıştır. Uzmanların katılımı özel sektör ile işbirliği içinde mevcuttur. Bununla birlikte, mevcut kaynaklar ve önlemler, ciddi ve kapsamlı BT güvenlik olayları veya siber saldırılar durumunda etkili ve hızlı eylem sağlamak için yeterli ve organize değildir. Ana hedef kapsamındaki eylemler şu şekildedir:

a. Olası bir siber kriz durumunda bir krizin tanımı, prosedürleri, mevzuatı ve kullanımı değerlendirilecek.
b. Birimin operasyonel kabiliyetini sağlayarak ve temin ederek, bir kriz durumunda tepki verme ve önemli olayların sonuçlarını yönetme yetenekleri geliştirilecek.
c. Kriz durumlarında yönetim yeteneklerinin desteklenmesini sağlamak için bilgi teknolojisi ve iletişim sistemleri geliştirilecek.
d. Karşılıklı anlayışı geliştirmek ve kriz durumlarının yönetimini koordine etmek için ulusal düzeyde üst düzey yetkililerin ve tüccarların katılımıyla düzenli teorik ve pratik eğitim düzenlenecek.
e. Küresel siber saldırılarına karşı devlet kurumlarının yetkinliği ve kaynakları iyileştirilecek.
f. Kriz durumunda destek sağlamak ve almak için düzenli eğitim sağlamak için bölgesel ve uluslararası işbirliği geliştirilecek.
g. Acil durumlar için bir elektronik iletişim ağı kurulacak.
h. Devlet kurumlarına altyapı sağlayan ve devlet bilgi sistemleri için yüksek gizlilik, bütünlük ve erişilebilirlik sağlayan teknolojik ve organizasyonel bir çözüm geliştirilecek.
i. Ulusal dış iletişim ağının dış kapsamı güçlendirilecek.

Eylem 4: Farkındalık Yaratma, Eğitim ve Araştırma: Bilgiye dayalı bir toplum, güvenli ve güvenilir bir siber alanın çok önemli bir parçasıdır. Bir ülkenin önde gelen yetkilileri tarafından uygulanan politika ve iletişim de dahil olmak üzere, amaca yönelik ve düzenli açıklayıcı çalışmalar, eğitim kurumlarındaki sorunları gündeme getirerek ve medyadaki uzmanların düzenli tartışmalarını organize ederek kaçınma sağlanır. Ana hedef kapsamındaki eylemler şu şekildedir:

a. Eğitim kurumlarının ve öğretim personelinin yetkinliklerini ve bu konuları eğitim sistemine entegre ederek ve bilgi güvenliği, mahremiyetin korunması ve kullanımı hakkında anlayış oluşturan öğrenme etkinlikleri düzenleyerek çocukları ve gençleri BİT güvenliği konularında eğitilmesi sağlanacak.
b. Eğitim kurumlarında ve ilgi gruplarında kullanılmak üzere siber güvenlik hakkında, kolaylıkla erişilebilen ve çeşitli yaş gruplarına göre farklılaştırılan eğitici ve bilgilendirici materyaller geliştirilecek.
c. Uzmanları eğitmek, yeniliği teşvik etmek, bilim ve araştırmanın desteklenmesi için kamu-özel ortaklıkları kurmak ve Avrupa fonlarını, hibelerini ve finansal araçlarını çekmek için siber güvenlik alanında akademik çalışmalar ve araştırmalar geliştirilecek.
d. Üniversiteler ve bilimsel enstitülerle işbirliği içinde bir güvenlik laboratuvarı oluşturmak ve siber güvenlik ve siber suçla ilgili güncel konular hakkında bilimsel konferanslar düzenlenecek.
e. Çeşitli güvenlik yazılımlarının erişilebilirliğini genişletmek için siber güvenlik, siber suçlar ve önemli tehditler hakkında toplumun genel anlayışını geliştirmek için eğitici ve bilgilendirici kampanyalar ve diğer önlemler uygulanacak.
f. Kamu yönetimi, sektör dernekleri, uzmanlar, iş liderleri ve ayrıca kamuoyu yaratıcıları - sivil toplum kuruluşları ve akademik ortam arasında bilgi ve fikir alışverişi geliştirilecek.
g. Siber güvenlik sektöründe yenilik teşvik edilecek ve yüksek kapasiteli bilgi işlem için birleşik bir akademik kaynaklar (süper bilgisayar) geliştirilecek.

Eylem 5: Uluslararası İşbirliği: Siber uzay tarafından sağlanan fırsatlar ve güvenlik tehditleri ulusal sınırları tanımamaktadır. Bu nedenle hiçbir devlet kendi başına yeni güvenlik zorluklarıyla etkili bir şekilde yüzleşemez. Ana hedef kapsamındaki eylemler şu şekildedir:

a. Baltık ve Kuzey Avrupa ülkeleriyle işbirliği güçlendirilecek. Ayrıca, güvenliği, erişilebilirliği ve özgürlüğü geliştirmek için NATO, AB, AGİT ve BM ile işbirliği yapılacak.
b. Uluslararası hukuk normlarının hem fiziksel hem de sanal ortama eşit uygulanabilirliğini vurgulayarak karşılıklı güven ve işbirliğini geliştirmeye yönelik uluslararası çabalar desteklenecek.
c. Güçlü ve nitelikli uzmanlar hazırlamak için bölgesel eğitim kaynaklarını birleştirmek için ortak bir Baltık Üniversitesi çalışma programı oluşturulacak.
d. Letonya'da düzenli olarak uluslararası siber güvenlik etkinliklerini organize edilecek ve Letonya'yı ulusal ve uluslararası düzeyde BİT güvenliğinden yararlanan bir ülke olarak vurgulanacak.
e. Letonya ile NATO arasındaki Mutabakat Zaptı ve NATO Siber Savunma Kavramı ile Eylem Planı uyarınca bir siber tehdit durumunda acil ve etkili yardım almak için ulusal prosedürler geliştirilecek.
f. Çeşitli uluslararası eğitim kurslarına, tatbikatlara ve NATO, AB ve diğer uluslararası kuruluşlar ve forumlarda siber saldırı simülasyonlarına katılarak siber koruma yetenekleri güçlendirilecek.

Siber güvenlik sürekli ve hızlı bir şekilde geliştiği için eylem planında önerilen çözümün ön değerlendirmesi yapılmamıştır. Ancak kılavuzlarda belirlenen eylem alanları Milli Güvenlik Kavramında belirtilen önceliklerin ve bugüne kadar başlatılan eylemlerin devamı niteliğindedir. Kılavuzlarda sağlanan siber güvenliğin değerlendirilmesi, daha fazla politika ve eylem planının değerlendirilmesi ve iyileştirilmesi için bir temel oluşturacaktır (Letonya, 2014).

4.23. Litvanya'nın Siber Güvenlik Stratejisi

Litvanya'nın Ulusal Siber Güvenlik Strateji belgesi 13 Ağustos 2018 tarihinde onaylanmış ve yürürlüğe girmiştir. Strateji belgesi dört ana bölümden oluşmaktadır. Milli Savunma Bakanı Raimundas Karoblis tarafından önsöz yazılmıştır. Bunun yanı sıra yalın ve sistematik bir yapıda hazırlanmıştır. Bilişim ve iletişim teknolojisinin hızla değiştiği ve hayatımızı değiştirmeye devam ettiği bu dönemde söz konusu teknolojik ilerlemeler özel sektör ve kamu sektörünün faaliyetlerini büyük ölçüde etkilemektedir. Şüphesiz, kötü niyetli yazılımların bir dezenformasyon kampanyası ile birlikte kullanılması yoluyla bir eyaletin

kritik altyapısına verilen herhangi bir hasar, bir ülkede kaosa yol açabilir. Siber olayların sayısı her yıl %10 artmaktadır. Siber olaylar giderek daha karmaşık hale geliyor, siber saldırılar daha uzun sürüyor ve daha iyi koordine ediliyor. Bu nedenle, mevcut tehditler yeni önlemler ve araçlar kullanılarak uygun bir şekilde karşılanmalıdır (Litvanya, 2018).

Strateji belgesinin temel amacı, Litvanya halkına karşı yürütülecek siber olayları zamanında ve etkin bir şekilde tespit ederek, siber olayları ve tekrarlarını önleyerek ve siber güvenliğin etkisini yöneterek bilgi ve iletişim teknolojisinin potansiyelini keşfetme fırsatı sağlamaktır. Strateji belgesiyle, devletin siber suçları önleyen ve soruşturan, siber güvenlik kültürünü ve yenilikçiliği teşvik eden, yakın özel-kamu ortaklığını (PPP) ve uluslararası işbirliğini geliştiren siber güvenlik ve siber savunma yeteneklerinin geliştirilmesini güçlendirmeyi ve 2023 yılına kadar ülke içinde uluslararası siber güvenlik yükümlülükleri yerine getirmeyi hedeflemektedir. Eylem planı, çevre analizi, yapılan araştırmalardan elde edilen veriler ve kamu ve özel sektör temsilcilerinin sunduğu öneriler dikkate alınarak geliştirilmiştir. Aşağıda eylem planının ana amaçları ve atılacak adımlar özetlenmiştir (Litvanya, 2018):

1. *Devletin Siber Güvenlik ve Siber Savunma Yetenekleri*: Stratejinin ilk hedefi, ülkede siber güvenliği güçlendirmek ve siber savunma yeteneklerini geliştirmektir. Stratejinin ilk hedefine ulaşmak için atılacak adımlar;
   a. *İlk hedefin ilk amacı, siber güvenlik ve önleyici faaliyetlere sistematik bir yaklaşım geliştirmektir:* Bu hedef, siber güvenlik risk tanımlama, değerlendirme ve tahmin yöntemlerini geliştirerek gerçekleştirilecektir. Bunlar; belirli sektörlerde tipik olarak karşılaşılan riskleri ortaya çıkarmak için bir siber güvenlik tanımlaması ve bir risk haritası oluşturarak, bir dizi siber güvenlik önlemi ile bölgesel siber güvenlik merkezi ve devlet kontrollü elektronik iletişim ağı kurarak, hayati devlet işlevlerini sağlamak için devlet seferberliği görevlerini yerine getiren devlet ve belediye kurumlarını, kurumlarını ve devlet şirketlerini birbirine bağlayarak, siber güvenlik durumu, ilerleme raporları veya olgunluk değerlendirmeleri hakkında anketler yaparak, siber güvenlik düzeyi ve önleyici faaliyetleri artırmak için diğer önlem ve eylemleri uygulayarak yapılacaktır.
   b. *Birinci hedefin ikinci amacı, siber güvenlik kurumlarına düşen idari yükü azaltarak siber güvenlik politikası oluşturma ve uygulama verimliliğini artırmaktır:* Bu hedef, siber güvenlik alanında yasal çerçeve geliştirilerek uygulanacaktır. Bunlar; standartlaştırılmış ancak farklılaştırılmış siber güvenlik gereksinimleri

hazırlayarak, en iyi uygulamaları, siber güvenliği sağlamak için geçerli standartları analiz ederek, siber güvenlik kuruluşlarını bu tür standartlara uymaya teşvik ederek, ilgili taraflar arasında her düzeyde işbirliğini sağlamak için ulusal bir entegre kriz yönetimi mekanizması kurarak, siber güvenlik risk değerlendirme sistemini güncelleyerek, fonların tahsisi ve kullanımı için öncelikler belirlerken siber güvenliği sağlamak için gerekli olan fonları izlemek ve kontrol etmek için metodolojik imkânları değerlendirerek, siber güvenlik politikası oluşturma ve uygulamasının diğer önlemlerini uygulayarak yapılacaktır.

c. *Birinci hedefin üçüncü amacı, ulusal siber güvenlik tatbikatlarını ve uluslararası tatbikatlara katılımı teşvik etmektir:* Bu hedef, periyodik olarak karmaşık ulusal siber güvenlik tatbikatları düzenleyerek ve AB, NATO ve diğer ülkeler tarafından düzenlenen uluslararası siber güvenlik tatbikatlarına katılarak uygulanacaktır. Bunlar; ulusal ve uluslararası uygulamalardan öğrenilen dersleri durumların yönetimi, olay değerlendirmesi, bilgi iletişimi ve diğer faaliyetlere dahil ederek yapılacaktır.

d. *Birinci hedefin dördüncü amacı, ülkenin siber savunma kabiliyetlerini geliştirmektir:* Bu hedefe Litvanya Silahlı Kuvvetleri ile sivil siber savunma yetenekleri arasında etkili etkileşim sağlanarak ulaşılacaktır. Bunlar; siber savunma yeteneklerini geliştirerek, diğer devlet ve belediye kurum ve kuruluşlarına yardım sağlayarak yapılacaktır.

2. <u>*Siber Suçlar*</u>: Stratejinin ikinci hedefi, siber suçların önlenmesi ve soruşturulmasını sağlamaktır. Stratejinin ikinci hedefine ulaşmak için atılacak adımlar:

a. *İkinci hedefin ilk amacı, ülkenin siber suçlarla mücadele için yetenek ve kapasitelerini geliştirmektir:* Bu amaca, yasal çerçeveyi iyileştirerek, kolluk kuvvetlerinin mesleki kapasitesini daha da güçlendirerek, bilgi ve/veya analiz sistemleri oluşturarak, siber suçlarla mücadele için özel olarak tasarlanmış gelişmiş operasyonel yöntemler, prosedürler ve teknik araçları uygulamaya koyarak ulaşılacaktır.

b. *İkinci hedefin ikinci amacı, siber suçların önlenmesi ve kontrolünü güçlendirmektir:* Bu hedef, toplumun kendini koruma kültürünü ve siber uzayda sorumlu davranışı teşvik ederek uygulanacaktır; kolluk kuvvetlerinin operasyonel etkinliğini artırarak ve siber suçları araştırırken etkili uluslararası işbirliğini sağlayarak; kolluk kuvvetleri ile akademi, özel ve kamu sektörü temsilcileri ve toplum arasında etkili işbirliğini geliştirerek ulaşılacaktır.

3. <u>*Siber Güvenlik Kültürü ve İnovasyon*</u>: Stratejinin üçüncü hedefi, siber güvenlik kültürünü ve yeniliğini teşvik etmektir. Stratejinin üçüncü hedefine ulaşmak için atılacak adımlar:
   a. *Üçüncü hedefin birinci amacı, siber güvenlik alanında yüksek katma değer yaratan bilimsel araştırma ve faaliyetler geliştirmektir:* Bu hedef, yeni, gelişmiş siber güvenlik girişimlerinin oluşturulması için uygun koşullar yaratılarak uygulanacaktır; siber güvenlik hizmetlerinin dış pazarlara ihracatını genişleterek siber güvenlik pazarının büyümesini teşvik ederek; finansal teknolojinin siber güvenlik sektörünü geliştirerek ve araştırmalar yaparak ulaşılacaktır.
   b. *Üçüncü hedefin ikinci amacı, pazarın ihtiyaçlarını karşılayan yaratıcılığı, gelişmiş yetenekleri ve siber güvenlik becerilerini ve yetkinliğini geliştirmektir:* Bu hedef, bir siber güvenlik yetkinlik modeli oluşturarak uygulanacaktır; siber güvenlik yeterlilik standartları oluşturarak; işgücü piyasasının ihtiyaçlarına yönelik eğitim, akreditasyon, sertifikasyon sistemleri geliştirerek; yetenekleri çekerek, besleyerek ve elde tutarak; siber güvenlik için eğitim ve test ortamları oluşturarak; yeni gelenlere öğreterek ve hassas verilerle çalışan çalışanları eğiterek ulaşılacaktır.
   c. *Üçüncü hedefin üçüncü hedefi, siber güvenlik alanında yenilik yaratırken kamu, özel ve akademik ortaklıkları teşvik etmektir:* Bu hedef, özel ve kamu sektörünün ortak ihtiyaçları ve bunların bilimsel siber güvenlik araştırmaları açısından önemi belirlenerek uygulanacaktır; teknik önlemler, yöntemler ve diğer kaynaklar oluşturarak; ve siber güvenlik sorunlarını çözmek veya siber güvenlik için diğer belirli görevleri yerine getirmek için gerekli uzmanlığı geliştirerek ulaşılacaktır.
4. <u>*Özel-Kamu Ortaklığı*</u>: Stratejinin dördüncü hedefi, PPP'nin yakınlaşmasını teşvik etmektir. Stratejinin dördüncü hedefine ulaşılmasına yönelik hedefler:
   a. *Dördüncü hedefin ilk amacı, PPP'nin koordinasyonunu iyileştirmektir:* Bu hedef, siber güvenlik alanında sürdürülebilir bir KÖİ modeli oluşturularak uygulanacaktır; siber güvenlikle ilgili sorumlulukları ve yetenekleri belirleyerek; siber tehditler, siber olaylar ve çıkarılan dersler hakkında etkili bilgi alışverişini geliştirerek; erken uyarı sistemini destekleyerek; yeni iletişim tekniklerini ve süreçlerini oluşturarak veya iyileştirerek ulaşılacaktır.
   b. *Dördüncü hedefin ikinci amacı, küçük ve orta ölçekli işletmelerin (bundan böyle KOBİ'ler olarak anılacaktır) siber güvenlik olgunluğunu artırmaktır:* Bu hedef, küçük işletmelerin siber güvenlik durumlarını doğrulamaları ve siber güvenlik açıklarını gidermeleri için teşvik edilerek uygulanacaktır.

c. *Dördüncü hedefin üçüncü amacı, sorumlu bir güvenlik açığı ifşa uygulaması geliştirmektir:* Bu amaç, operasyonel ilkeler, yöntemler, teknik yetenekler veya bu amaç için tasarlanmış diğer önlemler belirlenerek uygulanacaktır.

5. <u>*Uluslararası İşbirliği*</u>: Stratejinin beşinci hedefi, uluslararası işbirliğini geliştirmek ve siber güvenlik alanındaki uluslararası yükümlülüklerin yerine getirilmesini sağlamaktır. Stratejinin beşinci hedefinin gerçekleştirilmesi için atılacak adımlar:
   a. *Beşinci hedefin ilk amacı, siber güvenlik alanında Baltık bölgesi ülkeleriyle işbirliği de dahil olmak üzere uluslararası, sınır ötesi işbirliğini geliştirmektir:* Bu hedef, Avrupa Birliği, NATO, Birleşmiş Milletler, Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT), Baltık bölgesi teşkilatları ve diğer uluslararası kuruluşların faaliyetlerine katılarak gerçekleştirilecektir.
   b. *Beşinci hedefin ikinci amacı, uluslararası siber güvenlik yeteneklerini ve kapasitelerini güçlendirmektir:* Bu hedef, daha yüksek kriterleri karşılayan askeri yeteneklere sahip AB üye devletleri açısından güvenlik ve savunma alanında işbirliğinin geliştirilmesi için Güvenlik ve Savunma Politikasında Kalıcı Yapılandırılmış İşbirliği projesini başlatarak ve yöneterek uygulanacaktır.
   c. *Beşinci hedefin üçüncü hedefi, Amerika Birleşik Devletleri ile siber savunma alanında diyaloğu daha da geliştirmek ve Amerika Birleşik Devletleri'nin Litvanya'nın siber güvenlik projelerine katılımı için çabalamaktır:* Bu hedef, Litvanya ve ABD arasında teknik ve siyasi düzeylerde ikili işbirliği geliştirilerek ve Litvanya'nın siber savunma ve siber güvenlik yeteneklerini güçlendirecek faaliyetler sürdürülerek uygulanacaktır.

Litvanya Cumhuriyeti Hükümeti, stratejinin hedeflerini ve hedeflerini uygulamak için belirli önlemlerin ve fonların öngörüldüğü kurumlar arası bir operasyonel planı onaylayacaktır. Milli Savunma Bakanlığı bu planın hazırlanmasını koordine edecektir. Stratejinin kurumlar arası operasyonel planında belirtilen bakanlıklar, diğer devlet veya belediye yetkilileri, kurumları veya kuruluşları, yetkileri dahilinde stratejinin uygulanmasına katılacaktır (Litvanya, 2018).

4.24. Malta'nın Siber Güvenlik Stratejisi

Malta Siber Güvenlik Stratejisi 2016 yılında yayımlanmıştır. Sekiz ana bölümden oluşan eylem planı oldukça detaylı ve kapsamlıdır. Yönetici özetinde ve giriş kısmında tespitler ve

değerlendirmeler yer almaktadır. Siber uzay mükemmel olmaktan uzaktır. Güvenlik açıkları risk altındadır, bunlardan bazıları insan zafiyetlerini içerirken, diğerleri kötü niyetle karşı karşıyadır (Malta, 2016).

Ulusal ölçekte siber güvenliğin başlatılması, esas olarak planlı, toplu ve sistemik bir yaklaşımı gerektirir ve bu nedenle bir Ulusal Siber Güvenlik Stratejisine ihtiyaç duyulmuştur. Malta'nın siber alanın ayrılmaz bir parçası olarak dikkate alması gereken siber güvenlik, kapsamı ve sonuçları hakkında bir farkındalık aşılamayı amaçlamıştır. Ulusal Siber Güvenlik Stratejisi, siber güvenlik ile mücadelenin aşağıdakileri gerektirdiğini kabul etmektedir (Malta, 2016):

- Malta Anayasası ve Malta'nın Avrupa Birliği Üye Devleti rolüne uygun olarak hukukun üstünlüğünü korumak,
- Çok disiplinli bir yaklaşımı benimsemek,
- Siber uzayın tüm paydaşlarının olmasını sağlamak;
- Ortak sorumluluklarını anlamak ve
- Herhangi bir siber saldırıya karşı bağışıklığı garanti etmenin imkansız olduğu varsayımına dayanan risk temelli bir yaklaşım benimsemek.

Eylem planının vizyonu, siber güvenliği sağlamak için üç temel ulusal paydaşın (kamu sektörü, özel sektör ve sivil toplum) ihtiyaç ve beklentilerini kapsamaktadır. Beş boyut, vizyonun stratejiye eklenmesini sağlar. Bunlar, daha sonra önerilen stratejinin dayandığı politika, mevzuat, risk yönetimi, farkındalık ve eğitimdir. Bununla birlikte, stratejiyi önermeden önce, yerel bağlamda siber güvenliğe yönelik üst düzey pragmatik bir yaklaşım sağlamak için araştırma ve değerlendirmeler yapılmıştır (Malta, 2016).

1. *Hedef- Bir Yönetişim Çerçevesi Oluşturmak:* Bu, bir siber güvenlik stratejisinin oluşturulması ve daha da önemlisi, etkin bir şekilde uygulanması ve sürekli olarak sürdürülmesi gerektiği öncülüne dayanmaktadır. Bu nedenle, özellikle kamu ve özel sektörde siber risk yönetimine odaklanarak temel koordinasyon yapılarını, süreçlerini, rollerini ve uygulamalarını sağlama ihtiyacını öngörmelidir.
2. *Hedef- Siber Suçla Mücadele:* Siber suçla mücadele yeteneklerini sağlamayı ve sağlamlaştırmayı amaçlamaktadır.

3. *Hedef- Ulusal Siber Savunmayı Güçlendirmek:* Siber güvenlik bilgi ve istihbaratının paylaşımını teşvik etmeyi, mevcut mevzuat ve düzenlemeleri siber uzay gelişmeleri doğrultusunda gözden geçirmeyi, ulusal ve kurumsal geniş ölçekte dijital esnekliği sağlamayı amaçlayan, AB düzeyinde, özellikle ilgili mevzuat başta olmak üzere, son yasal gelişmelerdir.
4. *Hedef- Güvenli Siber Uzay:* Mevzuatın siber güvenlik taahhütleri için her derde deva olmadığını göz önünde bulundurarak, öz düzenlemeyi ve gönüllü öz taahhüdü teşvik etmeyi amaçlamaktadır. Ayrıca, birlikte çalışabilirliğe izin verirken güvenliği garanti eden standartların ve en iyi uygulamaların kullanımını teşvik etmeyi hedeflemektedir. Çevrimiçi kamu hizmetlerinin güvenliğini ve güvenini artırmak ve özel sektöre verilen desteği pekiştirmek için de özel bir önem verilmektedir.
5. *Hedef- Siber Güvenlik Farkındalığı ve Eğitim:* Siber güvenlik konusundaki farkındalığı, bilgiyi, yetenekleri ve uzmanlığı duyarlı hale getirme aracı olarak akademiyi, kamu ve özel sektörü ve vatandaşları hedeflemeyi amaçlamaktadır. Devam eden bir eğitim ve farkındalık kampanyasına yönelik ulusal bir stratejik yaklaşım özellikle tavsiye edilmektedir.
6. *Hedef- Ulusal ve Uluslararası İşbirliği*: Siber güvenliğin sınır tanımadığı anlayışından hareketle, AB ve uluslararası kurum ve faaliyetler tarafından sağlanan, ulusal düzeyde, Avrupa ve küresel bazda etkin danışma, işbirliği ve işbirliğini sağlamayı amaçlamaktadır.

Altı hedefin tümü, eylem planından beklenen iki temel stratejik sonucu, yani aşağıdakileri kapsamayı amaçlamaktadır (Malta, 2016):

- Ulusal bilgi altyapısını siber tehditlere karşı savunmak ve korumak.
- Siber uzay kullanıcılarının güvenliğini, güvenilirliğini ve korunmasını sağlamak.

Önerilen stratejik yaklaşım hiçbir şekilde kendi başına bir amaç değildir. Stratejinin başlatılmasının, aşağıdakiler doğrultusunda geçerliliğini ve etkinliğini sağlamak için uygulanmasını, değerlendirilmesini ve sürdürülmesini gerektiren sürekli bir sürecin yalnızca başlangıcı olduğu anlaşılmaktadır (Malta, 2016):

- Siber güvenliğin ulusal ölçekte başlatılması, esasen planlı, kolektif ve sistemik bir yaklaşımı gerektirir ve böylece bir Ulusal Siber Güvenlik Stratejisine ihtiyaç duyulması,
- Günlük kurumsal ve bireysel faaliyetlerde siber güvenlik önlemlerinin benimsenmesinin öneminin ülke çapında daha fazla tanınması,
- Genel siber güvenlik kapasitesinin gelişen olgunluğu,
- İlgili siber güvenlik zorluklarıyla birlikte teknolojik gelişmeler ve uygulanabilirliği,
- Siber suç davranışında evrim,
- Malta'nın bir parçasını oluşturduğu üye devletlere yönelik siber güvenliğe ilişkin Avrupa Birliği yönergesi doğrultusunda ulusal ölçekte gelişmeler.

Bu nedenle, eylem planının periyodik olarak gözden geçirilmesi ve güncellenmesi beklenmektedir. Nihayetinde, eylem planı, Malta'yı şu şekilde gösteren ulusal siber güvenlik yatırımı için bir araç olarak anlaşılmaktadır (Malta, 2016):

- Güvenli çevrimiçi yargı yetkisi,
- Siber uzay içinde etkileşimde bulunan çeşitli iş sektörlerinde mükemmellik merkezi.

Ulusal Siber Güvenlik Stratejisi, çeşitli hedefleri ve ilgili önlemleri aracılığıyla aşağıdakiler hedeflemektedir (Malta, 2016):

- Siber güvenliği ulusal bir yatırım olarak konumlandırmak,
- Siber güvenliğin tek başına sağlanamayacağına dair anahtar mesajın duyurmak,

Siber güvenlik tanımları çoktur; ancak hepsi esasen siber alanın güvenliğine işaret etmektedir. Bunlar (Malta, 2016);

- Birbirine bağlı BİT donanım ve yazılım altyapısı
- Ağlarda geçiş halindeki ve beklemedeki veriler
- Bağlı kullanıcılar
- Aralarında kurulan mantıksal bağlantılar

Eylem planında belirlenen kılavuz ilkeler aşağıdaki gibidir (Malta, 2016):

- *Hukuk Kuralı*: Siber güvenlik yaklaşımı, Avrupa Birliği ve ulusal mevzuatta belirtilen temel haklara, özgürlüklere saygı duyulur ve bunlar desteklenir. Tüm önlemler, hesap verebilirliği ve önlemeyi sağlamak için uygun önlemlerle birlikte gereklilik, orantılılık ve yasallık ilkelerine uygun olacaktır.
- *Çok Paydaşlı Ev İşbirlikçi Yaklaşım*: Siber uzayın yaygın doğası, esasen hem ulusal düzeyde hem de Malta kıyılarının ötesinde güvenliğine yönelik çok paydaşlı bir yaklaşım gerektirir. Bu nedenle, ulusal düzeyde, kamu sektörü, özel sektör, akademi ve sivil toplum dahil olmak üzere çeşitli paydaşların işbirliği ve işbirliği gereklidir. AB düzeyinde ve uluslararası düzeyde işbirliğine dayalı ve işbirliğine dayalı bir yaklaşım da gereklidir.
- *Paylaşılan Hedef ve Sorumluluk*: Etkili siber güvenlik, esasen sınırları aşan ortak bir hedefin paylaşılmasını gerektirir. Hükümet, ulusal ölçekte siber güvenliğe yönelik taahhüdünde liderlik ederken, tüm siber uzayı koruma sorumluluğunu tek başına üstlenemez. Tüm BİT kullanıcıları, sistemleri ve verileri tek tek ve toplu olarak korumak için makul adımlar atmakla yükümlüdür.
- *Risk Yönetimi*: Siber uzayın geniş çapta yaygın kullanımı, hızlı ve sürekli gelişimiyle birleştiğinde, herhangi bir siber saldırı türüne karşı bağışıklığı garanti etmeyi imkansız hale getirir. Bu nedenle, her türlü teknoloji yatırımı ile birlikte siber güvenliği sağlamak için değerlendirmek, önceliklendirmek ve önlem almak için risk temelli bir yaklaşım gereklidir.

Eklenen ilkeler bağlamında, Ulusal Siber Güvenlik Stratejisi için genel bir vizyon: "*Dijital ekonominin faydalarını en üst düzeye çıkarırken Malta'nın emniyetini ve güvenliğini destekleyen güvenli, esnek ve güvenilir bir dijital etkileşimli ortam sağlamak.*" şeklindedir. Ulusal Siber Güvenlik Stratejisi, önerilen vizyon ışığında yukarıdaki paydaşların her birinin ihtiyaç ve beklentilerini ele almayı amaçlamaktadır (Malta, 2016).

- Politika: Ulusal düzeyde yönü belirleyen siber güvenlik politikası ve stratejisi geliştirmek.
- Mevzuat: Stratejinin tüm yönlerini desteklemek için etkili yasal ve düzenleyici çerçeveler oluşturmak.
- Risk Yönetimi: Organizasyon, standartlar ve teknoloji aracılığıyla riskleri kontrol etmek.

- Kültür: Toplumda sorumlu bir siber kültürü teşvik etmek için farkındalığı teşvik etmek.
- Eğitim: Etkili eğitim yoluyla iş gücüne ve liderliğe siber beceriler kazandırmak.

Ulusal Siber Güvenlik Stratejisi için dört yüksek seviyeli hedef önermektedir (Malta, 2016):

- Siber Suçla Mücadele: Kolluk kuvvetleri, boşlukları tespit etmeli ve siber suçları araştırma ve bunlarla mücadele etme yeteneklerini güçlendirmelidir.
- Ulusal Siber Savunmanın Güçlendirilmesi: Kamu ve özel kuruluşlar, siber savunma yeteneklerini güçlendirmek için yönlendirilmeli ve yardım edilmelidir.
- Güvenli Siber Uzay: Farkındalık programları ve gizlilik, bütünlük, kullanılabilirlik ve mahremiyet sağlayan güvenilir, BİT destekli hizmetlerin sunulması yoluyla daha yüksek güven seviyeleri aşılanacaktır.
- Kapasite Oluşturma (Siber Güvenlik Farkındalığı ve Eğitim): Gerekli beceriler ve eğitim çerçeveleri belirlenmeli ve geliştirilmelidir.

Bununla birlikte, eylem planının sürekli olarak etkin bir şekilde uygulanması için gerekli olan sağlam ve istikrarlı yönetişim, iki başka hedefi de içermektedir (Malta, 2016):

- Ulusal Siber Güvenlik Stratejisi elde etmek için bir yönetişim çerçevesi oluşturulmalı: Bu aşamada sadece teknik ve operasyonel yapıların oluştuğu göz önüne alındığında. Siber güvenlikte uzun vadeli trendlere, analizlere ve koordinasyona odaklanan stratejik seviye de gereklidir.
- Ulusal ve uluslararası işbirliği siber ile ilgili faaliyetlerin sınırsız doğası, esasen özellikle ilgili güvenliğin ulusal odağı dışında küresel ve bölgesel boyutları vardır. Toplamda altı hedef, Stratejiden beklenen iki temel stratejik sonucu kapsamayı amaçlamaktadır:
  - ✓ Ulusal bilgi altyapısını siber tehditlere karşı savunmak ve korumak ve
  - ✓ Siber uzay kullanıcılarının güvenliğini, güvenliğini ve korunmasını sağlamak.

Aşağıdakilere dayalı olarak her bir ilgili hedef için bir dizi önlem aşağıda önerilmiştir (Malta, 2016):

- Analiz ve yerel bağlamda yürütülen istişareler,

- Avrupa Birliği içindeki ve dünya çapındaki siber güvenlik stratejilerinde belirtilen en iyi uygulamalar,
- AB yasal gereksinimleri ve yönü,
- Dijital Malta Devleti içindeki ilgili eylem öğeleri ve e-ticaret gibi diğer yerel stratejiler.

Ulusal Siber Güvenlik Stratejisi, hedefleri ve müteakip önlemleri aracılığıyla, yönetişim, mevzuat, düzenleme ve gönüllü taahhüt, risk yönetimi ve eğitim ve farkındalık alanlarını kapsamaktadır. Bunların tümü siber güvenliği sürdürülebilir bir konuma getirmektedir. Stratejinin uygulanmasının kamu ve özel sektördeki çok sayıda paydaşı ve sivil toplumla işbirliği ve koordinasyonu içermesi beklenmektedir. Ulusal ve Avrupa Birliği cephesinde ilgili yöndeki gelişmelerin yanı sıra bu uygulamadan kaydedilen ilerlemeye dayalı olarak periyodik olarak değerlendirilmesi beklenmektedir (Malta, 2016).

4.25. Polonya'nın Ulusal Siber Güvenlik Stratejisi

Polonya'nın Ulusal Siber Güvenlik Stratejisi 2017-2022 dönemini kapsamakta olup tam ismi "2017- Polonya Cumhuriyeti 2022 Dönemi Siber Güvenlik Politikasının Çerçevesi"dir. Belge 11 başlıktan oluşmaktadır. Başlıkları aşağıdaki gibi sıralamak mümkündür (Polonya, 2017):

1. Giriş
2. Stratejik bağlam
3. Ulusal Siber Güvenlik Politikası Çerçevesinin Kapsamı
4. Vizyon, Ana Hedef, Özel Amaçlar
5. *Özel Hedef 1:* Devletin işleyişi için hayati önem taşıyan BİT sistemlerinin güvenliğini tehlikeye atan olayların etkilerini önlemek, tespit etmek, mücadele etmek ve en aza indirmek için koordineli eylemler geliştirmek.
6. *Özel Hedef 2:* Siber tehditlere karşı koyma kapasitesini arttırmak.
7. *Özel Hedef 3:* Siber uzayda güvenlik alanındaki ulusal siber güvenlik potansiyelini ve yetkinliğini geliştirmek.
8. *Özel Hedef 4:* Polonya'nın siber güvenlik alanında güçlü bir uluslararası pozisyon oluşturmak.
9. Ulusal Güvenlik Politikası Çerçevesini Yönetme

10. Finansman
11. Sözlük

Strateji belgesinin giriş bölümünde sosyal ve ekonomik gelişmelerin, bilgiye hızlı ve engelsiz erişmenin önemini arttırdığı ve yönetim, üretim ve hizmet sektöründe veya kamu kuruluşlarının güveliğinin daha önemli bir hal aldığı ifade edilmiştir. Daha büyük veri kümelerinin analizini içeren ağ ve bilgi sistemlerinin sürekli gelişimi, iletişim, ticaret, ulaşım veya finansal hizmetlerin ilerlemesine yardımcı olmaktadır. İnternet, sosyal grupların davranışlarını etkilemenin yanı sıra siyasi alanda da etkili bir araç haline gelmiştir. Küresel ya da yerel siber alanın işleyişindeki herhangi bir kesinti, vatandaşın güvenliğinin ve güvenlik duygusunun, kamu sektörü kurumlarının etkinliğinin, üretim ve hizmet süreçlerinin ve nihayetinde ulusal güvenliğin üzerinde etkili olmaktadır (Polonya, 2017).

Bilgi güvenliğini sağlamak, ulusal siber güvenlik sistemini oluşturan tüm kuruluşların, yani bilgi iletişim teknoloji sistemlerini kullanan işletmeler, bireysel kullanıcılar, kamu otoriteleri, uzman kuruluşlar için hayati bir önem kazanmıştır. Bu nedenle, Polonya'nın AB, NATO, BM ve AGİT gibi örgütler içindeki uluslararası işbirliği yoluyla diğer devletlerle yakından bağlantılı olması gerektiği vurgulanmıştır. Bu işbirliği, siber alandaki yasa dışı faaliyetlerin neden olduğu artan olaylarla, maddi ve itibarî zararlara yol açan mücadelede önemli bir rol oynayacağı değerlendirilmiştir (Polonya, 2017).

Stratejik bağlam başlığı altında Polonya Cumhuriyeti'nin 2017-2022 Ulusal Siber Güvenlik Politikası Çerçevesi ve Koruma Politikası dahil olmak üzere siber güvenlik seviyesini yükseltmeyi amaçladığı, hükümet idaresi tarafından alınan ve devam eden eylemler sürecinde stratejik bir belge olarak tanımlanmıştır. Polonya'nın mevcut stratejilerin başarısının, hem ulusal kalkınma stratejilerine hem BT sistemlerine hem de ulusal güvenlik ve yasal düzenlemelere bağlanmıştır. Dijitalleştirme sadece bir ilerleme ve yenilik kaynağı değil aynı zamanda riskli olarak değerlendirilmiş ve ortaya çıkan tehditler ışığında, BT sistemlerinin yaygın kullanımının, toplumun ve girişimcilerin bu sistemlere artan bağımlılığının ulusal siber güvenlik sistemini genişletmek ve devletin genelinde tutarlı bir yaklaşımın alınmasını sağlamak için esas olduğu vurgulanmıştır (Polonya, 2017).

Belgenin amacı ise, ulusal bilgi iletişim teknolojileri sistemlerinin, temel hizmet sağlayıcıların, kritik altyapı operatörlerinin, dijital servis sağlayıcıların ve siber olaylara

yönelik kamu idarelerinin yüksek düzeyde esnekliğini sağlamaya yönelik çerçeve faaliyetlerini tanımlamak olarak belirlenmiştir. Önerilen stratejik amaçlar, kolluk kuvvetlerinin ve adli makamların suçları, terör eylemlerini ve siber alanda casusluk faaliyetlerinin tespitini artırması beklenmiştir. Polonya Hükümeti, Ulusal Siber Güvenlik Politikası Çerçevesini uygularken, mahremiyet hakkına tam olarak saygı göstereceğini ve ücretsiz, açık bir internet prensibini savunmuştur. Ulusal siber güvenlik politikası çerçevesinin kapsamı aşağıdaki şekilde tanımlanmıştır (Polonya, 2017):

- ✓ Bilgi iletişim teknolojilerinin güvenliğinin sağlanması,
- ✓ Ulusal siber güvenlik politikasının uygulanmasına katılan başlıca aktörlerin belirlenmesi,
- ✓ Ulusal siber güvenlik politikasının hedeflerine ulaşmak için yönetim çerçevesinin oluşturulması,
- ✓ Kamu ve özel sektör arasındaki işbirliğini artırmak ve siber saldırıları önleme, müdahale etme ve olayların ardından hizmetleri normale döndürülmesinin sağlanması,
- ✓ Risk değerlendirme yaklaşımın geliştirilmesi,
- ✓ Siber güvenlik ile ilgili eğitim, bilgilendirme ve eğitim programlarının düzenlenmesi,
- ✓ Bilgi iletişim teknolojileri güvenliği alanındaki araştırma ve geliştirme faaliyetlerinin desteklenmesi,
- ✓ Siber güvenlik alanında uluslararası işbirliğinin artırılması.

Ulusal Siber Güvenlik Politikası Çerçevesi, 2018 yılının Mayıs ayında Polonya Bakanlar Kurulu kararı ile kabul edilmiş ve uygulamaya konulmuştur. Belgede Polonya'nın siber güvenlik vizyonu "*2022'de Polonya, siber uzaydan saldırılara ve tehditlere karşı daha dayanıklı olacaktır. Ülke içi ve uluslararası faaliyetlerin bir araya gelmesiyle, Polonya'nın siber kapasitesi, devletin işlevlerini yerine getirebilmesi ve dijital ekonominin potansiyelini tam olarak kullanmasına izin verirken aynı zamanda kişisel haklara ve vatandaşların özgürlüklerine saygılı olacaktır.*" seklinde tanımlanmıştır. Ana amaç ise "*Temel ve dijital hizmetlerin sağlanması veya kullanılması sürecinde kamu ve özel sektörlerin yanı sıra vatandaşların yüksek düzeyde güvenliğinin sağlanması amaçlanmıştır.*" olarak belirlenmiştir. Özel hedefler ise aşağıda sunulmuştur (Polonya, 2017):

Özel Hedef 1: Devletin işleyişi için hayati önem taşıyan bilgi iletişim teknoloji sistemlerinin güvenliğini tehlikeye atan olayların engellenmesi, tespit edilmesi, mücadele edilmesi ve en aza indirilmesi için ulusal olarak koordine edilmiş eylemlerin hayata geçirilmesi.
Özel Hedef 2: Siber tehditlere karşı koymak için kapasite geliştirilmesi.
Özel Hedef 3: Siber uzayda güvenlik alanındaki ulusal potansiyel ve yetkinliğin arttırılması.
Özel Hedef 4: Polonya Cumhuriyeti için siber güvenlik alanında güçlü bir uluslararası konum oluşturulması.

Her bir özel hedefin altında belirlenen alt eylemler ve amaçları kısaca aşağıda açıklanmıştır:

1. Özel Hedef 1: Devletin işleyişi için hayati önem taşıyan bilgi iletişim teknoloji sistemlerinin güvenliğini tehlikeye atan olayların engellenmesi, tespit edilmesi, mücadele edilmesi ve en aza indirilmesi için ulusal olarak koordine edilmiş eylemlerin hayata geçirilmesi.
   a. *Yasal çevrenin siber güvenlik alanındaki ihtiyaç ve zorluklara uyarlanması:* Ulusal siber güvenlik sisteminin geliştirilmesinin yasal değişiklikler istediğinden Polonya, yasal hükümleri hayata geçireceğini açıklamıştır. Bunun yanı sıra, siber aleme uyum sağlamak, verimliliği artırmak ve ulusal siber güvenlik sisteminin oluşturulmasında yer alan tüm paydaşlar arasında bilgi akışını iyileştirmek için çalışmalar yapmayı taahhüt etmiştir.
   b. *Ulusal siber güvenlik sisteminin yapısının iyileştirilmesi:* Sistemin, ulusal güvenlikten sorumlu organları, terörle mücadele çabaları, iç güvenlik ve kamu düzeni, savcılık hizmeti ve yargı dahil olmak üzere, ulusal siber güvenlik sistemindeki çeşitli paydaşlar arasındaki ilişkinin geliştirmesi hedeflenmiştir.
   c. *Siber alanında güvenliği sağlayan işletmelerle işbirliğinin etkinliğini artırmak:* Tehditlere ve saldırılara etkin cevap vermenin temeli, ulusal siber güvenlik sisteminde paydaşlar arasında bilgi alışverişinde bulunmak için güvenilir ve güvenli mekanizmaların etkili işleyişi olduğunu ifade eden Polonya, Uluslararası işbirliği alanında, ulusal organizasyonlar, AB ve NATO organları ve diğer uluslararası aktörler tarafından gerçekleştirilen tatbikatlara aktif olarak katılmayı, gerçekleştirilen araştırma ve eğitimlere dayanarak, siber güvenliği geliştirmek için kılavuzlar ve tavsiyeler geliştirmeyi amaçlamaktadır.
   d. *Temel ve dijital servislerin ve kritik altyapının güvenliğini arttırmak:* Günümüzde bilgi ve iletişim teknolojileri, ekonomik gelişmenin temeli haline geldiği ifade

edilerek Bakanlar Kurulu bilgi iletişim teknolojileri (BİT) güvenliğini sağlamayı öncelik olarak kabul edeceğini ve hizmetlerin güvenliğini sağlama sorumluluğu temel olarak tedarikçilere ait olmasına rağmen hükümetin siber güvenlik konusundaki kapasitelerini artıracağı ve yeterliliklerini geliştirmek için harekete geçeceği vurgulanmıştır.

e. *Ağ ve bilgi sistemlerinin güvenliği ile ilgili standartların ve iyi uygulamaların geliştirilmesini ve uygulanmasını sağlamak:* Teknik korumalar, sistem konfigürasyonu, güvenli çalışma prosedürleri ve güvenli kullanım için öneriler geliştirileceği ve bireysel hedef grupların ihtiyaçlarına göre uyarlanmış bilgi politikaları hazırlanacağı taahhüt edilmiştir. BİT sistemlerinin tüm kullanım ömrü boyunca, üretimden kullanıma, imhaya kadar güvenlik sağlanması önemlidir. Polonya, Uluslararası standartlara uygun olarak, piyasa düzenleyicilerinden gelen tavsiyeler ve iyi uygulamalardan yararlanacaktır.

f. *Güvenli bir tedarik zincirini kurmak:* BİT sistemlerinin yüksek düzeyde güvenliğini sağlamak, tasarımdan üretime, işletmeden sunuma kadar güvenli bir tedarik zincirini zorunlu kılmaktadır. Polonya, bilişim ve iletişim sektöründeki ürün ve hizmetlerin değerlendirilmesi ve belgelendirilmesi için bir Avrupa sisteminin kurulmasına aktif olarak katılmayı ve sertifikalandırma organlarını toplayan uluslararası organizasyonlarda aktif olarak yer almayı hedeflemektedir.

g. *Siber kullanıcılara siber tehditlerden kaynaklanan riskler konusunda uyarı veren bir sistem oluşturmak:* BİT sistemlerinin güvenliğini sağlamak için temel bir gereksinimdir. Tehditler ve güvenlik açıkları hakkındaki bilgilerin yanı sıra, meydana gelen veya olası saldırılarla ilgili bilgilerin paylaşılması önemlidir. Bu amaçla, ulusal düzeyde bir siber güvenlik yönetimi sisteminin inşa edilmesi ve bu sistem ile tehditlerin ve güvenlik açıklarının rapor edilmesi amaçlanmıştır. Ayrıca, son kullanıcıları belirlenen tehditlerin etkilerinden korumak için vatandaşlar için ek bir bilgi sistemi oluşturulacaktır.

2. <u>Özel Hedef 2: Siber tehditlere karşı koymak için kapasite geliştirilmesi.</u>

   a. *Siber uzayda meydana gelen siber suç ve siber suçlamalarla mücadele, siber suçluluk ve terörist nitelikteki olayları içeren kapasitenin arttırılması:* Hızla değişen suç yöntemleri, siber suçlara karşı koyma alanında araştırmanın geliştirilmesini gerektirmektedir. Bunun sonucu olarak kanun uygulayıcılara destek sağlanacağı, yapılacak çalışmaların kolluk kuvvetleri ve adli makamların

çalışmalarında kullanılacağı ve önleyici tedbirlerin geliştirilmesi için materyal sağlanacağı taahhüt edilmiştir. Toplumu siber suç tehditleri ve bunların önlenmesi veya azaltılması için araçlar hakkında bilgilendirmek için bilinçlendirme kampanyaları yapılması amaçlanmıştır.

b. *Siber alanda tam bir askeri harekât yelpazesi gerçekleştirme kapasitesinin kazanılması:* Devletin savunma sisteminin temel bir unsuru olan Polonya Silahlı Kuvvetleri siber uzayda havada, karada ve denizde olduğu kadar etkili davranmayı amaçlamıştır. Bu nedenle, siber alanda tam bir askeri harekât yelpazesi yürütme kabiliyetleri "*tehditlerin belirlenmesi, bilgi sistemlerinin korunması, savunulması ve tehditlerle kaynağında mücadele edilmesi*" şeklinde sıralanmıştır.
c. *Ulusal düzeyde tehdit analizi alanında kapasite oluşturulması:* Siber güvenlik sisteminin önemli bir unsuru, siber tehditler alanındaki durumun genel bir değerlendirmesini ve belirli tehdit ve olayların doğrulanması ile derinlemesine analizini gerçekleştirmek için gereken ulusal analitik yetenekleri korumak ve geliştirmektir.
d. Siber güvenlik sisteminin temel bir unsuru, siber tehditler alanındaki durumun genel bir değerlendirmesini ve belirli tehdit ve olayların doğrulanması ve derinlemesine analizini yapmak için gereken ulusal analitik yeteneklerin korunması ve geliştirilmesidir. Polonya Ulusal Siber Güvenlik Merkezi, ulusal ve yabancı kaynaklardan gelen bilgilere ve kendi çalışmalarına ve işbirliği yapan organların araştırmalarına dayanarak analitik görevler gerçekleştirmeyi ve Polonya'nın siber güvenliğini artırmayı hedeflemiştir.
e. *Ulusal güvenlik amacıyla güvenli bir iletişim sistemi kurmak:* Güvenli bir iletişim sistemi oluşturulması amaçlanmıştır. Bu durumun, ulusal güvenlik komuta sistemindeki ilgili kurumlar arasında etkin bilgi alışverişine olanak sağlayacağı öngörülmüştür. Ayrıca, kamu güvenlik kullanıcılarını, çeşitli düzeylerde ele alarak, ulusal güvenlik yönetiminde, kriz yönetiminde ve ulusal savunmaya hazır olma aşamalarında güvenilir bir iletişim sağlanması hedeflenmiştir. Bunun yanı sıra sistemin, NATO ve AB dahil olmak üzere iç ve dış ilişkilerde güvenli, zamanında ve güvenilir bilgi alışverişini sağlayacağı planlanmıştır.
f. *Güvenlik denetimlerinin ve testlerinin yapılması:* Halen uygulanmakta olan bilgi güvenliği yönetim sistemlerinin etkinliğini ve oluşturulan korumaların yeterliliğini değerlendirmeyi mümkün kılan önlemler alınacaktır. Kurallar ve iyi uygulamalar temelinde, bireysel sektörlerin ihtiyaçları göz önüne alınarak, tutarlı denetim

metodolojileri geliştirilecektir. Bu yaklaşımın amacı denetimlerin sonuçlarını karşılaştırılabilir hale getirmektir. Güvenliği değerlendirmenin bir başka ölçüsü, sistemin tehditlere karşı direncinin gerçek bir değerlendirmesini sağlayan penetrasyon testidir. Bunun sonuçları, gerektiğinde bu sistemlerin güvenliğini artırmak için kullanılması amaçlanmıştır.

3. Özel Hedef 3: Siber uzayda güvenlik alanındaki ulusal potansiyel ve yetkinliğin artırılması.
   a. *Siber güvenlik amaçlı endüstriyel ve teknolojik kaynakların geliştirilmesi:* Polonya hükümeti, siber güvenliğin sağlanması için endüstriyel ve teknolojik kaynakların geliştirilmesine yatırım yapmayı ve işletmelerin geliştirilmesi için gerekli koşulları yaratmayı (örneğin yeni siber güvenlik çözümleri oluşturacak olan bilimsel araştırma merkezlerini ve yeni kurulan şirketleri) hedeflemektedir.
   b. *Kamu sektörü ve özel sektör arasında işbirliği mekanizmaları oluşturmak:* Siber alanda güvenliğin sağlanması özel sektör, kamu sektörü ve vatandaşların ortak çabalarını gerektirir. Hükümet, siber alanda güvenlik konusunda güven ve ortak sorumluluğa dayalı etkili bir kamu-özel ortaklık sistemi kurmak için çaba göstereceğini ifade etmiştir. Aynı zamanda, kamu yönetimi, BİT güvenliği ile ilgili tüm ekonomik sektörlere danışmanlık sağlama kapasitesini geliştirmeyi hedeflemiştir. Hükümet ayrıca, Avrupa kamu-özel işbirliğinin mevcut ve gelişmekte olan biçimlerine aktif olarak dahil olmayı ve böylece uluslararası ticareti teşvik etmeyi taahhüt etmiştir.
   c. *Bilgi ve iletişim teknoloji sistemlerinin güvenliği alanındaki araştırma ve geliştirmeyi teşvik etmek:* Dinamik olarak büyümekte olan BT pazarına bakıldığında, özellikle şu anda internette kullanılan IPv4'ün yerine IPv6 değişme olasılığı, nesnelerin interneti (Iot), akıllı şehirler, Endüstri 4.0'ın yanı sıra Cloud Computing'in geliştirilmesi ile bağlantılı olarak ve Büyük Veri gibi gelişmeler ortaya çıkmıştır. Aşağıdakileri sağlamak amacıyla bilimsel ve akademik toplulukla işbirliği içinde araştırma programları geliştirilmesi hedeflenmiştir:
      i. Polonya'nın siber tehditlere karşı direncinin etkinliğini değerlendirmek,
      ii. Tehditlere cevap vermenin etkinliğini değerlendirmek,
      iii. Siber suçlar, siber terörizm ve bunlarla mücadelede yeni eğilimleri analiz etmek,
      iv. Saldırı yöntemlerini ve bu saldırılara karşı koyma yollarını incelemek.

d. Siber güvenlik alanındaki araştırma, geliştirme ve üretim faaliyetlerini geliştirmeye ihtiyaç vardır.

4. Özel Hedef 4: Polonya Cumhuriyeti için siber güvenlik alanında güçlü bir uluslararası konum oluşturulması.
   a. *Stratejik ve politik düzeyde aktif uluslararası işbirliğinin sağlanması:* Yaygın küreselleşme süreçleri ve ülkeler arasındaki karşılıklı bağımlılık ile birlikte, küresel siber alan güvenliğinin sağlanması için uluslararası işbirliği çok önemli bir hale gelmiştir. Polonya, Avrupa'da bu görevleri yerine getirirken, büyümenin ve yeniliğin itici gücü olan Dijital Tek Pazar'ın güvenliğini sağlama çabalarını yoğunlaşmayı hedeflemiştir. Ayrıca, Avrupa Birliği Ortak Dış ve Güvenlik Politikasının geliştirilmesi çalışmalarında siber güvenliğin boyutlarını daha fazla dikkate almak için çaba sarf etmeyi planlamaktadır.
   b. *Operasyonel ve teknik düzeyde aktif uluslararası işbirliği çalışmaları:* Diğerlerinin yanı sıra, Avrupa Birliği düzeyinde bilgisayar olayları müdahale ekibi ağı içerisinde, belirli bir sektörün BT güvenlik durumunun kontrol ve takip edilmesi işbirliği ağları aracılığıyla gerçekleştirilmesi amaçlanmıştır. Böylece Polonya'nın teknolojik çözümlerini ve ülkenin uzman personelini tanıtmak için bir fırsat olacağı değerlendirilmiştir.

Ulusal Güvenlik Politikası Çerçevesini Yönetme bölümünde eylem planının 5 yıllık bir süre için kabul edildiği, Dijital İşler Bakanlığı'nın koordinasyonunda olduğu, kabul edildikten iki yıl sonra ve geçerliliğin dördüncü yılında gözden geçirilmeye ve değerlendirmeye tabi tutulacağı, gözden geçirmenin sonuçlarının Bakanlar Kuruluna sunulacağı ve inceleme sonucunda düzeltici faaliyet teklifi veya taslak belge hazırlanacağı hedefleri koyulmuştur.

Finansman bölümünde ise mevcut düzenlemelere göre, kamu görevlerini yerine getiren işletmelerin zaten siber güvenlik harcamalarını mali planlarına dahil etmeleri gerektiğinden yola çıkılarak eylem planının uygulanmasına yönelik finansman maliyetlerinin tahminin daha sonra yapılacağı ifade edilmiştir. Sonuç olarak, ulusal ve devlet bütçesi dahilinde, siber güvenlik alanındaki projelerin geliştirilmesi ve uygulanmasının Çok Yıllı bir Program ile yapılması gerektiği vurgulanmıştır (Polonya, 2017).

4.26. Slovakya'nın Siber Güvenlik Stratejisi

Slovak Cumhuriyeti'nin Siber Güvenlik Stratejisi 2015-2020 dönemi için hazırlanmış ve onaylanmıştır. Strateji belgesi dört ana bölümden oluşmaktadır. İlk olarak dünya ve Slovakya konularında siber güvenlik kapsamında değerlendirme ve tespitlere yer verilmiştir. 20. yüzyılın ikinci yarısında itibaren bilgi ve iletişim teknolojilerinin kullanımındaki büyüme, toplumdaki gelişme eğilimlerini önemli ölçüde etkilemiştir. Modern bilgi ve iletişim teknolojileri, toplumun ve ekonominin çeşitli alanlarından coğrafi olarak uzak varlıklar arasındaki olasılıkları önemli ölçüde genişletmiş, etkileşim yöntemlerinin etkinliğini artırmıştır. Bilgi ve iletişim teknolojilerinin artan sayıda kullanıcısı, hem kamu hem de özel sektörün bu teknolojilere bağımlılığının artmasıyla sonuçlanmakta ve bu da onları daha savunmasız hale getirmektedir (Slovakya, 2015).

Slovak Cumhuriyeti'nin 2015-2020 yılları için oluşturduğu bu Siber Güvenlik Stratejisi, siber güvenlik alanında ülkenin başlangıç konumunu ve hedeflerini tanımlar. Eylem planı, Slovak Cumhuriyeti Güvenlik Stratejisi ile uyumlu hale getirilmiştir ve siber güvenliği sağlamak için gerekli düzenlemelerin, standartların, metodik talimatların, kuralların, güvenlik politikalarının ve diğer araçların müteakip oluşturulması için temel ve başlangıç belgesini oluşturmaktadır. Slovak Cumhuriyeti'ndeki siber güvenlikteki mevcut duruma dayanarak, eylem planının amacı aşağıdaki gibidir (Slovakya, 2015):

- Ulusal siber alanın korunması, kavramsal, koordineli, verimli, etkin ve yasal olarak işleyen bir sistemdir.
- Toplumun tüm bileşenlerinin güvenlik bilinci sistematik olarak artmaktadır.
- Özel ve akademik sektörler ile sivil toplum, Slovak Cumhuriyeti'nin siber güvenlik alanındaki politikasının formülasyonuna ve uygulanmasına aktif olarak katılır.
- Hem ulusal hem de uluslararası düzeyde verimli işbirliği sağlanır.
- Kabul edilen tedbirler yeterlidir ve mahremiyetin korunmasına ve temel insan hak ve özgürlüklerine saygı gösterir.

Slovak Cumhuriyeti'nin siber alandan gelen riskleri ve tehditleri kullanım faydalarını kısıtlamadan azaltmaya çalışmak için kullanacağı yöntem ve araçlar tanımlanmıştır. Eylem planının, aşağıdakileri hedefin temel uygulama araçları olarak kabul etmektedir (Slovakya, 2015):

- Uzmanlaşmış kurumlar ve terminoloji alanı.
- Yüksek risk kontrolü kültürü, özel ve kamu sektörü arasında bilgi alışverişi ve aktörlerin kapasitelerinin artması.
- Siber güvenlik alanında sistematik bilgilendirme ve karmaşık bir eğitim sistemi.
- Kamu, özel ve akademik sektörlerden ilgili tüm kuruluşların ulusal ve uluslararası düzeyde işbirliği ve ortaklıkları ve sivil toplum.
- Özellikle hibeler, AB fonları ve yeni ortaya çıkan projeler veya başlangıçlar için desteğin yanı sıra siber güvenliğin endüstriyel ve teknolojik kaynaklarının araştırılması, geliştirilmesi ve yenileştirilmesi için destek kullanarak siber güvenlik ürün ve hizmetleriyle bir iç pazarın geliştirilmesi.

Eylem, öncelikler olarak aşağıdaki yedi temel önlemi benimsemeyi ve çözmeyi önermektedir (Slovakya, 2015):

1. Siber Güvenlik Yönetimi İçin Kurumsal Çerçeve Oluşturma: Siber güvenlik için merkezi devlet idare organı kurulacaktır. Eylem planı, kanun koyucunun bu yetkiyi Ulusal Güvenlik Kurumu'na vermesini tavsiye etmektedir.
   a. Ulusal Olay Çözüm Birimi (ulusal CERT/CSIRT): Siber güvenlik için merkezi devlet otoritesine bağlı, ulusal düzeyde siber güvenlik alanında maddi kapsamı olan özel birim (aynı zamanda "*bilgisayar acil müdahale ekibinin*" görevlerini de yerine getirecektir.
   b. Siber güvenlik için sektör odaklı otorite: Mevcut merkezi devlet yetkililerinin organizasyon birimi kurulacaktır.
   c. Siber Olay Müdahele Birimi: Siber güvenliğin maddi önemi olan otorite olarak merkezi devlet idare makamı kurulacaktır. Tüm yönetim sektörlerinde siber güvenlik birimlerin fiziksel olarak kurulması öngörülmemektedir.
2. Siber Güvenlik İçin Yasal Çerçevenin Oluşturulması Ve Kabul Edilmesi: Slovak Cumhuriyeti'nde siber alanın korumasının etkinliğinde önemli bir artış için en yüksek öncelik, siber güvenlik kontrol sisteminin resmi yasal düzenlemesidir. Sınırlama olmaksızın aşağıdakileri sağlayacak özel bir Siber Güvenlik Yasası kabul edilecektir:
   a. Siber güvenlikte birleşik devlet politikasının oluşturulması ve uygulanmasının koordinasyonunu resmen sağlamak,
   b. Kamu otoritelerinin maddi yetki ve yetkilerinin yanı sıra yetkilerinin kullanım alanı ve yöntemini açıkça belirlemek,

c. Diğer aktörlerin yetki ve yeterliliklerini, bunların kapsamını ve uygulama yöntemini açıkça tanımlamak,
d. Siber uzayda bilgi ve iletişim teknolojilerini kullanan kurumlara görevler kurmak,
e. Diğer tüzel kişilerin ve gerçek kişilerin haklarını, hukuken korunan menfaatlerini garanti edecek ve görevlerini tanımlayacak,
f. Siber güvenlik alanı için bağlayıcı terminoloji ve standartlar oluşturulacak,
g. Münferit sektörlerde, yasanın pratik uygulaması, sektörün yönetimi ve işleyişi sistemindeki standartlar için metodik bir rehber yayınlanacak.

3. Siber Alanın Yönetimini Sağlayan Temel Mekanizmaların Geliştirilmesi ve Uygulanması: Siber alanı dirençli kılmak için özel görevler sağlamak için eylem planı, aşağıdaki temel mekanizmaların uygulanmasını ve geliştirilmesini tanımlamış ve önermiştir:
   a. *Karar verme ve kontrol mekanizması:* Siber güvenlik tehditlerini en aza indirmeyi ve kriz durumlarında büyümelerini önlemeyi amaçlayan önlemlerin sürekli sektörler arası planlama, organize etme, koordinasyon, uygulama ve kontrolü sağlanacaktır,
   b. *Önleme mekanizması:* Ortaya çıkan kriz durumlarına karşı harekete geçmeyi ve çoğunlukla bilgi ve teknik iletişim araçları için ima edilen potansiyel riskleri en aza indirmeyi amaçlayan koruyucu önlemler alınacaktır.
   c. *Tepki mekanizması:* Saldırıyı perdelemek veya saldırganın hasara yol açmasını önlemek için devam eden saldırılar durumunda alınması gereken olaylar ve/veya kriz durumlarında nitelikli ve etkili bir tepkiyi hedefleyen önlemler alınacaktır.
   d. *Restorasyon mekanizması:* Siber saldırıların neden olduğu hasarın sonuçlarını azaltmayı ve orijinal duruma geri dönmeyi amaçlayan kurtarma önlemleri alınacaktır.
4. Siber Güvenlik Alanında Bir Eğitim Sisteminin Desteklenmesi, Formüle Edilmesi ve Uygulanması: Siber güvenlik alanındaki önlemlerin ve görevlerin performansının kalitesi, etkinliği ve etkililiği büyük ölçüde sosyal farkındalık düzeyine, toplumun eğitim düzeyine ve aynı zamanda alandaki aktörlerin yeteneklerine bağlıdır. Bu amaçla, eylem planında eğitim ve tanıtım faaliyetlerine yer verileceği ifade edilmiştir.
5. Risk Yönetimi Kültürü ve Paydaşlar Arası İletişim Sisteminin Belirlenmesi ile Uygulanması: Siber güvenliğin kontrol yapısının varlıkları arasında ve ulusal siber alandaki diğer ilgili aktörler ile çevrimiçi iletişim ve bilgi alışverişi için etkin ve güvenli bir sistem, kurulmasını sağlamak için optimum yetkinliklerin ayarlanması ile

gereklidir. Bu nedenle, ulusal ve sektörel düzeylerde, özel sektörden kilit aktörler düzeyinde faaliyet gösterilecektir.

6. Uluslararası İşbirliği: Küresel yapısı gereği siber güvenlik, hem ulusal hem de uluslararası düzeyde yoğun bir ortak bilgi kullanımını ve faaliyetlerin koordinasyonunu gerektirir. Slovak Cumhuriyeti, NATO ve AB üye devleti olarak uluslararası stratejik ve kavramsal belgelerin, uluslararası politikaların ve standartların hazırlanmasına katılacak ve aynı zamanda en verimli işbirliği, değişim ve ortak kullanım modelini inşa edecektir. Slovak Cumhuriyeti, uluslararası siber eğitim ve tatbikatlar düzenleyecek ve bunlara katılacaktır.
7. Siber Güvenlik Alanında Bilim ve Araştırmanın Desteklenmesi: Kamu sektörünün özel sektör ve akademik kurumlarla işbirliği çerçevesinde, Slovak Cumhuriyeti ayrıca araştırma projelerinde (nitel ve nicel araştırmalar dahil) işbirliğinin geliştirilmesini desteklemeyi amaçlamaktadır. 2014-2020 programlama dönemi için araştırma ve yenilikler işletim programı fonlarının kullanımını vurgulayarak, siber güvenlik alanındaki ulusal ve Avrupa araştırma projelerine ve faaliyetlerine katılımı destekleyecektir. Bölgedeki araştırma faaliyetleri, siber güvenlik için merkezi devlet idare otoritesi tarafından koordine edilecektir.

Ulusal siber alanı korumak, Slovak Cumhuriyeti'nin bir AB ve NATO üyesi ülke olarak taahhütlerini ve diğer üye devletlerden edinilen deneyimler temelinde diğer uluslararası taahhütleri yerine getirmeyi amaçlamaktadır. Eylem planı, siber güvenliği sağlamak için gerekli olan düzenlemelerin, standartların, metodolojinin, kuralların, güvenlik politikalarının ve diğer araçların müteakip formülasyonu için temel ve başlangıç belgesidir. Slovak Cumhuriyeti, AB, NATO ve diğer uluslararası kuruluşların kurumlarında kanun, standart ve normların hazırlanmasına aktif olarak katılmayı amaçlamaktadır (Slovakya, 2015).

4.27. Slovenya'nın Siber Güvenlik Stratejisi

Slovenya'nın Siber Güvenlik Stratejisi: Üst Düzey Siber Güvenliği Sağlamak İçin Bir Sistem Kurma başlıklı eylem planı 2016 yılında yayınlanmıştır. Slovenya'nın siber güvenlik eylem planı, ülkenin siber güvenlik güvence sistemini iyileştirirken aynı zamanda bu alanı sistematik olarak düzenleyecektir. Tüm toplumun bağlı olduğu sistemlerin sorunsuz işleyişi

için siber güvenliğin giderek artan önemi nedeniyle genel sistemin güçlendirilmesi gereklidir (Slovenya, 2016).

Eylem planı, siber güvenlik güvencesi ile ilgili alanlardaki duruma genel bir bakış, vizyonun ana hatlarını çizme ve hedefler belirlemeden oluşmaktadır. Ayrıca siber uzayda meydana gelen risklerin yanı sıra uygulanacağı alanları da tanımlamaktadır. Eylem planı, siber güvenlik güvence sisteminin nasıl organize edileceğini ve belirlenen hedeflere ulaşmak için gerekli önlemleri önermektedir. Siber güvenlik genellikle şu şekilde tanımlanır (Slovenya, 2016):

- Hem teknik hem de teknik olmayan, bilgisayarları, bilgisayar ağlarını, donanım ve yazılımı ve programlar ve veriler ile diğer siber uzay unsurları da dahil olmak üzere burada depolanan ve işlenen bilgileri tüm tehditlerden korumayı amaçlayan bir dizi faaliyet ve diğer önlemler ulusal güvenliğe yönelik tehditler;
- Bu faaliyetler ve tedbirler tarafından sağlanan koruma seviyesi;
- Bu önlemleri uygulamak ve iyileştirmek ve kalitelerini artırmak için araştırma ve geliştirme dahil ortak profesyonel çabalardır.

Ulusal güvenliğin önemli bir ayrılmaz unsuru olarak kapsamlı bir siber güvenlik sisteminin kurulması, devlet organlarının operasyonları ve yaşamı için önemli olan altyapının sorunsuz işlemesi için temel oluşturacak açık, güvenli ve emniyetli bir siber alanın sağlanmasına katkıda bulunulması hedeflenmektedir. 2020 yılına kadar Slovenya, güvenlik olaylarının sonuçlarını önleyecek ve aynı zamanda ortadan kaldıracak etkili bir siber güvenlik güvence sistemi kuracaktır (Slovenya, 2016).

Modern bir toplumda, hemen hemen tüm sosyal faaliyetler BİT sistemlerine bağlıdır ve daha fazla gelişmeyle bu bağımlılığın artması muhtemeldir. Sistemler arası bağlantı, birinin güvenlik açığının diğerinin işleyişini etkileyebileceği anlamına gelmektedir. Siber saldırılara, suiistimale, dolandırıcılığa, insani ve teknik hatalara ve diğer etkilere karşı tam güvenlik sağlamak imkansız olduğundan, belirli bir tehdidin önceliğini belirlemede kullanılan yaklaşım risk değerlendirmesine dayanmalıdır. Strateji uygulaması, güvenlik olaylarını önlemeye, güvenlik olaylarına müdahale etmeye ve siber güvenliğin önemi konusunda hedef grupların farkındalığını artırmaya odaklanacağı ifade edilmiştir. Aşağıdaki siber güvenlik eylem planı uygulama alanları sunulmuştur (Slovenya, 2016):

- *Önleme:* Güvenlik olaylarının önlenmesi, bilgi sistemi bileşenlerinin teknik tasarımından daha güvenli uygulamaların ve altyapının geliştirilmesine katkıda bulunan ulusal ve uluslararası yasal çerçeve ve düzenlemelere kadar uzanır. Ayrıca, programların ve BİT altyapısının tasarımının, bireylerin mahremiyetinin güvenliğini ve korunmasını içermesi ve şifreleme çözümlerinin kullanımı dahil sistemlerin güvenli ve sorunsuz çalışmasını sağlayan standartlara uyulması sağlanmalıdır.
- *Karşılık Verme:* Tek başına önleme, yüksek düzeyde bir siber güvenlik sağlamak için yetersizdir. Güvenlik olayları hiçbir zaman tam olarak ortadan kaldırılamayacağından, bunlara yanıt verecek uygun mekanizmaların sağlanması gerekir. Ayrıca, önleme aşamasından ve geçmiş güvenlik olayı müdahale olaylarından elde edilen deneyimin hesaba katılması da önemlidir. Deneyimler, siber güvenlik güvencesinden sorumlu yerli ve yabancı kurumlardan gelebilir ve bu nedenle, mümkün olan en iyi bağlantı olanakları çok önemlidir.
- *Farkındalık Yaratma:* İnsanlar, BİT geliştiren, inşa eden ve kullanan kişilerdir. Farkındalık yaratma ve eğitim, riskleri ortadan kaldırmaya ve güvenli teknoloji kullanımı kültürü oluşturmaya yardımcı olabilir. Farkındalık yaratma aşamasında, önleme ve müdahale aşamalarından elde edilen deneyim, kullanıcıların gerçek riskler ve bunlardan kaçınmanın etkili yöntemleri hakkında bilgi sahibi olması için kullanılmalıdır. Siber güvenlik hedeflerine ulaşmak için bir takım önlemler alınacaktır. Gerekirse, stratejinin uygulanması sırasında tedbirler buna göre yükseltilebilir.

Eylem planının ana ve alt hedefleri aşağıdaki gibidir (Slovenya, 2016):

1. <u>Ulusal Siber Güvenlik Güvence Sisteminin Güçlendirilmesi ve Sistematik Düzenlenmesi</u>
   a. Ulusal siber güvenlik güvence sisteminin merkezi bir koordinasyonunun kurulması;
   b. Bilgisayar acil müdahale ekibi uygulanmasıyla birlikte siber güvenlik güvence sisteminin işleyiş düzeyinde insan kaynakları ve organların teknolojik olarak güçlendirilmesi;
   c. Siber güvenlik ve ulusal tatbikatların organizasyonu ile ilgili uluslararası tatbikatlara düzenli katılım;
   d. Devlet organlarının sanal özel (Virtual Private Network/VPN) ağlarının, güvenli ve kullanıma uygun olduğu Sloven makamları tarafından uygun şekilde onaylanan ekipmanla kademeli olarak yükseltilmesi;

e. Mevcut ve yeni kurulan kurumlarda BİT ekipmanının yetkin güvenlik ve işlevsellik kontrollerinin uygulanması.

2. Vatandaşların Siber Uzayda Güvenliğinin Sağlanması
   a. Siber güvenlik konusunda bilinçlendirme programlarının düzenli olarak uygulanması;
   b. Eğitim ve öğretim programlarında siber güvenlik içeriğinin tanıtılması;
   c. Ekonomide siber güvenlik uygulamalarının geliştirilmesi;
   d. Siber güvenlik alanında yeni teknolojilerin geliştirilmesi ve kullanılmasının teşvik edilmesi;
   e. İşletmeler için siber güvenlik konusunda bilinçlendirme programlarının düzenli olarak uygulanması.
3. Kritik Altyapıların Güvenliğinin Sağlanması
   a. BİT destek sektörünün kritik altyapısının işleyişine yönelik risklerin düzenli olarak değerlendirilmesi, uygun koruma önlemlerinin planlanması ve bu alandaki risk değerlendirmesinin güncellenmesi.
4. Kamu Güvenliğini Sağlamak ve Siber Suçlarla Mücadele Etmek İçin Siber Güvenlik Güvencesinin Sağlanması
   a. Polisin BİT sistemlerini korumak için uygun siber kapasitelerin uygulanması;
   b. Kamu güvenliği için siber kapasitelerin geliştirilmesine ve siber suçla mücadeleye katılan kolluk kuvvetlerine yönelik düzenli siber güvenlik eğitimi;
   c. BİT'in gelişmesine paralel olarak kanunların ve prosedürlerin düzenli olarak güncellenmesi.
5. Savunma Siber Yeteneklerinin Geliştirilmesi
   a. Savunma BİT sistemlerini korumak için uygun siber yeteneklerin geliştirilmesi.
6. Büyük Doğal Afetler ve Diğer Felaketler Durumunda Kilit Bit Sistemlerinin Güvenli İşletiminin ile Kullanılabilirliğinin Sağlanması
   a. Büyük doğal afetler ve diğer felaketler durumunda kilit BİT sistemlerinin sorunsuz çalışması için koşulların sağlanması.
7. Uluslararası İşbirliği Yoluyla Ulusal Siber Güvenliğin Güçlendirilmesi
   a. Sloven uzmanların siber güvenlik alanındaki ilgili uluslararası çalışma organlarına ve derneklere katılımı için koşulların sağlanması.

Stratejinin uygulanmasındaki en büyük risk, düşük genel güvenlik kültürü ile el ele giden siber güvenlik güvencesinin önemi konusunda yetersiz farkındalık ve bu alanın ulusal düzeyde sistemik düzenlemesi için siyasi irade ve fikir birliğinin olmamasıdır. Siber

güvenlik güvencesi gibi böylesine önemli bir alanın sistematik olmayan bir şekilde geliştirilmesi, devlet için çok zararlı sonuçlar doğuracaktır (Slovenya, 2016).

Stratejinin başarılı bir şekilde uygulanması, tam tersine, artan güvenlik seviyesi ile ilişkili olumlu çarpımsal etkilerle birlikte, ulusal güvenliğin güvencesi üzerinde olumlu bir etkiye sahip olacaktır. Ayrıca, kullanıcıların internete olan güveninin artmasında ve dolayısıyla kullanımıyla ilişkili yeni hizmetlerin ve iş modellerinin geliştirilmesinde etkisi olacak ve bu, dijital ekonomik büyümeye ve daha fazla sosyal refaha yansıyacaktır. Ülkenin SWOT (güçlü (strengths) ve zayıf (weaknesses) yönler ile çevresel fırsat (opportunities) ve tehditleri (threats)) analizi aşağıdaki gibidir (Slovenya, 2016):

Güçlü Yönler

- Operasyonel siber güvenlik güvencesi seviyesi oluşturulmuştur.
- Sistemin operasyonel seviyesinde yetersiz insan kaynağı olmasına rağmen kaliteli insan kaynağına sahiptir.
- Şimdiye kadar uygulanan önleyici tedbirlerin (bilinçlendirme programları) iyi sonuçlar elde edilmiştir.
- Ortak uluslararası tatbikatlara katılım sağlanmıştır.

Zayıflıklar

- Stratejik düzeyde siber güvenlik güvencesi oluşturulmamıştır.
- Kaynak eksikliği (mali, insani, maddi ve teknik) vardır.
- Kilit paydaşlar arasında yetersiz işbirliği vardır.
- Alanın düzenleyici bir çerçevesi yoktur.

Fırsatlar

- Kullanıcıların (işletmeler, devlet idareleri, bireyler) internet kullanımına olan güveninin artması, internetin kullanımını arttırır, işletme maliyetlerini düşürür ve sonuç olarak dijital büyümeye izin verir.
- Mevcut kabiliyetlerin entegrasyonu ve sinerjilerin kullanılması yeni fırsatlar doğurur.

Tehditler

- Bölgenin önemi ve buna bağlı olarak siyasi irade eksikliği ve ulusal düzeyde hızlı ve etkili eylem ve sistemik düzenleme için fikir birliği eksikliği konusunda yetersiz farkındalık vardır.

- Sistem güçlendirilmezse güvenlik olaylarında artış olması durumunda sistem arızası olasılığı mevcuttur.

4.28. Bulgaristan'ın Ulusal Siber Güvenlik Stratejisi

Ülke 2020 yılı Ulusal Siber Güvenlik Stratejisini hazırlamış ve yayınlamıştır. Küresel internet ailesinin bir parçası olan Bulgar toplumunun, dijital ve bilgi çağında yoğun ve kendinden emin bir şekilde geliştiği ifade edilmiştir. Devlet, iş dünyası ve vatandaşlar, iletişim ve bilgi sistemlerinin, teknolojinin ve internet ortamının güvenilir işleyişine veya halihazırda yaşanan ve gelişen siber uzaya dayanmaktadır. Siber güvenlik eylem planı, dokuz temel alanda kalkınma hedeflerini ve önlemlerini tanımlamaktadır (Bulgaristan, 2020):

1. Ulusal siber güvenlik ve korunma sisteminin kurulması ve geliştirilmesi,
2. Siber dayanıklılığın temeli olan ağ ve bilgi güvenliğinin kurulması,
3. Dijital olarak bağımlı kritik altyapıların korunması ve esnekliğinin sağlanması,
4. Devlet, iş dünyası ve toplum arasındaki etkileşimi ve bilgi paylaşımını iyileştirmek,
5. Düzenleyici çerçevenin geliştirilmesi ve iyileştirilmesi,
6. Siber suçla mücadelenin güçlendirilmesi,
7. Siber savunma ve ulusal güvenliğin korunması,
8. Farkındalık, bilgi ve yetkinliklerin artırılması ve siber güvenlik araştırmaları ile inovasyon için teşvik edici bir ortam geliştirilmesi ve
9. Siber diplomasi ve operasyonel etkileşim çerçevesinde uluslararası ilişkilerin geliştirilmesidir.

Hedeflerin ve belirlenen önlemlerin uygulanması için Siber Güvenlik Yol Haritası Planı da geliştirilecektir. Hedeflere başarılı ve hızlı bir şekilde ulaşmanın ana faktörleri ise aşağıdaki gibi belirlenmiştir (Bulgaristan, 2020):

- Bulgaristan Cumhuriyeti Sürdürülebilir Kalkınma için Hükümet Programının (2014-2018) öncelikleri ve hedeflerine ve ulusal sektörel stratejilere bağlı hareket edecektir;
- Tüm paydaşların belirlenmesi ve katılımının sağlanması ile stratejik, politik, operasyonel ve teknik seviyelerde koordinasyon için bir model ve mekanizma kurulacaktır;

- Belirlenen önlemlerin uygulanması, elde edilen sonuçların ve kabiliyetlerin net bir şekilde değerlendirilmesi için etkili proje yönetimi geliştirilecektir;
- Aktif uluslararası işbirliği (AB ve NATO'daki önde gelen ortakların deneyimlerini kullanmak, ortaklık programlarına ve girişimlerine aktif katılım ve ortak kapasite ve yetenekler oluşturmak için bölgedeki ortaklıkların yoğunlaştırılması) yapılacaktır.

Bulgaristan, planın uygulanmasının izlenmesi, ulaşılan hedeflerin açıklanması, stratejinin güncellenmesi veya yenilenmesi, siyasi, stratejik ve operasyonel-teknik düzeyde kurulan koordinasyon sistemi yardımıyla yürütülecektir. Ancak Bulgaristan, artan dijital bağımlılık, karmaşık hale gelen sistemler ve siber uzaydaki tehditleri tahmin etmesi giderek zorlaşan küresel sürecin bir parçası olarak bir takım risklerle karşı karşıya olduğunu kabul etmektedir. Bulgaristan Cumhuriyeti, Avrupa Birliği ve NATO'nun stratejileri ve politikalarına uygun olarak birleşik bir ulusal siber güvenlik politikası izleyeceğini açıklamıştır. Eylem planının aşamaları ve hedefleri aşağıda sunulmuştur (Bulgaristan, 2020):

1. *Aşama (Başlangıç): Siber Güvenlik İle İlgili Kurumlar:* Ulusal siber güvenlik stratejisi ve eylem planının öncelikleri üzerinde bir yol haritası oluşturulacaktır. Bu amaçtan yola çıkılarak kurumlar arasında, koordineli bir yaklaşım oluşturmak, ulusal bir siber güvenlik sistemi için ortak bir çerçeve meydana koymak, temel yapıları ve temel kapasiteyi tanımlamak, kalkınma için süreçleri ve ilkeleri belirlemek, kilit paydaşlarla istişare halinde siber güvenlik politikasını oluşturmak hedeflenmektedir.
2. *Aşama (Geliştirme - Kapasiteden Yeteneklere): Siber Sürdürülebilir Kurumlar ve "Siber Güvenli" Bir Toplum Oluşturmak:* Sürdürülebilirliğin bireysel kuruluşlar düzeyinde uygulanması için aşama 1'de belirlenen ve tesis edilen kapasitenin siber olaylara ve krizlere koordineli yanıt verme yeteneklerinin, sistematik önleme faaliyetlerinin düzenlenmesi sağlanacaktır.
3. *Aşama (Olgunluk): Siber Sürdürülebilir Bir Toplum Meydana Getirmek:* Ulusal ve uluslararası (AB ve NATO) kurumlarla operasyonel ve stratejik düzeyde etkili iletişim kurulacaktır.

Stratejinin hedeflerine başarılı ve hızlı bir şekilde ulaşılması için Eylem Planında belirlenen ana faktörler aşağıdaki gibidir (Bulgaristan, 2020):

- Bulgaristan, ulusal sektörel stratejilerin önceliklerine ve hedeflerine bağlılık kalarak siber uzay ve dijital ortam güvenliğinin sağlanması esas olarak belirlemiştir.
- Tüm kilit paydaşları belirlemek, sürece dahil etmek (aşamalı faaliyetlerin rollerini, sorumluluklarını açıkça tanımlamak ve öncelikleri üzerinde anlaşmaya varmak) ve bu ilkeyi tüm düzenleyici ve denetleyici çerçevelerde uygulamak ana amaçtır.
- Belirlenen önlemlerin uygulanması, elde edilen sonuçların ve kabiliyetlerin net bir şekilde değerlendirilmesi için etkin proje yönetiminin başlatılması gerekmektedir.
- Etkili uluslararası işbirliği, ulusal ve uluslararası proje ve programların etkili bir şekilde birbirine bağlanması için hayatidir.

Bu eylem planında belirlenen hedeflere ulaşmak ve amaçlanan önlemleri uygulamak için aşağıdaki temel ilkeler takip edilecektir (Bulgaristan, 2020):

- Siber güvenliğin ulusal güvenlikten ayrılmazlığı;
- Vatandaşların temel haklarının, ifade özgürlüğünün, kişisel verilerinin ve kişisel yaşamının korunması;
- Orantılılık;
- Paylaşılan;
- Siber tehdit ve risklerin durumunun periyodik olarak değerlendirilmesi, standartlaştırılmış yöntemlere risklerin sınıflandırılmasına dayalı olarak siber güvenlik seviyesinin ve ilgili yeteneklerin değerlendirilmesi, strateji ve önlemlerin yeterli şekilde güncellenmesi;
- Siber güvenlik ve dayanıklılık politikalarının formülasyonunda ve uygulanmasında şeffaflık;
- Tüm paydaşların katılımı ve kamu-özel sektör ortaklıkları için etkili ve verimli mekanizmalarının geliştirilmesi;
- Uluslararası taahhütler, işbirliği ve etkileşim ilkeleri ile tutarlılık, siber uzayın korunması için ortak kapasite ve yetenekler oluşturulmasına aktif katılım;
- Hedefleri ve önlemleri, sürekli olarak iyileştirilen ve geliştirilen belirli bir eylem planına, sorumluluklara ve göstergelere bağlamak.

Eylem planında belirlenen ana hedef ve alt hedefler aşağıdaki gibidir (Bulgaristan, 2020):

Eylem 1- Ulusal Siber Güvenlik Sisteminin Kurulması ve Geliştirilmesi

- *Ana hedef: Etkili ve verimli bir siber güvenlik sistemi kurmak:*
  a. *Hedef 1:* Siber güvenlik için gerekli kapasite ve yetenekleri geliştirmek için politik ve stratejik düzeyde koordineli eylem mekanizması oluşturmak.
  b. *Hedef 2:* Güncel bir siber durumu ortaya çıkarmak ve siber uzaydaki durumun anlaşılmasını sağlamak.
  c. *Hedef 3:* Etkili ve koordineli önleme, müdahale ve kurtarma için etkileşim mekanizması kurmak.
- *Ana hedef: Siber dayanıklılığın temeli olarak ağ ve bilgi güvenliğini sağlamak:*
  a. *Hedef 1:* Ana amaç, siber uzayın tüm segmentlerinde yüksek bir bilgi ve iletişim teknoloji düzeyine ulaşmak, ulusal ve özel ağların bilgi sistemlerinin güvenliğini artırarak her düzeyde bilgi güvenliğini sağlamaktır.
  b. *Hedef 2:* Genel olarak yüksek düzeyde ağ ve bilgi güvenliği sağlamak.
  c. *Hedef 3:* Devlet kurumlarının, idarenin ve e-devletin iletişim ve bilgi sistemlerinin güvenliği ve sürdürülebilirliğini sağlamak.
  d. *Hedef 4:* Özel sektörün iletişim ve bilgi sistemlerinin iyileştirilmesine dahil edilmesi.
  e. *Hedef 5:* Siber güvenlikten siber dayanıklılığa geçişi tamamlamak.
- *Ana hedef: Dijital olarak bağımlı kritik altyapıların korunması ve esnekliğini sağlamak.*
  a. *Hedef 1:* Temel işlevlerin güvenilir ve sorunsuz bir şekilde gerçekleştirilmesini sağlamak için iletişim ve bilgi sistemleri ile kritik altyapı yönetim sistemlerinin korunmasını ve esnekliğini geliştirmek.
  b. *Hedef 2:* Devlet ile kritik altyapı operatörleri arasındaki etkileşimin iyileştirilmesi sağlanacak.
  c. *Hedef 3:* Kritik altyapı yönetimi ve koruma sistemlerinin geliştirilmesi ve modernizasyonu sağlanacak.
  d. *Hedef 4:* Yeni siber uzay alanlarının zamanında korunması sağlanacak.
- *Ana hedef: Devlet, iş dünyası ve toplum arasındaki etkileşimin ve bilgi paylaşımının iyileştirilmesi sağlanacaktır.*
  a. *Hedef 1:* Açık ve güvenli siber alana ulaşmak için tüm paydaş grupları arasında bilgi paylaşımı ve etkileşim geliştirilecektir.

b. *Hedef 2:* Tüm paydaşların bilgi paylaşımı ve katılımı için etkili mekanizmalar oluşturulacaktır.
c. *Hedef 3:* Endüstriyel teknolojik kapasite ve paylaşılan yeteneklerin geliştirilmesi sağlanacaktır.
d. *Hedef 4:* Küçük ve orta ölçekli işletmelere odaklanılacaktır.
e. *Hedef 5:* Siber etkiler ve karşı önlemler konusunda farkındalık için ortak bir iletişim stratejisi oluşturulacaktır.
f. *Hedef 6:* Güvenli, ücretsiz ve güvenilir internet ortamı kurulacaktır.

- *Ana hedef: Düzenleyici çerçevenin geliştirilmesi ve iyileştirilmesi sağlanacaktır.*
  a. *Hedef 1:* Toplu siber savunmanın tam gelişimi ve taahhütlerin uygulanması için uluslararası kuruluşların ve ortaklıkların yasal çerçevesiyle uyumlaştırma sağlanacaktır.
  b. *Hedef 2:* Yasal ve düzenleyici çerçevenin modernizasyonu sağlanacaktır.
  c. *Hedef 3:* Düzenleme, özdenetim ve sertifikasyon için etkili bir mekanizma oluşturulacaktır.
- *Ana hedef: Siber suçla mücadelenin güçlendirilmesi sağlanacaktır.*
  a. *Hedef 1:* Etkili ve verimli bir önleme, koruma, müdahale, soruşturma ve yeterli kanuni yaptırım süreci oluşturulacaktır.
  b. *Hedef 2:* Yetkili makamların siber uzayda suç faaliyetlerini tespit etme, araştırma ve yaptırım yapma kapasitesini artırılacaktır.
  c. *Hedef 3:* Siber suçun önlenmesi için çalışılacaktır.
  d. *Hedef 4:* Yetkili yapıların idari, organizasyonel ve teknik kapasite ile yeteneklerinin artırılması sağlanacaktır.
- *Ana hedef: Siber savunma ve ulusal güvenliğin korunması için çalışmalar yürütülecektir.*
  a. *Hedef 1:* Devletin ve toplumun güvenliğini ve istikrarlı işleyişini ve gelişimini tehdit eden çeşitli saldırı türlerinin ve yıkıcı nitelikteki organize eylemlerin ve ayrıca ortak ülkelerin karşılıklı anlaşmalar ve taahhütler yoluyla korunması ve karşı eylemine yönelik çalışmalar yürütülecektir.
  b. *Hedef 2:* Siber savunma ve siber silahlı kuvvetler yapıları oluşturulacaktır.
  c. *Hedef 3:* Hibrit tehditlerle ve siber terörizmle mücadele edilecektir.
  d. *Hedef 4:* Siber istihbarat kapasitesi geliştirilecektir.

- *Ana hedef: Farkındalık çalışmaları, bilgi ve yetkinliklerin artırılması ve siber güvenlik araştırmaları ile inovasyon için teşvik edici bir ortam geliştirilmesi sağlanacaktır.*
  a. *Hedef 1:* Tüm hedef gruplar ve paydaşlar için yüksek farkındalığın sağlanması, artan küresel dijital bağımlılıkla ilgili tehditlerin eşit şekilde anlaşılması, değerlendirilmesi ve bilgi ve siber güvenliğe ulaşmak için her düzeyde yeterli önlemlere ihtiyaç duyulması ile ortak bir siber kültürün geliştirilmesi çalışmaları yürütülecektir.
  b. *Hedef 2:* Siber güvenlik araçlarının kullanılması ve dijital çağda ekonominin, toplumun ve hükümetin güvenli ve sürdürülebilir gelişimi için tüm eğitim ve öğretim düzeylerinde çalışmalar yapılacaktır.
  c. *Hedef 3:* Araştırma ve yenilikçi uygulamaların geliştirilmesi için idari kurumların önde gelen bir merkeze dönüştürülmesi için uygun bir ortam yaratılacaktır.
- *Ana hedef: Uluslararası etkileşim geliştirilecektir.*
  a. *Hedef 1:* Bulgaristan, Avrupa ve küresel düzeyde siber güvenlik alanında uluslararası işbirliğinde aktif bir rol oynayacaktır.
  b. *Hedef 2:* Bulgaristan, siber savunma alanındaki NATO taahhütlerini yerine getirmeye devam edecek ve siber savunma alanındaki Mutabakat Muhtırasının ve Galler'deki İttifak Zirvesi sırasında onaylanan İşbirliği Girişimi'nin uygulanmasına aktif olarak katılacaktır. siber savunma endüstrisi ile.
  c. *Hedef 3:* Bulgaristan'ın AB taahhütleri, Avrupa Siber Güvenlik Stratejisi ve Avrupa Siber Savunma Politikası Çerçevesi gibi temel belgelerde belirlenen önceliklerle bağlantılıdır. Ana amaç, garantili maksimum güvenli İnternet erişimi oluşturmaktır. Ulusal yetenekleri geliştirmek ve siber tehditlerle mücadele etmek için Bulgaristan, siber güvenlik konuları (Avrupa Ağ ve Bilgi Güvenliği Ajansı, Europol, Avrupa Savunma Ajansı) ile ilgilenen AB organlarıyla aktif olarak işbirliği yapmalı ve bölgesel ve ikili işbirliği ve etkileşim.
  d. *Hedef 4:* Siber diplomasi kapasitesi geliştirilecektir.
  e. *Hedef 5:* Operasyonel ve teknik düzeyde tatbikatlar yapılacaktır.

Bulgaristan Siber Sürdürülebilir Eylem Planı, 2020 yılına kadar ana faaliyet alanlarının, önlemlerin ve kalkınma aşamalarının belirlenmesine paralel olarak, stratejinin uygulanmasına geçilecektir (Bulgaristan, 2020).

Tüm paydaşları temsil eden kuruluşlar (hükümet, iş ve sanayi, akademik ve araştırma kuruluşları, sivil toplum kuruluşları) planın hazırlanmasında, projelerin ve girişimlerin önceliklendirilmesinde ve yol haritasının tanımlanmasında yer almıştır. Eylem planı, gerekli referanslar ve açıklamalarla birlikte tüm AB ve NATO Ortak ülkelerinin yanı sıra diğer ülke ve kuruluşlara siber güvenlik alanındaki ikili anlaşmalar ve ilişkiler (AGİT, BM, ITU, bölge ülkeleri ve vb.) için kullanılacaktır (Bulgaristan, 2020).

4.29. Romanya'nın Siber Güvenlik Eylem Planı

Romanya'nın Siber Güvenlik Stratejisi 2015 yılında yayımlanmıştır. Eylem planı altı ana bölümden oluşmakta olup kısmen detaya girilmeden hazırlanmıştır. Eylem planının başlangıcında bir takım değerlendirmeler ve tespitlerde bulunulmuştur. Bilgi Toplumunun geliştirilmesi için olmazsa olmaz bir koşul olan modern bilgi ve iletişim teknolojilerinin hızlı gelişimi, sosyal çevre üzerinde büyük bir etkiye sahip olmuştur ve bu etki ekonomi, politika ve kültürün işletme felsefesinde gerçek bir dönüşüme neden olmuştur. Siber uzay, sınırların, dinamizmin ve anonimliğin yokluğu ile karakterize edilmektedir ve hem bilgiye dayalı bilgi toplumu geliştirmek için eşit fırsatlar hem de işlevselliği (bireyde, devlette ve hatta sınır ötesi) için riskler üretmektedir. Modern toplumda bilgisayarlaştırmanın sunduğu inkar edilemez faydaların yanı sıra, aynı zamanda güvenlik açıkları da ortaya çıkarır, bu nedenle siber uzayın güvenliği, özellikle bu alanda tutarlı politikalar geliştirme ve uygulama sorumluluğunun yoğunlaştığı kurumsal düzeyde tüm paydaşlar için önemli bir sorun olmaktadır (Romanya, 2015).

Romanya, hem birlikte çalışabilirliğe ve belirli bilgi toplumu hizmetlerine dayalı dinamik bir bilgi ortamı hem de vatandaşların temel hak ve özgürlüklerinin ve ulusal güvenlik çıkarlarının uygun bir yasal çerçeve içinde uygulanmasını amaçlamaktadır. Romanya devleti, AB ve NATO girişimlerine uygun olarak ulusal düzeyde siber güvenlik faaliyetlerinin koordinatörü rolünü üstlenmektedir. Siber savunma mekanizmalarının geliştirilmesi için gerekli düzenleyici yaklaşımları uygulayan bu kurumlar için siber güvenlik konusu öncelik haline gelmiştir (Romanya, 2015).

Romanya'nın siber güvenlik stratejisinin amacı, ulusal güvenlik ve iyi hükümet için önemli bir destek oluşturacak, ulusal siber altyapılara dayalı, yüksek derecede esneklik ve güvene sahip güvenli bir sanal ortam tanımlamak ve vatandaşlar, işletmeler ve bir bütün olarak

Romanya toplumunun siber güvenliğini sürdürmektir. Ülkenin siber güvenlik stratejisiyle, siber güvenlik tehditlerini, güvenlik açıklarını ve risklerini anlamak, önlemek ve bunlara karşı koymak ve ülkenin siber uzaydaki çıkarlarını, değerlerini ve ulusal hedeflerini desteklemek için hedefler, ilkeler ve temel eylem yönlerini belirlenmiştir. Romanya'nın siber güvenliğini sağlamak için strateji aşağıdaki hedefleri belirlenmiştir (Romanya, 2015);

- Düzenleyici ve kurumsal çerçeveyi siber uzay tehdit dinamiklerine uyarlamak;
- Kritik altyapıların düzgün işlevselliği açısından ulusal siber altyapılar için güvenlik profilleri ve minimum gereksinimleri oluşturmak ve uygulamak;
- Siber altyapının dayanıklılığını sağlamak;
- Romanya'nın siber güvenliğine yönelik güvenlik açıklarını, riskleri ve tehditleri anlayarak, önleyerek ve bunlarla mücadele ederek güvenliği sağlamak;
- Siber uzayda ulusal çıkarları, değerleri ve hedefi teşvik etme fırsatlarından yararlanmak;
- Siber güvenlik alanında ulusal ve uluslararası düzeyde kamu ve özel sektör arasında işbirliğini teşvik etmek ve geliştirmek;
- Siber uzaydan kaynaklanan güvenlik açıkları, riskler ve tehditler ve bilgi sistemlerinin korunmasını sağlama ihtiyacı konusunda halkı bilinçlendirerek bir güvenlik kültürü geliştirmek;
- Romanya'nın siber uzayın kullanımına ilişkin bir dizi uluslararası güven artırıcı önlemi tanımlamada ve oluşturmada parçası olduğu uluslararası kuruluşların girişimlerine aktif katılım sağlamak.

Siber güvenliğin sağlanması, risk değerlendirmesine, kaynak önceliklendirmesine, risk yönetimi ve uyumluluk uygulamasıyla belirlenen güvenlik önlemlerinin etkinliğini izlemeye, uygulamaya ve aşağıdaki ilkelere uymaya dayalı bir yaklaşım öngörülmüştür (Romanya, 2015):

- *Koordinasyon:* Faaliyetler, her bir kuruluşun görev ve sorumluluklarına uygun olarak siber güvenlik için yakınsak eylem planlarına dayalı olarak üniter olarak yürütülecektir;
- *İşbirliği:* İlgili tüm kuruluşlar (kamu veya özel sektörde) uzay sibernetiğinden gelen tehditlere yeterli bir yanıt sağlamak için ulusal ve uluslararası olarak çalışmaktadır;
- *Verimlilik:* Mevcut kaynakların optimal yönetimini hedefleyen adımlar atılacaktır;

- *Önceliklendirme:* Çabalar ulusal ve Avrupa kritik altyapılarını destekleyen siber altyapının güvenliğini sağlamaya odaklanacaktır;
- *Yaygınlaştırma:* Siber altyapıyı korumak için bilgi, uzmanlık ve en iyi uygulamaların aktarılması sağlanacaktır;
- *Değerlerin korunması:* Siber güvenlik politikaları, siber uzayda artan güvenlik ihtiyacı ile mahremiyetin ve diğer değerlerin ve vatandaşların temel özgürlüklerinin korunması arasında bir denge sağlayacaktır;
- *Hesap verebilirlik:* Siber altyapının tüm sahipleri ve kullanıcıları, altyapılarını güvence altına almak ve diğer kullanıcıları etkilememek için gerekli adımları atılacaktır;
- *Ağların ayrılması:* Sibernetik saldırıların ortaya çıkma olasılığının azaltılması, kritik devlet işlevleri sağlayan siber altyapılar üzerinde özel internet ağı, özel ağlar ve ayrı internet kullanımına odaklanılacaktır.

Siber uzaya yönelik belirli tehditler, keskin asimetri, dinamikler ve küresel bir yapı ile karakterize edilir, bu da etki riskleriyle orantılı önlemlerle tespit edilmesini ve bunlara karşı koyulmasını zorlaştırır. Siber uzaydan gelen tehditler (insani, teknik ve prosedürel nitelikteki güvenlik açıklarından yararlanarak) aşağıdaki gibi özetlenmiştir (Romanya, 2015):

- Kamu işlevlerini veya bilgi toplumu hizmetlerini destekleyen altyapıya yönelik siber saldırılar, kesintisi veya hasarı ulusal güvenlik için tehlike oluşturabilecek;
- Siber altyapılara yetkisiz erişim;
- Bilgisayar verilerinin değiştirilmesi, silinmesi veya bozulması veya bu tür verilere erişimin izinsiz yasadışı kısıtlanması;
- Siber casusluk ve
- Patrimonyal zarara neden olmak, kamusal ve özel şahıs ve işletmeleri taciz etmek ve şantaj yapmak.

Aynı zamanda, modern toplum içinde yeni bir etkileşim alanı haline gelen siber uzay, kendi özgünlüğünün ürettiği bir dizi fırsat sunmaktadır. Böylelikle Romanya'nın siber uzay yoluyla yararlanabileceği aşağıdaki fırsatlar tespit edilmiştir (Romanya, 2015):

- Politikaları desteklemek ve ulusal çıkarları desteklemek;
- İş ortamını geliştirmek ve desteklemek;

- Bilgi toplumu hizmetlerinin geliştirilmesi yoluyla yaşam kalitesinin iyileştirilmesi;
- Yeterli siber yetenek ve araçları temin ederek bilgi çağında ulusal politika kararları için bilgi ve desteği geliştirmek;
- Ulusal güvenlik riskleri ve tehditlerinin erken uyarısı için bilgi ve tahmin kapasitesinin artırılması;
- Ulusal güvenlik hedeflerine ulaşmak için teknik kapasiteyi ve insan kaynakları becerilerini artırmak.

Romanya, bilgiyi, yetenekleri ve karar mekanizmalarını geliştirerek fırsatları değerlendirip siber uzayda normalliği sağlamayı ve riskleri azaltmayı amaçlamaktadır. Bu bağlamda, ana hedefleri aşağıdaki yönlere odaklanacaktır (Romanya, 2015):

1. Siber güvenliğin sağlanması için gerekli kavramsal, organize edici ve eylemsel çerçevenin oluşturulması:
   a. Ulusal bir siber güvenlik sistemi oluşturmak ve işletmek;
   b. Ulusal siber altyapılar için asgari güvenlik gereksinimlerinin oluşturulması ve uygulanması da dahil olmak üzere, sahadaki ulusal yasal çerçevenin tamamlanması ve uyumlu hale getirilmesi;
   c. Tehditler, güvenlik açıkları ve risklerin yanı sıra siber olaylar ve saldırılarla ilgili karşılıklı bilgi alışverişini teşvik etmek de dahil olmak üzere kamu ve özel sektör arasında işbirliğini geliştirmek.
2. Ulusal bir programa dayalı olarak ve aşağıdaki hususları içerecek şekilde siber güvenlik alanında ulusal risk yönetimi ve tepki yeteneklerinin geliştirilmesi:
   a. Yetkili makamlar düzeyinde, tehditleri anlama, önleme ve bunlara karşı koyma ve siber alandan yararlanmayla ilişkili riskleri en aza indirme potansiyelini pekiştirmek;
   b. Siber olaylarla ilgili etkin erken uyarı ve müdahale mekanizmalarının oluşturulması da dahil olmak üzere, siber güvenlik alanında kamu-özel işbirliğini geliştirmek için araçlar sağlamak;
   c. Siber güvenlik alanında araştırma, geliştirme ve yenilik yeteneklerini teşvik etmek;
   d. Siber altyapıların dayanıklılık düzeyini artırmak;
   e. Hem kamu hem de özel sektörde siber güvenlik kuruluşlarının geliştirilmesi.
3. Siber alanda güvenlik kültürünü teşvik etmek ve pekiştirmek:

   a. Siber uzay kullanımına özgü tehditler, güvenlik açıkları ve risklerle ilgili nüfus, kamu yönetimi ve özel sektör düzeyinde bilinçlendirme programlarının geliştirilmesi;
   b. İnternetin ve bilgi işlem ekipmanının güvenli kullanımına ilişkin zorunlu eğitim döngüleri dahilinde eğitim programlarının geliştirilmesi;
   c. Siber güvenlik alanında çalışan kişilere uygun mesleki eğitim ve profesyonel sertifikalar alanının yaygın şekilde tanıtılması;
   d. Kamu ve özel sektör yöneticilerine yönelik mesleki eğitim programlarına siber güvenlikle ilgili unsurların dahil edilmesi.
4. Siber güvenlik konusunda uluslararası işbirliği geliştirin:
   a. Büyük siber saldırılar durumunda müdahale kapasitesini artırmak için uluslararası işbirliği anlaşmalarının imzalanması;
   b. Siber güvenlik alanındaki uluslararası programlara katılım;
   c. Romanya'nın taraf olduğu ulusal siber güvenlik işbirliği formatlarının çıkarlarını desteklemek.

Ulusal siber güvenlik sistemi, akademi ve iş dünyası ile profesyonel, profesyonel işbirliği dahil olmak üzere siber uzay güvenliği için ulusal düzeyde eylemlerin koordinasyonunu sağlamak için alandaki sorumluluk ve yeteneklere sahip kamu kurum ve kuruluşlarını bir araya getiren genel işbirliği çerçevesi geliştirilecektir. Proaktif önlemlerle aşağıdakiler hedeflemektedir (Romanya, 2015):

- Ulusal güvenlik düzenleyicilerinin siber ortamını referans gelişmeler doğrultusunda güncellemek ve uyumlu hale getirmek;
- Politikaların, kavramların, standartların ve güvenlik yönergelerinin uygulanması;
- Siber uzayda tanımlanan paylaşılan tehditler, güvenlik açıkları ve riskler hakkında veri ve bilgi toplamak;
- Siber güvenlik durumundaki gelişmeleri analiz ve tahmin etmek;
- Kamu ve özel sektör arasında, siber altyapı sahipleri ve devlet yetkilileri arasında tehditleri önlemek ve bunlara karşı koymak bir siber saldırının etkilerini en aza indirmek için tedbirler almak;
- Siber uzay kullanımından kaynaklanan riskler konusunda eğitim ve farkındalık yaratma;
- Güvenlikteki diğer ulusal ve uluslararası sorumluluklarla birlikte çalışabilirlik;

- Uzay sibernetiğindeki gelişmelere göre yüksek derecede kendi kendine adaptasyon sağlamak;
- Siber uzayda gizlilik, bütünlük, kullanılabilirlik, özgünlük bilgilerinin sağlanması;
- Siber uzayda kimlik yönetiminin sağlanması;
- Yönetim sonuçları dahil olmak üzere sibernetik güvenlik olaylarının yönetimi için operasyonelleştirme yetenekleri;
- Kültür güvenliğini artırmak için mekanizmalar geliştirilmesi.

Siber güvenlik sorumluluğu, yürütülen operasyonların yasallığını sağlamak için bu alandaki tamamlayıcı çıkarları dikkate alarak tüm paydaşlara aittir. Siber suç ve altyapı koruması kritik birbirine bağlı siber uzay ve karşılıklı güvene dayanmaktadır. Kamu ve özel sektör arasındaki işbirliğinin temel hedefleri aşağıdaki gibidir (Romanya, 2015):

- Tehdit, güvenlik açıkları ve riskler hakkında bilgi alışverişi;
- Erken uyarı yeteneklerinin geliştirilmesi ve siber olaylara ve saldırılara yanıt verilmesi;
- Siber uzay güvenliği konusunda ortak tatbikatlar yapmak;
- Eğitim programları ve araştırmaların geliştirilmesi;
- Emniyet kültürünün geliştirilmesi;
- Büyük siber saldırılar durumunda ortak müdahale.

Siber uzaydaki küresel gelişmelerin dinamizmi ve bilgi toplumunun geliştirilmesi ve büyük ölçekli elektronik hizmetlerin uygulanmasındaki hedefler göz önüne alındığında ayrıntılı bir ulusal program geliştirmek gereklidir (Romanya, 2015).

4.30. Hırvatistan'ın Ulusal Siber Güvenlik Stratejisi

7 Ekim 2015 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren Hırvatistan Cumhuriyeti'nin Ulusal Siber Güvenlik Stratejisi 7 bölümden oluşmakta olup oldukça kapsamlı ve detaylı bir şekilde hazırlanmıştır. Giriş kısmında siber güvenlik, ülkenin durumu ve uluslararası ilişkiler kapsamı incelenmiştir (Hırvatistan, 2015).

Teknolojik gelişme hiçbir yerde iletişim ve bilgi teknolojisi alanından daha dinamik ve kapsamlı olmamıştır. Teknolojik gelişmelerin odak noktası her zaman yeni hizmetlerin ve

ürünlerin hızlı gelişimi ve tanıtımı olmuştur; güvenlikle ilgili yönler genellikle yeni teknolojilerin geniş kabulü üzerinde çok daha az etkiye sahiptir. Modern toplumlar, iletişim ve bilgi teknolojisiyle derinden ilişkilidir. Günümüzde insanlar, kullanımı artan Nesnelerin İnterneti (IoT) trendi dahil olmak üzere metin, görüntü ve ses iletimi için çeşitli teknolojiler kullanarak bağlantı kuruyor. Bu birbirine bağlı sistemlerin veya parçalarının düzgün çalışmasındaki sapmalar artık sadece teknik zorluklar değildir; küresel güvenlik etkisiyle tehlike oluştururlar. Modern toplumlar, topluca "siber güvenlik" adı verilen bir dizi faaliyet ve önlemle bunlara karşı koymaktadır (Hırvatistan, 2015).

"Siber" terimi, 2002 yılında Budapeşte Siber Suç Sözleşmesinin onaylanmasının ardından Hırvat hukuk sistemine girmiştir. Orijinal "sibernetik" (Hırvatça "*kibernetika*") terimi, yirminci yüzyılın ortalarında oluşturulmuştur ve genel olarak biyolojik, teknik, ekonomik ve diğer sistemlerde otomatik kontrol sistemleri ve kontrol süreçleri bilimini ifade eder. Farklı sistemlerdeki kontrol süreçlerine atıfta bulunan sibernetik kavramının daha geniş anlamıyla çok daha yaygın olan terim, geçen yüzyılın ikinci yarısında tanıtılan "*sistem teorisi*" dir (Hırvatistan, 2015).

Siber uzayda güvenliğin önemini toplumun tüm kesimlerinin ortak bir sorumluluğu olarak kabul etmek, bu Stratejinin oluşturulmasına yol açtı. Amacı, siber uzayda güvenli bir toplum oluşturmak amacıyla Hırvatistan'ın siber güvenlik alanındaki yeteneklerini geliştirmek için gerekli faaliyetlerin sistematik ve koordineli bir şekilde uygulanmasını sağlamaktır. Amaç ayrıca bir bütün olarak bilgi toplumunun tam pazar potansiyelinden ve özellikle siber güvenlik ürün ve hizmetlerinden yararlanmaktır (Hırvatistan, 2015).

Bu, siber güvenlik alanındaki ilk kapsamlı Hırvat Stratejisi olduğu için, Stratejinin temel amacı, uygulanmasında örgütsel sorunları tanımak ve bu konunun toplumdaki önemi konusundaki anlayışı genişletmektir (Hırvatistan, 2015).

Eylem planı ile Hırvatistan'ın öncelikli siber güvenlik alanları belirlenmiş ve bunlar öncelikle Stratejinin genel hedefleri ile bağlantılı olarak analiz edilmiştir. Stratejide belirlenen siber güvenlik alanlarının her biri için aynı şekilde özel hedefler tanımlanmıştır. Bu hedeflere yönelik uygulama önlemleri, Stratejinin uygulanmasına yönelik eylem planında daha ayrıntılı olarak ele alınacaktır. Bu yolla, strateji tarafından tanımlanan toplum

sektörleriyle ilgili her bir alanın özelliklerini ve çeşitli siber güvenlik paydaşlarının karşılıklı işbirliği ve koordinasyon biçimlerini de dahil etmek mümkün olmuştur (Hırvatistan, 2015).

Hırvat yargı yetkisi altındaki siber uzay, altyapı ve kullanıcıları (vatandaşlık, kayıt, alan adı, adres) kapsayan siber güvenlik yaklaşımının kapsamlı yapısı içinde yer almaktadır. Bu yapı (Hırvatistan, 2015);

- Daha güvenli bir siber uzay oluşturmak için farklı siber güvenlik alanlarından kaynaklanan faaliyetlerin ve önlemlerin entegrasyonu ve bunların birbirine bağlanması ve tamamlanması;
- Faaliyetlerin ve önlemlerin sürekli ayarlanması ve bunların kaynaklandığı stratejik çerçevenin yeterli periyodik adaptasyonu yoluyla proaktif yaklaşım;
- Gizlilik, bütünlük ve belirli bilgi gruplarının ve tanınmış sosyal değerlerin evrensel kriterlerini uygulayarak dayanıklılığı, güvenilirliği ve uyarlanabilirliği güçlendirmek, mahremiyetin korunması ve bir bütün olarak iş süreçleri;

Siber uzay alanında modern toplumun örgütlenmesinin temeli olarak temel ilkelerin toplumun sanal boyutu olarak uygulanmasını aşağıdaki gibi sınıflandırmak mümkündür (Hırvatistan, 2015):

1. İnsan hak ve özgürlüklerini, özellikle mahremiyet, mülkiyet ve organize bir çağdaş toplumun diğer tüm temel özelliklerini korumak için hukukun uygulanması;
2. Devlet ve özel sektör düzeylerindeki düzenleyici mekanizmaların tüm segmentlerinin sürekli iyileştirilmesi uyumlu bir yasal çerçeve geliştirilmesi;
3. Yetki ikamesi ilkesinin, organizasyondan koordinasyon ve işbirliğine kadar, siber güvenlik için önemli alanlarda çözülen konuya en yakın yetkili makamına siber güvenlik konularında karar vermek ve rapor vermek için sistematik olarak ayrıntılı bir güç devri yoluyla uygulanması, belirli iletişim ve bilgi altyapısına yönelik bilgisayar tehditlerine yanıt vermenin teknik sorunları;
4. Her alandaki koruma düzeyini ve ilgili maliyetleri, bunlara neden olan tehditleri sınırlandırmadaki ilgili risk ve yeteneklerle orantılı olarak artırmak için orantılılık ilkesinin uygulanması.

Stratejinin genel hedefleri ise aşağıdaki gibi sınıflandırılabilir (Hırvatistan, 2015);

1. Uluslararası yükümlülükler ve küresel siber güvenlik eğilimleri ile uyumu akılda tutarak, toplumun yeni siber güvenlik boyutunu dikkate almak için ulusal yasal çerçevenin uygulanmasında ve geliştirilmesinde sistematik yaklaşım;
2. Siber uzayda kullanılan ilgili bilgi gruplarının kullanılabilirliğini, bütünlüğünü ve gizliliğini sağlamak için uygulanması gereken siber uzayın güvenliğini, esnekliğini ve güvenilirliğini artırmaya yönelik faaliyetlerin ve önlemlerin, hem çeşitli elektronik hem de elektronik sağlayıcılar tarafından takip edilmesi ve altyapı hizmetleri ve kullanıcılar tarafından, yani bilgi sistemleri siber alana bağlı olan tüm tüzel kişiler ve kişiler tarafından;
3. Yeterli ve uyumlu veri koruma standartlarının uygulanmasını sağlamak için her paydaşın, özellikle belirli bilgi gruplarıyla ilgili olarak gerekli olduğu, siber uzayda daha yüksek bir genel güvenlik düzeyi sağlamak için gerekli olan daha verimli bir bilgi paylaşım mekanizmasının oluşturulması;
4. Kamu ve ekonomik sektörlerin, tüzel kişiliklerin ve bireylerin özelliklerini birbirinden ayıran ve gerekli eğitim unsurlarının düzenli ve ders dışı okul etkinliklerine dahil edilmesini içeren bir yaklaşımla tüm siber uzay kullanıcılarının güvenlik bilincinin artırılması;
5. Akademik, kamu ve ekonomik sektörleri birbirine bağlayarak hedefli ve uzmanlık kursları aracılığıyla okullarda ve yükseköğretim kurumlarında uyumlu eğitim programlarının geliştirilmesini teşvik etmek;
6. Uygun asgari güvenlik gereksinimlerini tanımlayarak e-hizmetlerde kullanıcı güvenini oluşturarak e-hizmetlerin gelişimini teşvik etmek;
7. Akademik, ekonomik ve kamu sektörlerinin potansiyelini harekete geçirmek ve uyumlu çabaları teşvik etmek için araştırma ve geliştirmeyi teşvik etmek;
8. Küresel ölçekte ticari faaliyetlere başarılı katılım için yetenekleri tanımak ve yaratmak amacıyla, toplumun farklı yetkili ulusal makamları, kurumları ve sektörleri arasında verimli bir bilgi aktarımı ve koordineli bilgi paylaşımını mümkün kılan uluslararası işbirliğine sistematik yaklaşım.

Siber güvenlik paydaşlarının işbirliği biçimlerinin yanı sıra, bu Eylem Planının amaçları açısından toplum sektörlerinin ve anlamlarının tanımlanması sağlamıştır. Strateji tarafından öngörülen siber güvenlik paydaşlarının işbirliği biçimleri şunlardır (Hırvatistan, 2015):

- Kamu sektörü içinde koordinasyon;

- Kamu, akademik ve ekonomik sektörlerin ulusal işbirliği;
- İlgili halkla istişare ve vatandaşları bilgilendirme;
- Siber güvenlik paydaşlarının uluslararası işbirliği.

Eylem planının hedefleri aşağıdaki gibi sistematik bir hale getirilmiştir (Hırvatistan, 2015):

1. Elektronik İletişim ve Bilgi Altyapısı Ve Hizmetleri

   a. *Kamu Elektronik İletişimleri (A):* Kamu elektronik iletişimleri, bir elektronik iletişim ağının sağlanmasını ve/veya bir elektronik iletişim hizmetinin sağlanmasını içermektedir. Hedefler;
      - *Hedef A.1.* Operatörler tarafından ağlarının ve hizmetlerinin güvenliğini sağlamak için alınan teknik ve organizasyonel önlemlerin incelenmesi ve kamu iletişim ağlarının ve/veya hizmetlerinin operatörlerini yüksek düzeyde güvenlik ve kamu iletişiminin kullanılabilirliğini sağlamak amacıyla ağlar ve hizmetleri yönlendirmek.
      - *Hedef A.2.* Elektronik haberleşme alanındaki ulusal düzenleyici otorite ile bilgi güvenliği alanından sorumlu ulusal ve uluslararası otoriteler arasında doğrudan teknik koordinasyon oluşturulması.
      - *Hedef A.3.* Hırvatistan'daki kullanıcılara hizmet sağlamak için, kamuya açık iletişim ağları ve/veya hizmet sağlayıcılarının internet alışverişi için ulusal merkezi kullanmalarını teşvik etmek.
   b. *E-Devlet (B):* E-Devlet, tüm vatandaşlar için siber uzay aracılığıyla hızlı, şeffaf ve güvenli bir hizmet sağlayan Hırvatistan'ın stratejik hedefidir. Hedefler;
      - *Hedef B.1.* Kamu sektörü kurumlarının bilgi sistemlerinin birbirine bağlanmasını ve bunların devlet bilgi altyapısını kullanarak kamusal internete bağlanmasını teşvik etmek.
      - *Hedef B.2.* Kamu sektörü bilgi sistemlerinin güvenlik seviyesinin yükseltilmesi.
      - *Hedef B.3.* e-Devlet hizmet sağlayıcıları ve kimlik bilgileri sağlayıcıları arasında belirli kimlik doğrulama seviyelerinin kullanımı için kriterler oluşturmak
   c. *Elektronik Finansal Hizmetler (C):* Bilgi teknolojisi ve faydaları, finansal hizmetler sağlama alanında da yaygın olarak kullanılmaktadır. Tatmin edici güvenlik seviyelerine ulaşmak, her modern devletin hedefidir ve Hırvatistan Cumhuriyeti'nin elektronik finansal hizmetler alanında siber güvenlikle ilgili temel hedefleri şunlardır:

- *Hedef C.1.* Elektronik finansal hizmetlerin gelişimini teşvik etmek amacıyla siber uzayın güvenliğini, dayanıklılığını ve güvenilirliğini artırmaya yönelik faaliyetler ve önlemler üstlenmek.
- *Hedef C.2.* Elektronik mali hizmet sağlayıcıları, düzenleyici ve denetleyici kurumlar ve diğer ilgili makamlar arasında bilgisayar güvenliği olayları hakkında bilgi paylaşımını geliştirmek.

d. *Kritik İletişim, Bilgi Altyapısı ve Siber Kriz Yönetimi (D):* Kritik Altyapılar Yasası'nın ve alt mevzuatın yürürlüğe girmesi, aşağıdaki amaçlarla belirlenen kritik altyapı sektörlerinde kritik iletişim ve bilgi altyapısında başarılı risk yönetimi için yasal ön koşulları oluşturmuştur:

- *Hedef D.1.* Kritik iletişim ve bilgi altyapısını belirlemek için kriterleri belirlemek.
- *Hedef D.2*. Belirlenmiş kritik iletişim ve bilgi altyapısının sahipleri/operatörleri tarafından uygulanacak bağlayıcı güvenlik önlemlerinin belirlenmesi.
- *Hedef D.3.* Risk yönetimi yoluyla önleme ve korumayı güçlendirmek.

Sektör risk analizi aşağıdakileri içerir:

- ✓ Kritik işlevlerin tanımlanması (prosedürler, bilgiler, ağlar, vb.);
- ✓ Tehditlerin belirlenmesi;
- ✓ Tehditlerin, güvenlik açıklarının ve etkinin değerlendirilmesi;
- ✓ Risklerin analizi ve önceliklendirilmesi;
- ✓ Kabul edilebilir risk ve risk tedavisinin belirlenmesi.

- *Hedef D.4.* Bilgisayar güvenliği olaylarının tedavisinde kamu-özel sektör ortaklığını ve teknik koordinasyonu güçlendirmek.
- *Hedef D.5.* Siber krize neden olabilecek bir tehdide etkin yanıt verme kapasitelerini geliştirmek.

e. *Siber Suç (E):* Bilgisayar suçu veya siber suç, bilgisayar sistemlerini, programlarını ve verilerini içeren, iletişim ve bilgi teknolojilerini kullanarak siber uzayda işlenen ve daha güvenli bir bilgi toplumu elde etmek için tehdit oluşturan suçtur. Hedefler;

- *Hedef E.1.* Uluslararası yükümlülükler dikkate alınarak ulusal mevzuatın sürekli olarak iyileştirilmesi.
- *Hedef E.2.* Etkin bilgi paylaşımı için uluslararası işbirliğini geliştirmek ve teşvik etmek.

- *Hedef E.3*. Özellikle bilgisayar güvenliği olayı durumunda, ulusal düzeyde verimli bilgi alışverişi için iyi kurumlar arası işbirliğini geliştirmek.
- *Hedef E.4.* İnsan kaynaklarının güçlendirilmesi, ilgili devlet kurumlarının yetkinliklerinin ve siber suç alanındaki cezai soruşturmaların araştırılması, yürütülmesi ve ceza davalarının kovuşturulması için teknik yeteneklerinin yeterli geliştirilmesi ve gerekli finansmanın sağlanması.
- *Hedef E.5.* Ekonomik sektörle işbirliğinin teşvik edilmesi ve sürekli geliştirilmesi.

2. Siber Güvenlik Alanlarının İlişkileri

a. *Bilgilerin Korunması (F):* Bir bilgi parçasının yaşam döngüsünde, üretilir üretilmez, belirli bir korunan bilgi grubuna ait olup olmadığını belirlemek ve bu tür bilgileri korumak için uygun önlemleri uygulamak gerekir. Sadece işlerinde kullandıkları bilgilerin gizliliğine ve mahremiyetine dikkat etmekle kalmayıp, aynı zamanda korunan her bilgi işlemcisinin ve korunan bilgilerin her yetkili kullanıcısının sorumluluğundadır. Hedefler;
   - *Hedef F.1.* Ticari sırlar alanındaki ulusal düzenlemelerin iyileştirilmesi.
   - *Hedef F.2.* İlgili yönetmeliklerin uygulanmasında uyumu sağlamak için ulusal ortamda özel korunan bilgi grupları için yetkili makamların sürekli işbirliğini teşvik etmek.
   - *Hedef F.3.* Kritik bilgi kaynakları olan ulusal elektronik kayıtların ve bunların korunmasından sorumlu kuruluşların belirlenmesi için kriterlerin belirlenmesi.
   - *Hedef F.4.* Korunan bilgilerin, korunan bilgilerden, korumalı bilgi işlemcilerinden ve korunan bilgilerin yetkili kullanıcılarından sorumlu kuruluşlar tarafından ele alınma şeklinin iyileştirilmesi.
   - *Hedef F.5.* ISO/IEC 270006 standart setini kullanarak yaklaşımın birleştirilmesi.

b. *Bilgisayar Güvenliği Olaylarının Tedavisinde Teknik Koordinasyon (G):* Teknik koordinasyon, olay öncesi duruma dönmek için kullanılabilirliğin, bilginin gizliliğinin veya bütünlüğünün bozulmasına neden olan bilgisayar güvenliği olaylarının tedavisinde uygulanacak temel işlevlerden biridir. Hedefler;
   - *Hedef G.1.* Bilgisayar güvenliği olayları hakkında bilgi toplamak, analiz etmek ve depolamak için mevcut sistemlerin sürekli iyileştirilmesi ve bu tür olayların hızlı ve etkili bir şekilde ele alınması için gerekli olan diğer bilgilerin güncel olduğundan emin olunması.

- *Hedef G.2.* Uyarılar ve tavsiyeler yayınlayarak güvenliği iyileştirmeye yönelik önlemlerin düzenli olarak uygulanması.
- *Hedef G.3.* Bilgisayar güvenliği olaylarına ilişkin sürekli bilgi paylaşımının yanı sıra belirli siber suç vakalarının çözümünde ilgili bilgi ve uzmanlığın sağlanması.

c. *Uluslararası İşbirliği (H):* Siber uzay ve ilgili teknolojiler ve bilgi, politik, güvenlik, ekonomik ve sosyal boyutlar da dahil olmak üzere toplumun genel gelişiminde artan bir role sahiptir. Aynı güvenlik, hukukun üstünlüğü ilkeleri ve yerleşik hak ve özgürlüklerin teminatlarının, bu insan faaliyeti alanındaki tüm bireylere ve tüzel kişilere de aynı şekilde uygulanmasının ne kadar gerekli olduğu oldukça açıktır. Hedefler:
   - *Hedef H.1.* Üçüncü devletlerle karşılıklı işbirliği de dahil olmak üzere, özellikle AB ve NATO içinde ortak devletlerle dış ve güvenlik politikası alanlarında uluslararası işbirliğinin güçlendirilmesi ve genişletilmesi.
   - *Hedef H.2.* Avrupa Konseyi Siber Suç Sözleşmesinin ve beraberindeki protokollerin uygulanmasının teşvik edilmesi ve iyileştirilmesine vurgu yaparak uluslararası yasal çerçevenin güçlendirilmesi.
   - *Hedef H.3.* Uluslararası derneklerle mevcut ve gelecekteki anlaşmalar çerçevesinde ikili ve çok taraflı işbirliğinin devamı ve geliştirilmesi.
   - *Hedef H.4*. Siber güvenlikte güven oluşturma konseptini teşvik etmek.
   - *Hedef H.5.* Uluslararası sivil ve askeri tatbikatlara ve diğer uzmanlık programlarına katılmak ve bunları organize etmek.
   - *Hedef H.6.* Avrupa kritik altyapıları için risk yönetimi alanında işbirliğinin güçlendirilmesi.

d. *Siber Uzayda Eğitim, Araştırma, Geliştirme ve Güvenlik Bilincini Artırma (I):* Güvenli bir toplum oluşturmak ve bilgi güvenliği ve bilgi toplumunun pazar potansiyelini bir bütün olarak kullanmak için, tüm toplumun siber güvenlik alanındaki yeterlilik düzeyini yükselterek sistematik bir yaklaşım uygulamak gerekir. Hedefler;
   - *Hedef I.1.* İletişim ve bilgi teknolojisi güvenliği alanında insan kaynaklarının geliştirilmesi.
   - *Hedef I.2.* Siber uzayda güvenlik bilincini geliştirmek ve yükseltmek.
   - *Hedef I.3.* Ulusal yeteneklerin geliştirilmesi, araştırılması ve ekonominin canlandırılması.

Stratejinin uygulanmasına yönelik Strateji ve Eylem planının uygulanmasını gözden geçirmek ve iyileştirmek amacıyla, Hırvatistan Cumhuriyeti Hükümeti Ulusal Siber Güvenlik Konseyi (Ulusal Konsey) kurulacak ve bu konsey:

- Stratejinin uygulanmasını sistematik olarak izlemek, koordine etmek ve siber güvenlikle ilgili tüm konuları tartışmak,
- Stratejinin uygulanmasına yönelik Strateji ve Eylem planının uygulanmasını iyileştirmek için önlemler önermek,
- Siber güvenlik alanında ulusal tatbikatların düzenlenmesini önermek,
- Strateji ve Eylem planının uygulanmasıyla ilgili öneriler, görüşler, raporlar ve yönergeler yayınlamak ve
- Yeni gerekliliklere uygun olarak Strateji ve Eylem planında değişiklikler önerilmesi veya yeni bir Strateji ve eylem planlarının benimsenmesi.

Ulusal Konsey, siber kriz yönetimi alanında açıklanan gereksinimlere dayanarak:

- Siber kriz yönetimi için gerekli olan sorunları ele alarak ve daha yüksek verimlilik için önlemler önerecek,
- Operasyonel ve Teknik Siber Güvenlik Koordinasyon Grubu tarafından sunulan güvenlik durumuna ilişkin raporlar hazırlanacak,
- Güvenlik durumu ile ilgili periyodik değerlendirmeler yapılacak,
- Siber kriz eylem planlarını hazırlamak ve
- Operasyonel ve Teknik Siber Güvenlik Koordinasyon Grubu için programlar ve eylem planları hazırlamak ve çalışmaları yönlendirmek.

5. YÖNTEM

Bu bölümde çalışmanın modeli, evreni, örneklemi ve verilerin toplanması konuları incelenecektir.

5.1. Araştırmanın Yöntemi

Araştırmanın yönetimi olarak genel olarak nitel modelden yararlanılmış olup doküman analizi yöntemi kullanılmıştır. Doküman analizi yöntemi, yazılı veya basılı belgelerin içeriğini titizlikle ve sistematik olarak analiz etmek için kullanılan bir nitel araştırma yöntemlerinden bir tanesidir (Wach, 2013). Bu yöntem, başta basılı ve elektronik dokümanlar olmak üzere tüm belgeleri incelemek ve değerlendirmek için kullanılan sistemli bir modeli ifade etmektedir. Nitel araştırmada kullanılan diğer yöntemler gibi doküman analizi de anlam çıkarmak, ilgili konu hakkında bir anlayış oluşturmak, ampirik bilgi geliştirmek için verilerin incelenmesini ve yorumlanmasını hedeflemektedir (Corbin ve Strauss, 2008).

Dokümanlar genel olarak araştırmacının herhangi bir müdahalesi olmadan kaydedilmiş metinleri, evrakları ve resimleri ifade etmektedir. Araştırmalarda kullanılabilecek doküman çeşitleri ise; reklamlar, ajandalar, katılım kayıtları, davetiyeler, toplantı tutanakları, kılavuzlar, notlar, kitap ve broşürler, günlükler, dergiler, program kayıtları, mektuplar, muhtıralar, haritalar, çizelgeler, gazeteler, sanat eserleri, program detayları, radyo TV program senaryoları, örgütsel raporlar, anket verileri, çeşitli kamu kayıtları, not defterleri, fotoğraf albümleri vb. şeklinde sıralanabilir. Bu dokümanlar araştırmalarda kullanılmak üzere çalışmalar için veri sağlamaktadır (Labuschagne, 2003; Balcı, 2016). Doküman, literatürde fiziksel veri olarak da adlandırılmakta ve kişilere, topluluklara ya da kültürlere ilişkin önemli bilgiler içermektedir (Baş ve Akturan, 2017).

Diğer birçok modelde olduğu gibi doküman analizi yönteminde de araştırmacılar genellikle kendilerinden önceki araştırmaları inceler, alan yazını gözden geçirir ve bu bilgileri araştırmalarına dâhil ederler. Bu analitik bir yöntemi ifade etmektedir. Dokümanlar da bulunan verileri bulma, seçme, anlamlandırma ve değerlendirme ve sentezleme bu açıdan hem kendi içinde hem de diğer modeller için önemlidir (Labuschagne, 2003). Doküman analizi çalışmalarında iki tür belge/doküman kullanılmaktadır: Birincil belgeler ve ikincil

belgeler. Birincil belgeler, incelenmesi istenen belirli bir olayı veya davranışı deneyimleyen kişiler tarafından üretilen, onların görgü tanıklarına atıfta bulunan belgelerdir. İkincil belgeler ise, olay yerinde bulunmayan ancak belgeleri derlemek için görgü tanıklarının ifadelerini almış veya bu ifadeleri okumuş kişiler tarafından üretilen belgelerdir (Bailey, 1994).

Bir araştırma yöntemi olarak doküman analizi özellikle nitel model için önemlidir. Tek bir olgu, olay, örgüt veya programı ortaya çıkarmak amacıyla yapılan çalışmalarda da kullanılır (Stake, 1995; Yin, 1994). Raporlar ve iç yazışmalar gibi teknik olmayan alan yazın, vaka çalışmaları için potansiyel ampirik veri kaynağıdır (Mills, Bonner ve Francis, 2006). Ayrıca Merriam'a (1988) göre her türden doküman, araştırmacının konuyu anlamasına, keşfetmesine, anlayış geliştirmesine ve araştırma problemiyle ilgili belirsizliklerin giderilmesine yardımcı olabilir. Burada nitel araştırmanın sağlam veri toplama teknikleri ve araştırma yönteminin önemini belirtmek gerekir. Çalışmanın nasıl tasarlandığı ve yürütüldüğü hakkında ayrıntılı bilgi araştırma raporunda verilmelidir. Doküman analizi çoğunlukla diğer araştırma yöntemlerini tamamlayıcı nitelikte olmasına rağmen, bağımsız bir yöntem olarak da kullanılabilir. Örneğin Kıral ve Çilek (2020) yaptıkları araştırmada devlete ait kurumsal bir doküman olan Milli Eğitim Bakanlığı 2023 Vizyon Belgesi'ni karakter eğitimi bakımından değerlendirmişlerdir. Burada analiz edilen resmi bir belgedir. Bu belge Milli Eğitim Bakanlığı'nın resmi web sitesinden edinilmiş ve diğer veri toplama yöntemleri kullanılmamıştır. Ayrıca doküman analizi, karşılaştırmalı eğitim çalışmalarında da sıkça kullanılan bir yöntemdir. Bektaş ve Zabun (2019) tarafından yapılan karşılaştırmalı bir araştırmada Türkiye ve Fransa arasındaki vatandaşlık eğitiminde değerler karşılaştırılmıştır. Bu çalışmada resmi bir kaynak olan program Talim ve Terbiye Kurulu'nun sayfasından, Fransanınki ise Fransız Resmi Gazetesi'nden edinilmiş ve incelenerek analiz edilmiştir. Diğer bir araştırma türü ise makalelerin, tezlerin, çalışmaların bir takım kriterlere göre değerlendirilmesidir. Buna bir örnek verilecek olunursa Kaya (2019) tarafından yapılan bir araştırmada 1995- 2018 yılları arasındaki Yüksek Öğretim Kurumu Tez Merkezi'ndeki Denetim alanında yazılmış olan 128 doktora tezinin değerlendirilmesi yapılmıştır. Burada tüm tezler konu, yıl, sayfa, araştırma yaklaşımı vb. gibi kriterler açısından analiz edilmiştir. Görüldüğü gibi dokuman analizi hem diğer araştırmalarla hem de tek başına kullanılabilmektedir (Kıral, 2020, 178).

Bu kapsamda, öncelikle literatür taranmış, mevzuat incelenmiş, ülkelerin uygulamaları ve politikaları ele alınmış ve son olarak yayımlanan stratejileri ve eylem planları detaylı olarak analiz edilmiştir.

Özellikle strateji ve eylem planlarına ulaşılması için Türkiye için BTK ile Ulaştırma ve Altyapı Bakanlığının dokümanlarından ve Avrupa Birliği için ENISA yayınlarından yararlanılmıştır. Literatür taraması kapsamında ulusal ve uluslararası makaleler, yüksek lisans ve doktora tezleri, raporlar ve güncel veri temelli yayınlar incelenmiştir.

5.2. Evren ve Örneklem

Araştırmanın evreni çalışmanın yapısı açısından siber güvenlik stratejisi ve eylem planı yayımlamış tüm dünya ülkeleri olup örneklemi ise AB üyesi olan 27 ülke ve İngiltere'den oluşmaktadır. Çalışmanın giriş kısmında açıklandığı gibi siber güvenlik alanı en kapalı ülkeleri dahi içine alan küreselleşmiş bir alandır. Bu açıdan tüm ülkeler benzer amaç ve stratejilere sahip olduğu varsayımından hareket edilmiştir. İngiltere'nin analize dahil edilmesinin temel nedeni daha önce AB üyesi olması ve siber güvenlik alanında oldukça güncel dokümanlara sahip olmasıdır. Bunun yanı sıra incelenen strateji ve eylem planlarının çoğunun İngiltere stratejisi ve eylem planından yararlanmasıdır. Örneklemin AB ülkelerini kapsamasının temel gerekçesi ise ENISA'nın internet sitesinden tüm üye ülkelerin strateji ve eylem planlarına ulaşmanın mümkün olması ve Türkiye'nin AB ile neredeyse her konudaki yakın ilişkisi ve işbirliğidir. Ayrıca, İngiltere ve AB ülkelerinin siber güvenlik alanındaki yatırımları ile gelişmişlik düzeyleri örneklem seçimini doğrudan etkilemiştir.

5.3. Verilerin Toplanması

Çalışmada, makaleler, yüksek lisans ve doktora tezleri, raporlar, veri temelli çalışmalar, internet kaynakları, ülke raporları, stratejileri ve eylem planları dokümanlarından yararlanılmıştır. Özellikle AB ülkelerinin siber güvenlik stratejileri ve eylem planlarının elde edilmesi doğrudan ENISA kaynaklarından yararlanılmıştır. Kıyaslamanın yapılmasında kullanılan kriterler ise siber güvenlik stratejileri ve eylem planlarında yer alan hedeflerden uzman görüşmeleri sonunda elde edilen bilgiler kullanılarak yazar tarafından oluşturulmuştur.

Yöntemin uygulanmasında öncelikle akademik yayınlardan yararlanılmıştır. Ancak daha sistematik bir karşılaştırma yapılması için özellikle AB ve İngiltere'nin son stratejileri ve eylem planları incelenmiştir. Böylece kıyaslamanın sağlıklı olması, ana ve alt amaçlardaki soru kümelerinin nesnel bir şekilde cevaplanması ve özellikle öneriler kısmındaki karşılaştırma sonuçlarından elde edilen verilerin kullanılması sağlanmıştır.

5.4. Uygulama

Uygulama aşamasında öncelikle Türkiye, İngiltere ve AB ülkelerinin siber güvenlik stratejileri ve eylem planları detaylı olarak incelenmiştir. Bu inceleme sonunda stratejileri ve eylem planları için genel bir kavrayışa ulaşılmıştır. Stratejiler ve eylem planları konusunda siber güvenlik alanında çalışan beş uzman rastgele seçilmiş, kişilere genel bir açıklama yapılmış, açık uçlu soru ve yargılarla yapılandırılmamış mülakat yönteminden yararlanılmıştır. Gerçekleştirilen görüşmeler ile mülakatlar sonunda elde edilen uzman görüşleri verileriyle iyi bir eylem planının veya stratejinin sahip olması gereken on bir kriter belirlenmiştir. Genel olarak bu kriterler; siber güvenlik stratejileri ve eylem planlarının sürekliliği, siber güvenliğin sağlanması için yatırım, siber güvenliğin geliştirilmesi için Ar-Ge, altyapıların gelişen teknolojiye uyumlaştırılması, siber güvenlik alanında liderlik, siber uzayda ittifaklar, siber güvenlik alanında insan kaynağının geliştirilmesi, siber güvenlik eğitimleri ile devlet, iş dünyası ve sivil toplum arasında ortaklık kurulması olarak belirlenmiştir. Daha sonra belirlenen kriterlere göre Türkiye, İngiltere ve AB ülkeleri kıyaslanmış ve kriterlere sahip ülkeler "*evet*" sahip olmayan ülkeler "*hayır*" şeklinde etiketlenmiştir. Son olarak Türkiye'nin stratejisi ve eylem planları tüm belirlenen kriterler açısından değerlendirilmiştir. Türkiye'nin gelecek eylem planına yönelik öneriler oluşturulmuş ve sonuç bölümüyle ile çalışma tamamlanmıştır.

5.5. Verilerin Çözümü ve Yorumlanması

Çalışma kapsamında seçilen ülkelerin (Türkiye, İngiltere, Almanya, Fransa, Belçika, İtalya, Lüksemburg, Hollanda, İngiltere, Danimarka, İrlanda, Yunanistan, Portekiz, İspanya, Avusturya, Finlandiya, İsveç, Güney Kıbrıs, Çekya, Estonya, Macaristan, Letonya, Litvanya, Malta, Polonya, Slovakya, Slovenya, Bulgaristan, Romanya ve Hırvatistan) siber güvenlik stratejileri ve eylem planları (Türkiye'nin tüm diğer ülkelerin son stratejilerine ve eylem planlarına odaklanılmıştır) sistematik olarak analiz edilmiş ve bir önceki kısımda

açıklandığı gibi uzman görüşmeleri ile genel uygulama alanına sahip on bir kriter belirlenmiştir. Daha sonra bu kriterler özelinde stratejileri ve eylem planları yeniden sistematik analize tabi tutulmuş ve ülkelerin yayımlanan stratejileri ve eylem planları belgelerinden kriterlerdeki alanların yer alıp almadığı değerlendirmeye tabi tutulmuştur. Bazı ülkeler strateji açıklarken diğerleri eylem planlarını da yayımlamıştır. Son olarak kıyaslama Türkiye özeline çekilerek kriterlerin Türkiye'nin eylem planlarında karşılığa sahip olup olmadığı incelenmiştir. Böylece Türkiye, İngiltere ve AB ülkelerinin eylem planları nitel araştırma modelinden olan doküman analizi yönteminden yararlanılmış, bulgular kısmındaki bilgilere ulaşılmış ve öneriler yapılması için veri üretilmiştir.

6. ARAŞTIRMANIN BULGULARI

Bu bölümde incelenen ülkelerin siber güvenlik stratejileri ve eylem planı ile Türkiye'nin siber güvenlik stratejisi ve eylem planları karşılaştırılacak olup karşılaştırma konu ve başlık temelli yapılacaktır. Karşılaştırma için on iki ana başlık belirlenmiştir. Araştırma bulgularının oluşturulmasında Türkiye'nin tüm strateji ve eylem planlarından yararlanılmış olup AB ve İngiltere'nin yayımlanan son strateji ve eylem planları kullanılmıştır. Böylece genel olarak bulguların 2012-2023 dönemini kapsadığı ifade edilebilir.

6.1. Stratejilerin ve Eylem Planlarının Karşılaştırılması

Türkiye'nin hazırladığı üç adet strateji ve eylem planı ile AB ülkeleri ve İngiltere'nin strateji ve eylem planları karşılaştırılacaktır. Bu bölümden elde edilen veriler ve bilgiler öneriler başlığı altında kullanılacaktır. Stratejileri ve eylem planlarının karşılaştırması on bir ana kriter belirlenmiştir. Bu bölüm içinde oluşturulan on bir alt amacın gerçekleştirilmesi hedeflenmiştir.

6.1.1. Stratejilerin ve eylem planlarının sürekliliği

Türkiye'nin 2013-2014, 2016-2019 ve 2020-2023 dönemi Ulusal Siber Güvenlik Stratejisi ve Eylem Planları çalışmada ayrıntılı olarak incelenmiştir. Bu planların birbirlerini takip etmesiyle Türkiye'nin siber güvenlik eylem planının sürekliliğinin olduğunu söylemek mümkündür. Her ne kadar kopuk 2 yıl ve daha sonra 1 yıl olmasına rağmen dönemin ve ülkenin koşullarına göre kapsamlı ve gelişmeye açık bir eylem planı hazırlanmıştır. Ancak 2020 yılının sonunda açıklanan strateji ve eylem planının 2020 yılını kapsadığı anlaşılmaktadır. Bu durum strateji ve eylem planının ya geç açıklanmasıyla ya da 2020 yılını atlamasıyla açıklanabilir. Ayrıca Siber Güvenlik Kurulu yapısının güncellenmemiş olması bir diğer eleştirilecek noktadır.

Çizelge 6.1. Türkiye ile incelenen ülkelerin stratejileri ve eylem planlarının süreklik açısından karşılaştırılması

Ülkeler	Strateji ve Eylem Planlarının Sürekliliği
Türkiye	Var
Almanya	Var
Fransa	Yok
Belçika	Yok
İtalya	Yok
Lüksemburg	Yok
Hollanda	Yok
İngiltere	Var
Danimarka	Yok
İrlanda	Yok
Yunanistan	Yok
Portekiz	Yok
İspanya	Var
Avusturya	Yok
Finlandiya	Yok
İsveç	Var
Güney Kıbrıs	Yok
Çekya	Var
Estonya	Var
Macaristan	Yok
Letonya	Yok
Litvanya	Yok
Malta	Yok
Polonya	Var
Slovakya	Yok
Slovenya	Yok
Bulgaristan	Yok
Romanya	Yok
Hırvatistan	Yok

Almanya'nın "*2011 Almanya Siber Güvenlik Strateji Belgesi*" ve "*2016 Almanya Siber Güvenlik Strateji Belgesi*" ile stratejisinde sürekliliğinin olduğunu söylemek mümkündür. Bunun yanı sıra stratejisinde herhangi bir son tarih verilmemesine rağmen planların 5 yıllık olduğu göz önüne alınarak hedefler belirlenmiştir. Ancak bazı eylem ve alt eylemlerin sürekli olarak devam edeceği vurgulanmıştır. İngiltere oldukça kapsamlı bir siber güvenlik stratejisi yürütmektedir. Gerek süreklilik gerekse hedeflerin spesifik olarak belirlenmesi hususunda Türkiye dahil tüm ülkelerden daha ileri olduğu ifade edilebilir.

Fransa'nın ulaşılabilen tek strateji 2015 yılında yayımlanmış olup "*Fransız Ulusal Dijital Güvenlik Stratejisi*" başlığını taşımaktadır. Söz konusu planın ardılı veya öncesine rastlanılmadığı için ülkenin politikalarının sürekliliğinin eksik olduğu söylenebilir. Bunun yanı sıra açıklanan planda son tarihler belirlenmediği için hedeflere ne zaman veya nasıl ulaşılacağı eksik kalmıştır. Polonya ise 2017-2022 dönemi ve 2009-2011 dönemlerini kapsayana planlar geliştirmiş olup ayrıca 2013 yılında ayrı bir strateji ve eylem planını kamuoyuna açıklamıştır. Dönemler itibarıyla sürekliliğin sağlandığı Polonya'nın öne çıkan ülkelerden olduğunu söylemek mümkündür. Bunun yanı sıra hedeflerin genel olması ve ayrıntılı olarak belirlenmemesi planın ölçülebilirliğine zarar vermiştir.

2019 yılı İspanya Ulusal Siber Güvenlik Stratejisi, siber güvenlik alanındaki 2017 Ulusal Güvenlik Strateji belgesinin devamıdır. Genel hedefleri, alanın özel hedefini ve bunlara ulaşmak için belirlenen eylem çizgilerini dikkate almaktadır. Yeni strateji daha fazla uluslararası işbirliğine odaklanmış olup gelişen ve karmaşıklaşan siber saldırılara karşı işbirliğinin açık bir kabulünü yansıtmaktadır. Çekya Ulusal Güvenlik Kurumunu 2011 yılında kurmuş olup strateji ve eylem planlarının takip ve hazırlanmasında yetkili kılınmıştır. Estonya, AB ülkeleri içinde siber güvenlik alanında güçlü bir sürekliğe sahiptir. 2008-2013, 2014-2017 ve 2019-2022 dönemleri için siber güvenlik stratejisi ve eylem planı hazırlamıştır.

6.1.2. Kritik altyapı güvenliği için yatırım

Türkiye'de Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na bağlı olarak kurulan Siber Güvenlik Kurulu'nun yetkilerinden bir tanesi kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamaktır. Ancak Ulaştırma ve Altyapı Bakanlığına dönüştürüldükten sonra ve Siber Güvenlik Kurulu üyelerinin belirlenmesi usulü güncellenmediğinden

Kurul'un görevini yerine getiremediğini söylemek mümkündür. Son olarak bu görev Dijital Dönüşüm Ofisi bünyesinde olan Siber Güvenlik Dairesi Başkanlığına verilmiştir. Buna rağmen uzun yıllar ülkemizde kritik altyapıların belirlenmesine yönelik herhangi bir adım atılamamış olup 2020-2023 dönemini kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planında kritik altyapılar belirlenmiştir. Ayrıca Bilgi ve İletişim Güvenliği Rehberi ile kritik altyapılara ve bu altyapıları işleten firma veya kurumlara yönelik ayrıntılı denetim ve geliştirme faaliyetleri tanımlanmıştır.

Çizelge 6.2. Türkiye ile incelenen ülkelerin kritik altyapı güvenliği için yatırım yapılması açısından karşılaştırılması

Ülkeler	**Kritik Altyapı Güvenliği İçin Yatırım**
Türkiye	Var
Almanya	Var
Fransa	Var
Belçika	Var
İtalya	Var
Lüksemburg	Var
Hollanda	Yok
İngiltere	Var
Danimarka	Var
İrlanda	Var
Yunanistan	Var
Portekiz	Yok
İspanya	Var
Avusturya	Var
Finlandiya	Var
İsveç	Var
Güney Kıbrıs	Var
Çekya	Var
Estonya	Var
Macaristan	Var
Letonya	Var
Litvanya	Var
Malta	Yok
Polonya	Var

Çizelge 6.2. (devam) Türkiye ile incelenen ülkelerin kritik altyapı güvenliği için yatırım yapılması açısından karşılaştırılması

Ülkeler	Kritik Altyapı Güvenliği İçin Yatırım
Slovakya	Var
Slovenya	Yok
Bulgaristan	Var
Romanya	Var
Hırvatistan	Var

2019-2023 Stratejik Planında Türkiye'nin kritik altyapı sistemlerinin ve siber güvenliğinin izlenebileceği bir merkeze sahip olması hedefi koyulmuş ve Ulusal Siber Olaylara Müdahale Merkezi 2014 yılında faaliyete geçmiştir. Merkezin bir görevi de Kurumsal SOME ile sektörel bazda olan durumları kritik alt yapı işletmecileri (kamu veya özel sektör) için de gerektiğinde koordinasyona geçmek olarak belirlenmiştir. Medyaya düşen haberlere göre Merkezin sık sık kamu kurumlarına kritik alt yapı tesislerine yönelik kamu kurumlarına danışmanlık ve teknik destek verdiğidir. Ancak söz konusu desteğin çoğunlukla yetersiz kaldığı bilinmektedir. Özellikle kritik alt yapı tesislerinin belirlenmesi ve bunlara özel strateji ve eylem planları oluşturulması gerektiği değerlendirilmektedir. Son olarak 2020-2023 dönemini kapsayan strateji ve eylem planında kritik altyapılar "***elektronik haberleşme***", "***enerji***" "***finans***", "***ulaştırma***", "***su yönetimi***" ve "***kritik kamu hizmetleri***" olarak tanımlanmıştır.

Almanya, strateji ve eylem planının girişinde kritik altyapılara vurgu yaparak konunun önemine dikkat çekmiştir. Bunun yanı sıra ülke kritik altyapıların korumasına ilişkin uygulama planı ve federal yönetim için uygulama planı tarafından oluşturulan yapılar temelinde mevcut tehditlere yönelik önlemlerinin alınacağı ifade ederek sağlam bir zemine oturmuştur. Strateji ve Eylem Planında kritik altyapılar; (a) enerji, (b) BİT ve telekomünikasyon, (c) ulaştırma, (d) sağlık, (e) su tesisleri, (f) gıda, (g) finans ve sigorta sektörü, (h) devlet ve kamu yönetimi ile (i) medya ve kültür olarak belirlenmiştir.

İngiltere, özellikle de kritik ulusal altyapısının siber güvenliğiyle ilgili iyileştirmeleri teşvik etmek ve müdahale etmek için önlemler almayı ana hedeflerinden birisi olarak belirlemiştir. Ayrıca, "*Kritik Ulusal Altyapı ve Diğer Öncelik Sektörlerin Korunması*" alt eylemi ile konunun önemine vurgu yapılmıştır. Fransa ise ilk stratejik hedefini bilgi sistemlerinin

savunulması ve güvenliğinin sağlanması ile kritik altyapılar korunması, büyük siber güvenlik kriziyle mücadele etmektir şeklinde belirleyerek kritik altyapıların korunmasının öncelikli hedef olduğunu vurgulamıştır.

Polonya ana amaçlarından birini kritik altyapı operatörlerinin, dijital servis sağlayıcıların ve siber olaylara yönelik kamu idarelerinin yüksek düzeyde esnekliğini sağlamaya yönelik çerçeve faaliyetlerini tanımlamak olarak belirlenmiştir. Bunun yanı sıra ülke temel ve dijital servislerin ve kritik altyapının güvenliğini arttırmak olarak sağlam bir stratejik hedef oluşturmuştur.

Genel olarak incelenen tüm ülkeler için kritik altyapıların korunması ana hedef olarak belirlendiğini söylemek mümkündür. Örneğin İrlanda ekonomik kurum ve kuruluşlar dahil olmak üzere kritik altyapılarının korunmasını ana hedeflerinden biri olarak belirlemiştir. Bunun yanı sıra Macaristan kritik altyapıların envanterini oluşturmayı amaçlamaktadır.

6.1.3. Siber güvenlik alanında ar-ge çalışmalarının yapılması

Türkiye'nin bütün strateji ve eylem planlarında siber güvenlikte yerli teknolojilerin geliştirilmesi için Ar-Ge faaliyetlerinin teşvik edilmesi ve siber güvenlik konusunda Ar-Ge laboratuvarlarının kurulması hedefleri konuya oldukça ciddi yaklaşıldığının bir göstergesidir. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının hazırlanmasında Ar-Ge koordinasyonu önemli bir konu olarak görülmüş olup siber güvenlikte dışa bağımlılığı azaltmak için Ar-Ge faaliyetlerine önem verilerek yerli ürünlerin geliştirilmesi hedeflenmiştir. 2020-2023 dönemini kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planında ise Ar-Ge, yenilikçilik ve güçlü teknolojik altyapı anlayışı ile siber güvenlikte yerli ve milli ürün ve hizmet kullanımı teşvik edileceği ifade edilmiştir.

Çizelge 6.3. Türkiye ile incelenen ülkelerin siber güvenlik alanında Ar-Ge çalışmaları yürütülmesi açısından karşılaştırılması

Ülkeler	Siber Güvenlik Alanında Ar-Ge Çalışmalarının Yapılması
Türkiye	Var
Almanya	Yok
Fransa	Var
Belçika	Yok

Çizelge 6.3. (devam)Türkiye ile incelenen ülkelerin siber güvenlik alanında Ar-Ge çalışmaları yürütülmesi açısından karşılaştırılması

Ülkeler	Siber Güvenlik Alanında Ar-Ge Çalışmalarının Yapılması
İtalya	Var
Lüksemburg	Var
Hollanda	Var
İngiltere	Var
Danimarka	Var
İrlanda	Var
Yunanistan	Var
Portekiz	Var
İspanya	Var
Avusturya	Var
Finlandiya	Var
İsveç	Var
Güney Kıbrıs	Yok
Çekya	Var
Estonya	Var
Macaristan	Var
Letonya	Var
Litvanya	Var
Malta	Yok
Polonya	Var
Slovakya	Var
Slovenya	Var
Bulgaristan	Var
Romanya	Var
Hırvatistan	Var

Ar-Ge konusuna özel önem veren ülkelerden olan İngiltere strateji ve eylem planında Ar-Ge'ye yapılan yatırımların yükseltilmesini hedeflemiştir. Fransa, Ar-Ge yatırımlarını artırmayı amaçlamıştır.

Genel olarak değerlendirildiğinde tüm ülkelerin siber güvenlik alanına yönelik yatırım yapmayı hedeflediği ancak doğrudan Ar-Ge konularında bir miktar geri kaldığı anlaşılmıştır. Türkiye açısından ise siber güvenlikte dışa bağımlılığı azaltmak ve yerli ürünlerin

geliştirilmesi için Ar-Ge'ye büyük önem atfedilmiştir. Bu durum Ar-Ge çalışmalarının yapılması konusunda ülkemizin diğer ülkelere göre önde olduğunu göstermektedir.

6.1.4. Altyapının gelişen teknolojiye adapte edilmesi

Türkiye 2013- 2014 döneminde gerçekleştirilmesi planlanan ulusal siber güvenlik altyapısının güçlendirilmesi stratejik eylemi ile gelişen teknolojiye adapte edilmesi mevcut altyapının uyumlu hale getirilmesine büyük önem verdiğini göstermiştir. Bunun yanı sıra 2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016-2019 Ulusal Siber Güvenlik Eylem Planıyla ve ve 2020-2023 dönemi Ulusal Siber Güvenlik Stratejisi ve Eylem Planıyla ulusal kritik altyapı envanterinin oluşturulması ve kritik altyapıların güvenlik gereksinimlerinin karşılanması için gelişen teknolojiye uyum sağlaması hedeflenmiştir.

Çizelge 6.4. Türkiye ile incelenen ülkelerin altyapının gelişen teknolojiye adapte edilmesi açısından karşılaştırılması

Ülkeler	Altyapının Gelişen Teknolojiye Adapte Edilmesi
Türkiye	Var
Almanya	Var
Fransa	Var
Belçika	Var
İtalya	Var
Lüksemburg	Var
Hollanda	Var
İngiltere	Var
Danimarka	Var
İrlanda	Var
Yunanistan	Var
Portekiz	Var
İspanya	Var
Avusturya	Yok
Finlandiya	Yok
İsveç	Var
Güney Kıbrıs	Var
Çekya	Var

Çizelge 6.4. (devam) Türkiye ile incelenen ülkelerin altyapının gelişen teknolojiye adapte edilmesi açısından karşılaştırılması

Ülkeler	Altyapının Gelişen Teknolojiye Adapte Edilmesi
Estonya	Var
Macaristan	Var
Letonya	Var
Litvanya	Yok
Malta	Var
Polonya	Var
Slovakya	Yok
Slovenya	Var
Bulgaristan	Var
Romanya	Var
Hırvatistan	Var

Almanya, kullanılan teknolojilerin ve enformatik altyapının geliştirilmesine ayrıntılı önem vermiştir. İngiltere 2021 yılına kadar, siber bilim ve teknolojide bir dünya lideri olmayı hedeflemekte olup siber güvenlik alanında etkili ufuk açıcı araştırmalar yapmayı planlamaktadır. Ayrıca İngiltere hükümeti, gelecekteki teknolojik gelişmelere yönelik olarak politikalar geliştirmeyi amaçlamaktadır.

Fransa, kullanımlara uyarlanan ve belirlenen riskleri hafifletebilecek güvenlik düzeyine sahip teknolojilerin geliştirilmesini hedeflemiştir. Polonya bilgi iletişim teknolojileri güvenliğini geliştirmeyi öncelik olarak belirlemiştir. Ayrıca ülke siber güvenlik amaçlı endüstriyel ve teknolojik kaynakların geliştirilmesini stratejik amaçlarından biri saymıştır.

Diğer incelenen ülkeler mevcut altyapıların gelişen teknolojiye adapte edilmesine yönelik hedef veya faaliyete yer vermiştir. Mevcut altyapının geliştirilmesi için sürekli olarak ülkeler, kurumlar, şirketler yatırım yapmak zorundadır. Her ne kadar bazı ülkeler böyle bir hedefe yer vermemesine rağmen uygulamada neredeyse bütün ülkelerin bu tarz yatırımlar yaptığını söylemek mümkündür. Çünkü sadece güvenlik için değil aynı zamanda kullanıcı dostu gelişmeler için gelişim ve adaptasyon zorunludur.

6.1.5. Gelişen teknolojide liderlik yapmak

Türkiye sektör düzenleyici kurum, bakanlık vb. kuruluşların siber güvenlik kapsamında düzenleme ve denetleme farkındalıklarının ve yetkinliklerinin geliştirilmesi amacıyla sektörde kamu kurum ve kuruluşlarının liderlik yapmasını amaçlamıştır. Bu amaç uzun yıllardır ülkemizde önem verilmeyen siber güvenlik alanının yeni yeni geliştiğini göstermektedir. Yerli ürünlerin geliştirilmesi ile birlikte liderlik rolünün yükseldiğini söylemek mümkündür. Ancak liderlik konusu strateji ve eylem planlarında ayrıntılı ve spesifik olarak ele alınmamıştır. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında Türkiye liderliğinde Uluslararası Siber Güvenlik Tatbikatlarının ilkinin düzenlenmesi hedefine yer verilmesine rağmen genel olarak siber güvenlik alanında liderliğin hedeflenmediği görülmektedir.

Çizelge 6.5. Türkiye ile incelenen ülkelerin gelişen teknolojide liderlik yapma açısından karşılaştırılması

Ülkeler	Gelişen Teknolojide Liderlik Yapmak
Türkiye	Yok
Almanya	Yok
Fransa	Yok
Belçika	Yok
İtalya	Yok
Lüksemburg	Yok
Hollanda	Var
İngiltere	Var
Danimarka	Yok
İrlanda	Yok
Yunanistan	Yok
Portekiz	Yok
İspanya	Yok
Avusturya	Var
Finlandiya	Yok
İsveç	Var
Güney Kıbrıs	Yok
Çekya	Var
Estonya	Var

Çizelge 6.5. (devam) Türkiye ile incelenen ülkelerin gelişen teknolojide liderlik yapma açısından karşılaştırılması

Ülkeler	Gelişen Teknolojide Liderlik Yapmak
Macaristan	Var
Letonya	Yok
Litvanya	Yok
Malta	Yok
Polonya	Yok
Slovakya	Yok
Slovenya	Yok
Bulgaristan	Yok
Romanya	Yok
Hırvatistan	Yok

AB risk yönetiminin geliştirilmesi ile siber güvenlik alanında lider ülke konumunun korunması hedeflenmiştir. Böylece ülke siber güvenlik alanında lider olduğuna ayrıca vurgu yapmıştır. İngiltere ise 2021 yılına kadar, siber bilim ve teknolojide bir dünya lideri olmayı hedeflemektedir. Ancak diğer ülkelerin siber güvenlik alanında liderlik yarışında olmadığını söylemek hata olacaktır.

Çekya, modern bir Orta Avrupa ülkesi olarak AB, NATO, BM ve diğer uluslararası kuruluşların aktif bir üyesi olarak lider bir rol oynamayı amaçlamaktadır. Avusturya, AB güvenlik araştırma programlarında aktif tematik liderliğe ulaşmak için çalışmalar yapmayı hedeflemektedir. İsveç ise AB içindeki dijital liderliğini sürdürmek, dijital tek pazarı tamamlayarak ve gelecekteki konulardaki tartışmalarda itici bir güç olarak dijital gündemi ileriye taşınacak politikalar geliştirmeyi öngörmüştür.

6.1.6. Siber uzayda güçlü ittifak kurmak

Türkiye'nin gerek Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında gerek 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı gerekse 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında siber uzayda ittifak kurulması veya ortak hareket edilmesine yönelik bir amaç veya eylem öngörülmemiştir. Bu durum siber güvenlik alanının önemli bir noktasında hataya neden olmuştur. Küresel veya bölgesel ittifaklar olmadan siber güvenlik politikalarının başarıya ulaşması zordur. Buna rağmen uluslararası işbirliği ve bilgi

paylaşımı için diplomatik, teknik ve kolluk iletişim kanallarının sürekli ve etkin kullanımının esas alınmasının bir noktada ittifak kurulmasına ima olduğu söylenebilir. Ayrıca, kamu, özel sektör, üniversiteler, sivil toplum kuruluşları ve bireyler dâhil tüm paydaşlar arasında işbirliğinin vurgulanması ülke içindeki yakınsamanın bir göstergesidir. Son strateji belgesinde ulusal ve uluslararası düzeydeki paydaşlarla bilgi paylaşımı ve iş birliğini sağlayacak mekanizmaların geliştirilmesi ana hedeflerden biri olarak belirlenmiştir.

Çizelge 6.6. Türkiye ile incelenen ülkelerin siber uzayda güçlü ittifak kurma açısından karşılaştırılması

Ülkeler	**Siber Uzayda Güçlü İttifak Kurmak**
Türkiye	Var
Almanya	Var
Fransa	Var
Belçika	Var
İtalya	Var
Lüksemburg	Var
Hollanda	Var
İngiltere	Var
Danimarka	Var
İrlanda	Var
Yunanistan	Var
Portekiz	Var
İspanya	Var
Avusturya	Var
Finlandiya	Var
İsveç	Var
Güney Kıbrıs	Var
Çekya	Var
Estonya	Var
Macaristan	Var
Letonya	Var
Litvanya	Var
Malta	Var
Polonya	Var
Slovakya	Var
Slovenya	Var

Çizelge 6.6. (devam) Türkiye ile incelenen ülkelerin siber uzayda güçlü ittifak kurma açısından karşılaştırılması

Ülkeler	Siber Uzayda Güçlü İttifak Kurmak
Bulgaristan	Var
Romanya	Var
Hırvatistan	Var

Almanya doğrudan siber güvenlik alanda uluslararası işbirliğini artırmayı amaçladığını vurgulamıştır. İngiltere diğer devletler ile iyi siber güvenlik uygulamaları arasındaki işbirliğini teşvik etmeyi amaçlamıştır. Bu durum ittifaklar kurulmasına vurgu yapılması ile pekiştirilmiştir. Fransa siber güvenlik alanında uluslararası işbirliğinin başarı için kritik olduğunu vurgulamıştır. Fransa, ulusal ve uluslararası düzeylerde özel paydaşlarla işbirliğini genişleterek ittifaklar kurmayı hedeflemiştir. Polonya uluslararası işbirliği yoluyla diğer devletlerle yakından bağlantılı olması gerektiği vurgulamış ve bu ittifakların başarı için önemli olduğunu değerlendirmiştir.

Diğer tüm ülkelerin siber güvenlik alanında işbirliği geliştirmeye yönelik politikalar geliştirdiği görülmektedir. Siber güvenlik geniş uygulama alanına sahip ve çok aktörlü bir yapıya sahiptir. Bu yüzden ittifaklar kurulması, işbirlikleri geliştirilmesi ve bilgi alış verişi yapılması ulusal güvenlik gibi siber güvenlik için de bir zorunluluktur.

6.1.7. Siber güvenlik insan kaynağının geliştirilmesi

Türkiye siber güvenlik uzmanlığına yönlendirme programının yürütülmesi ile siber güvenlik alanında yetkin personel yetiştirilmesi ve bu alanda uzmanlaşmak isteyen personel, araştırmacı ve öğrencilerin teşvik edilmesini ana amaçlar olarak belirlemiştir. Siber güvenlik alanında başarının temel anahtarı yetişmiş insan kaynağıdır. Türkiye bu durumun farkında olup strateji ve eylem planında hedefleri içine koymuştur. Üniversitelerdeki siber güvenlik ile ilişkili bölümlerin çoğalması ise gelişmeler olduğunu göstermektedir. 2020-2023 Stratejisi ve Eylem Planında örgün ve yaygın eğitimde siber güvenlik eğitiminin yaygınlaştırılmasına ve eğitim içeriklerinin zenginleştirilmesine özel önem verilmiştir.

Çizelge 6.7. Türkiye ile incelenen ülkelerin siber güvenlik insan kaynağının geliştirilmesi açısından karşılaştırılması

Ülkeler	Siber Güvenlik İnsan Kaynağının Geliştirilmesi
Türkiye	Var
Almanya	Var
Fransa	Var
Belçika	Var
İtalya	Var
Lüksemburg	Var
Hollanda	Var
İngiltere	Var
Danimarka	Yok
İrlanda	Var
Yunanistan	Var
Portekiz	Var
İspanya	Var
Avusturya	Var
Finlandiya	Var
İsveç	Var
Güney Kıbrıs	Var
Çekya	Var
Estonya	Var
Macaristan	Var
Letonya	Var
Litvanya	Var
Malta	Var
Polonya	Var
Slovakya	Yok
Slovenya	Var
Bulgaristan	Yok
Romanya	Var
Hırvatistan	Var

Almanya federal yetkilileri arasında yoğunlaşmış personel değişiminin ve uygun ileri eğitim önlemleri bakanlıklar arası işbirliğinin artırılması amaçlanmıştır. Böylece insan kaynağını geliştirmeyi ve yetişmiş insan kaynağının dengeli dağıtılmasını hedeflemiştir. İngiltere daha

yetenekli ve nitelikli siber güvenlik uzmanlarına ihtiyaç duyduğunu ifade ederek siber güvenlik becerilerinin güçlendirilmesini ayrı bir stratejik hedef olarak belirlemiştir.

Fransa dünya standartlarında teknik uzmanlar tarafından desteklenen özerk stratejik planlamayı geliştirmeyi hedeflemiştir. Ayrıca, kamu ve özel sektörden siber güvenlik konusundaki artan talepleri karşılamak için, bu alandaki uzmanların eğitiminin artırılacağı vurgulanmıştır. Polonya siber uzayda güvenlik alanındaki ulusal potansiyel ve yetkinliğin arttırılmasını hedefleyerek insan kaynağına yatırım yapılacağı vurgulanmıştır.

İnsan kaynaklarının geliştirilmesi tüm ülkelerin ortak hedeflerindendir. Çekya ana hedeflerinden birini eğitim, bilinçlendirme ve bilgi toplumu geliştirme olarak belirlenmiştir. Slovenya siber güvenlik alanında bir eğitim sisteminin desteklenmesi, formüle edilmesi ve uygulanması şeklinde ana hedef belirlemiştir. Portekiz strateji ve eylem planının ana eksenlerinden bir tanesini önleme, eğitim ve farkındalık yaratma olarak açıklamıştır. Siber güvenliğin sağlanması için insan kaynaklarının kaliteli olması ve uluslararası gelişmeleri takip etmesi zorunludur. Çünkü çok değişken yapısından dolayı siber güvenlik gelişmelerini takip edecek bilgi düzeyinin korunması elzemdir.

6.1.8. Kamu düzeyinde eğitim sağlanması

Türkiye strateji ve eylem planlarında siber güvenlik eğitim altyapısının güçlendirilmesini ve ilk, orta, lise öğretimi ve yaygın eğitimde siber güvenlik eğitimlerinin yaygınlaştırılmasını amaçlamıştır. Ayrıca toplumun her kesiminde siber güvenlik bilincinin oluşturulması için eğitime vurgu yapılmıştır.

Çizelge 6.8. Türkiye ile incelenen ülkelerin kamu düzeyinde eğitim sağlanması açısından karşılaştırılması

Ülkeler	Kamu Düzeyinde Eğitim Sağlanması
Türkiye	Yok
Almanya	Var
Fransa	Var
Belçika	Var
İtalya	Var
Lüksemburg	Var

Çizelge 6.8. (devam) Türkiye ile incelenen ülkelerin kamu düzeyinde eğitim sağlanması açısından karşılaştırılması

Ülkeler	Kamu Düzeyinde Eğitim Sağlanması
Hollanda	Yok
İngiltere	Var
Danimarka	Var
İrlanda	Var
Yunanistan	Yok
Portekiz	Var
İspanya	Var
Avusturya	Var
Finlandiya	Var
İsveç	Var
Güney Kıbrıs	Var
Çekya	Var
Estonya	Var
Macaristan	Var
Letonya	Var
Litvanya	Var
Malta	Var
Polonya	Var
Slovakya	Var
Slovenya	Var
Bulgaristan	Var
Romanya	Var
Hırvatistan	Var

Almanya federal makamlarda personel eğitiminin sağlanması amacıyla uygun ileri eğitim önlemlerinin uygulanmasını amaçlanmıştır. İngiltere siber güvenlik yeteneklerini geliştirmek için eğitim ve öğretim alanına yenilenmiş insan kaynağı gücüne bağlı olduğunu vurgulamıştır. Fransa ise özellikle eğitim konusunda uluslararası işbirliğine vurgu yapmıştır. Ayrıca ülke siber güvenlik alanında başlangıç eğitimi verilecek ve diğer eğitimleri sürekli kılmayı ana strateji olarak belirlemiştir.

Macaristan eğitim, araştırma ve geliştirme hedefine ilk, orta ve yükseköğrenimin bilgi teknolojisi müfredatında, hükümet görevlileri için eğitim kurslarında ve mesleki eğitim

kurslarında eğitim, araştırma ve geliştirme faaliyetleri yürütmesi kapsamında ulaşılması amaçlanmaktadır. Malta ana hedeflerinden birini siber güvenlik farkındalığı oluşturmak ve eğitim faaliyetleri düzenlenmek olarak belirlemiştir. Litvanya ise üçüncü hedefin ikinci amacında, pazarın ihtiyaçlarını karşılayan yaratıcılığı, gelişmiş yetenekleri ve siber güvenlik becerilerini ve yetkinliğini geliştirmek şeklinde oluşturmuştur. Bu açıdan bakıldığında neredeyse tüm ülkelerin eğitim ve farkındalık konularına eğildiğini söylemek mümkündür.

6.1.9. Devlet, iş dünyası ve sivil toplum arasında ortaklık

Türkiye, özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına ayrıca önem vermektedir. Bu durum siber güvenliğin ulusal boyutuna verilen önemin bir göstergesidir. Daha önce kısaca ele alınıldığı gibi özel sektör ile işbirliğinin geliştirilmesi ile siber ortam güvenliğinin sağlanması ve sürdürülmesinde kamu, özel sektör, üniversiteler ve sivil toplum örgütleri işbirliğine vurgu yapılmıştır. Türkiye'de yaygın olarak kullanılan kamu-özel sektör işbirlikleri siber güvenlik alanında devlet, iş dünyası ve sivil toplum arasında ortaklık kurulmasında kullanılacaktır.

Çizelge 6.9. Türkiye ile incelenen ülkelerin dünyası ve sivil toplum arasında ortaklık açısından karşılaştırılması

Ülkeler	Devlet, İş Dünyası ve Sivil Toplum Arasında Ortaklık
Türkiye	Var
Almanya	Var
Fransa	Var
Belçika	Var
İtalya	Var
Lüksemburg	Var
Hollanda	Var
İngiltere	Var
Danimarka	Var
İrlanda	Var
Yunanistan	Var
Portekiz	Var
İspanya	Var
Avusturya	Var

Çizelge 6.9. (devam) Türkiye ile incelenen ülkelerin dünyası ve sivil toplum arasında ortaklık açısından karşılaştırılması

Ülkeler	Devlet, İş Dünyası ve Sivil Toplum Arasında Ortaklık
Finlandiya	Yok
İsveç	Var
Güney Kıbrıs	Var
Çekya	Var
Estonya	Var
Macaristan	Var
Letonya	Var
Litvanya	Var
Malta	Var
Polonya	Var
Slovakya	Var
Slovenya	Yok
Bulgaristan	Var
Romanya	Var
Hırvatistan	Var

Almanya, özellikle kritik altyapıların korunması için kamu ve özel sektörün, yoğunlaştırılmış bilgi paylaşımına dayanarak daha yakın koordinasyon geliştirmesine odaklanmıştır. Bunun yanı sıra ülke Ulusal Siber Güvenlik Konseyi'nde özel sektör ve sivil topluma da yer vermeyi hedeflemiştir. İngiltere, kamu ve özel sektördeki ulusal ihtiyaçlarını karşılama becerisi sağlayan personele sahip olduğunu vurgulayarak kamu ve özel sektör kuruluşlarının ve kurumlarının kendilerini savunmak için doğru bilgilere erişmelerini sağlamak ve aralarındaki ortaklıkları geliştirmek için önlemler alacağını taahhüt etmiştir.

Polonya, kamu sektörü ve özel sektör arasında işbirliği mekanizmaları oluşturmayı ayrı bir stratejik hedef olarak belirlemiştir. Ülke etkili kamu- özel sektör ortaklıkları geliştirmeyi stratejik hedeflerinden biri olarak belirlemiştir. Kamu özel ortaklıkları veya işbirlikleri yeni bir model olarak öne çıkmaktadır. Örneğin Güney Kıbrıs Cumhuriyeti'nde kritik bilgi altyapısının korunması alanında dinamik bir PPP (Kamu-Özel Ortaklığı) oluşturma olasılığını araştırılacak ve uluslararası forumlara katılım yoluyla uluslararası kuruluşlarla aktif işbirliğini teşvik edilecektir. Bulgaristan söz konusu modeli stratejik bir hedef olarak belirlemiştir. Diğer ülkelerde benzer hedef ve önceliklere yer vermiştir.

6.1.10. Siber saldırılara karşı yasal önlemler geliştirilmesi

Türkiye, 2013- 2014 dönemini kapsayan Eylem Planında yasal düzenlemelerin yapılmasını ayrı bir stratejik amaç olarak belirlemiş ve Siber Güvenlik Kurulunun faaliyetlerine başlaması ile siber güvenlik konusunda mevzuat çalışmalarının yapılmasını hedeflemiştir. Siber Güvenlik Kurulu oluşturulmuş ancak yeni hükümet sistemine göre güncellenmemiştir. Yasal düzenlemelere ise peyderpey devam edilmekledir. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında ise siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması ana hedeflerden birisi olarak seçilmiştir. 2020-2023 dönemi Strateji ve Eylem Planında ise mevzuata yönelik herhangi bir hedefe veya faaliyete yer verilmemiştir.

Çizelge 6.10. Türkiye ile incelenen ülkelerin siber saldırılara karşı yasal önlemlerin geliştirilmesi açısından karşılaştırılması

Ülkeler	Siber Saldırılara Karşı Yasal Önlemlerin Geliştirilmesi
Türkiye	Var
Almanya	Var
Fransa	Var
Belçika	Var
İtalya	Var
Lüksemburg	Yok
Hollanda	Var
İngiltere	Var
Danimarka	Var
İrlanda	Var
Yunanistan	Yok
Portekiz	Var
İspanya	Var
Avusturya	Var
Finlandiya	Yok
İsveç	Var
Güney Kıbrıs	Var
Çekya	Var
Estonya	Var
Macaristan	Yok

Çizelge 6.10. (devam) Türkiye ile incelenen ülkelerin siber saldırılara karşı yasal önlemlerin geliştirilmesi açısından karşılaştırılması

Ülkeler	Siber Saldırılara Karşı Yasal Önlemlerin Geliştirilmesi
Letonya	Var
Litvanya	Var
Malta	Var
Polonya	Var
Slovakya	Var
Slovenya	Yok
Bulgaristan	Var
Romanya	Yok
Hırvatistan	Var

Almanya, federal düzeyde veya bölge düzeyinde ek yasal düzenlemelerin oluşturulacağını vurgulamıştır. İngiltere, internet ve telekomünikasyon trafiğini, kötü niyetli aktörlere karşı korumak için yasaların sağlamlaştırılmasını amaçlamıştır. Fransa, siber zorbalık mağdurlarına yardım edeceğini taahhüt etmiş ve söz konusu durumu yasal zemine oturtmayı planlamıştır. Polonya, BT sistemlerini yasal düzenlemelere bağlanmıştır. Ayrıca, yasal çevrenin siber güvenlik alanındaki ihtiyaç ve zorluklara uyarlanması hedeflenmiştir.

Yasal altyapının geliştirilmesi ülkelerin ortak hedefleri arasındadır. Çünkü yasal altyapının kurulması hem caydırıcılık hem de hareket alanının belirlenmesi için önemlidir. Ayrıca yasal altyapı ile kurumların alması gereken önlemler ve sahip olması gereken standartlar belirlenebilir. Örneğin Güney Kıbrıs dördüncü eylemin ikinci aşamasında siber güvenlik stratejisinin hükümlerini tam olarak desteklemek için uygun bir yasal çerçevenin oluşturulması hedeflenmektedir. Bulgaristan benzer hedeflere strateji ve eylem planında yer vermiştir. Belçika strateji ve eylem planının başarısı için hedeflerin yasal zemine oturtulması gerektiğini ifade etmiştir. Avusturya ise yasal zeminin kritik altyapı için önemli olduğunu savunmaktadır. Hırvatistan yasal altyapının kamu özel sektör işbirliği için önemine dikkat çekmiştir. Malta hukuk kuralı ilkesinden yola çıkarak yasal ve AB mevzuatına dikkat çekmiştir. İsveç ise uluslararası işbirliğini yasal altyapı açısından değerlendirmiştir.

6.1.11. Siber caydırıcılığın oluşturulması

Türkiye, Siber Güvenlik Kuruluna siber saldırılara karşı caydırıcılık sağlamak için gerekli tedbirlerin alınmasını sağlamayı bir görev olarak yüklemiştir. Buna rağmen gerek Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planında gerekse 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında caydırıcılığın nasıl sağlanacağına yönelik herhangi bir amaç belirlenmemiştir. Ancak, siber caydırıcılığın oluşturulması için 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planında tehdit unsurlarının saldırı yapmadan önce bertaraf edilmesi için ulusal proaktif siber savunma yeteneğinin geliştirilmesi hedeflenmiş olup söz konusu amacın siber caydırıcılığın oluşturulmasına yöneliktir. Ayrıca son strateji ve eylem planında siber suçların en aza indirgenmesi ve caydırıcılığın artırılması hedeflenmektedir.

Çizelge 6.11. Türkiye ile incelenen ülkelerin siber caydırıcılığın oluşturulması açısından karşılaştırılması

Ülkeler	Siber Caydırıcılığın Oluşturulması
Türkiye	Var
Almanya	Yok
Fransa	Yok
Belçika	Yok
İtalya	Yok
Lüksemburg	Yok
Hollanda	Var
İngiltere	Var
Danimarka	Yok
İrlanda	Yok
Yunanistan	Yok
Portekiz	Yok
İspanya	Yok
Avusturya	Yok
Finlandiya	Yok
İsveç	Yok
Güney Kıbrıs	Yok
Çekya	Yok
Estonya	Yok

Çizelge 6.11. (devam) Türkiye ile incelenen ülkelerin siber caydırıcılığın oluşturulması açısından karşılaştırılması

Ülkeler	Siber Caydırıcılığın Oluşturulması
Macaristan	Yok
Letonya	Yok
Litvanya	Yok
Malta	Yok
Polonya	Yok
Slovakya	Yok
Slovenya	Yok
Bulgaristan	Yok
Romanya	Yok
Hırvatistan	Yok

İngiltere, caydırıcılık alanına ayrı bir başlık açarak siber uzayda her türlü saldırganlık için zor bir hedef olmayı hedeflemiştir.

Hollanda tek başına veya bir koalisyonun parçası olarak, devlet aktörlerinin dijital saldırılarına anında ve uygun şekilde yanıt verebilmeyi ve caydırıcılığa katkıda bulunan saldırı yetenekleri geliştirmeyi hedeflemektedir. Böylece caydırıcılık konusu ülke hem kendi başına hem de ittifaklar ile sahip olmayı amaçlamıştır. Caydırıcılık tehdit ortaya çıkmadan gerekli olan bir güçtür. Ancak pek çok ülkenin caydırıcılığa doğrudan eğilmemesine rağmen liderlik ve gelişmişlik hedefleri vardır.

6.1.12. Kriterlerin genel değerlendirilmesi

Elde edilen bulgular bu bölümde çizelge haline getirilmiş olup Türkiye ile incelenen ülkeler belirlenen kriterler açısından kıyaslanmıştır. Bu kapsamda, belirlenen on bir adet kriterin ülkeler açısından değerlendirilmesi özeti aşağıda sunulmuştur:

Çizelge 6.12. Strateji ve eylem planlarının kriter bazında karşılaştırılması

	Strateji ve Eylem Planlarının Sürekliliği	Kritik Altyapı Güvenliği İçin Yatırım	Siber Güvenlik Alanında AR-GE Çalışmalarının Yapılması	Altyapının Gelişen Teknolojiye Adapte Edilmesi	Gelişen Teknolojide Liderlik Yapmak	Siber Uzayda Güçlü İttifak Kurmak	Siber Güvenlik İnsan Kaynağının Geliştirilmesi	Kamu Düzeyinde Eğitim Sağlanması	Devlet, İş Dünyası ve Sivil Toplum Arasında Ortaklık	Siber Saldırılara Karşı Yasal Önlemlerin Geliştirilmesi	Siber Caydırıcılığın Oluşturulması
Türkiye	Var	Var	Var	Var	Yok	Var	Var	Yok	Var	Var	Var
Almanya	Var	Var	Yok	Var	Yok	Var	Var	Var	Var	Var	Yok
Fransa	Yok	Var	Var	Var	Yok	Var	Var	Var	Var	Var	Yok
Belçika	Yok	Var	Yok	Var	Yok	Var	Var	Var	Var	Var	Yok
İtalya	Yok	Var	Var	Var	Yok	Var	Var	Var	Var	Var	Yok
Lüksemburg	Yok	Var	Var	Var	Yok	Var	Var	Var	Var	Yok	Yok
Hollanda	Yok	Yok	Var	Var	Var	Var	Var	Yok	Var	Var	Var
İngiltere	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Danimarka	Yok	Var	Var	Var	Yok	Var	Yok	Var	Var	Var	Yok
İrlanda	Yok	Var	Var	Var	Yok	Var	Var	Var	Var	Var	Yok
Yunanistan	Yok	Var	Var	Var	Yok	Var	Var	Yok	Var	Yok	Yok
Portekiz	Yok	Yok	Var	Var	Yok	Var	Var	Var	Var	Var	Yok
İspanya	Var	Var	Var	Var	Yok	Var	Var	Var	Var	Var	Yok
Avusturya	Yok	Var	Var	Yok	Var	Var	Var	Var	Var	Var	Yok
Finlandiya	Yok	Var	Var	Yok	Yok	Var	Var	Var	Yok	Yok	Yok
İsveç	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var	Yok
Güney Kıbrıs	Yok	Var	Yok	Var	Yok	Var	Var	Var	Var	Var	Yok
Çekya	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var	Yok
Estonya	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var	Yok
Macaristan	Yok	Var	Var	Var	Var	Var	Var	Var	Var	Yok	Yok
Letonya	Yok	Var	Var	Var	Yok	Var	Var	Var	Var	Var	Yok
Litvanya	Yok	Var	Var	Yok	Yok	Var	Var	Var	Var	Var	Yok
Malta	Yok	Yok	Yok	Var	Yok	Var	Var	Var	Var	Var	Yok
Polonya	Var	Var	Var	Var	Yok	Var	Var	Var	Var	Var	Yok
Slovakya	Yok	Var	Var	Yok	Yok	Var	Yok	Var	Var	Var	Yok
Slovenya	Yok	Yok	Var	Var	Yok	Var	Var	Var	Yok	Yok	Yok
Bulgaristan	Yok	Var	Var	Var	Yok	Var	Yok	Var	Var	Var	Yok
Romanya	Yok	Var	Var	Var	Yok	Var	Var	Var	Var	Yok	Yok
Hırvatistan	Yok	Var	Var	Var	Yok	Var	Var	Var	Var	Var	Yok

Siber güvenlik konusunda belirlenen ana kriterlerin güçlü bir sistemin sahip olması gereken özelliklerden seçilmesine dikkat edilmiştir. Strateji ve eylem planlarının sürekli olması yani dönemsel olarak birbirlerini takip etmesi başarı için son derece önemlidir. Çünkü strateji veya eylem planları adından anlaşılacağı üzere bir dönem içinde ulaşılması arzulanan hedefleri içermektedir ve her zaman bunlara ulaşmak mümkün olmamaktadır. Gelecek dönemin strateji ve eylem planları eski planın zayıflıklarının giderilmesine, başarılamayan hedeflerin daha sistematik ele alınmasına ve gerçekleşmelere odaklanmaktadır. Diğer kriterlerin değerlendirilmesi ise sonuç ve değerlendirme kısmında ayrıntılı olarak açıklanmıştır.

6.2. Türkiye'nin Strateji ve Eylem Planı İçin Öneriler

Bu bölümde gelecek dönem için oluşturulacak strateji ve eylem planı için öneriler oluşturulmuştur. Önerilerin AB ülkeleri ve İngiltere strateji ile eylem planlarının incelenmesinden ortaya çıkmış olup ve yukarıdaki kıyaslama kapsamında olmasına dikkat edilecektir. Aynı zamanda strateji ve eylem planlarının genelinde olmayan farklı değişkenler de dikkate alınacaktır. Geliştirilen önerilerin çoğu Türkiye'nin strateji ve eylem planlarında yer almaktadır. Bunun yanı sıra çoğu öneri alanında Türkiye ileri seviyededir. Ancak yine de spesifik olarak verilen bu önerilerin ayrı strateji ve eylemler şeklinde üst politika belgelerinde yer almasının önemli olduğu değerlendirilmektedir. Bölüm ile on ikinci sırada yer alan alt amacın gerçekleştirilmesi hedeflenmiştir.

6.2.1. Strateji ve eylem planlarının sürekliliği korunmalı

Türkiye'nin siber güvenlik politikasına yönelik olarak daha önce 2013-2014 ve 2016-2019 dönemlerini kapsayan siber güvenlik strateji ve eylem planı hazırlanmıştır. 2020 yılının sonunda 2020-2023 dönemini kapsayan Strateji ve Eylem Planı yayımlanmıştır. Ancak strateji ve eylem planı hem 2020 yılını kapsayacak şekilde hazırlanmış hem de 2020 yılının sonunda yürürlüğe koyulmuştur. Bu açıdan bir kopukluk ve kayıp bir yıl ortaya çıkmıştır. Strateji ve eylem planları 2013 yılında başlamış olup 2023 yılının sonunda üçüncü eylem planının süresi dolmuştur. Ayrıca 2014-2016 döneminde süreklilik açısından kopukluk meydana gelmiştir.

Bakanlar Kurulu'nun 11/06/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararı ile Siber Güvenlik Kurulu kurulmuştur. Kurulun en önemli görevleri siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak ve kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamaktır. 02/07/2018 tarihinde Kurul mülga edilmeden önce Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında, Dışişleri Bakanlığı Müsteşarı, İçişleri Bakanlığı Müsteşarı, Milli Savunma Bakanlığı Müsteşarı, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanından oluşmaktaydı.

Kurulun mülga edilmesiyle mevcut ve yeni strateji ve eylem planlarının koordinasyonuna zarar vermiştir. Kurulun görevlerinin bir kısmı Dijital Dönüşüm Ofisine bağlı Siber Güvenlik Dairesi Başkanlığına verilmiş olmasına rağmen tam anlamıyla kurumlar arasındaki koordinasyonun sağlanabileceği şüphelidir. Bu durum sürekliliğe zarar vermiştir. Sürekliliğin bir diğer yansıması ile ortak politikaların yürütülmesindeki yeknesaklık kriterinin kaybedilmesidir. Böyle bir durum kurumların, bakanlıkların veya özel sektör ile sivil toplumun ayrı politikalar yürütmesine neden olmuştur. Bu durum siber güvenlik açıklarının artmasıyla ve siber saldırılara karşı kurumların zafiyet göstermesiyle sonuçlanmıştır.

Siber güvenlik konusu sürekli değişen yapısından dolayı süreç olarak ele alınması gereken bu konudur. Bu yüzden strateji ve eylem planları sürekli olmalı ve politikaların kurumsal bir sahibi olmalıdır. Ülkemizde BTK kısmen bu açığı kapatmasına rağmen doğrudan yürütücü bir kurumsal yapının yeniden oluşturulması gerektiği değerlendirilmektedir.

6.2.2. Kritik altyapı güvenliği için yatırım yapılmalı

20/06/2013 tarih, 2 sayılı Siber Güvenlik Kurulu kararı uyarınca kritik altyapılar "*Elektronik Haberleşme*", "*Enerji*", "*Su Yönetimi*", "*Kritik Kamu Hizmetleri*", "*Ulaştırma*" ve "*Bankacılık ve Finans*" sektörlerini ifade etmektedir.

Kritik altyapılara yönelik BTK'nın 2019-2023 Stratejik Planındaki siber güvenlik ile hedeflerinden birisi "*Türkiye'nin ülkemizin kritik altyapı sistemlerinin siber güvenliğinin izlenebileceği bir merkeze sahip olması*" olarak belirlenmiştir.

Türkiye'nin kritik altyapıları genel bir değerlendirmeyle enerji üretim ve dağıtım sistemleri, ulaşım sistemleri, su yönetimi ve tedarik sistemleri, sağlık sistemleri, gıda üretim ve dağıtım sistemleri, kimya endüstrisi, bilgi ve iletişim teknolojileri, araştırma ve geliştirme faaliyetleri tesisleri ile finansal servisler olarak daha geniş bir şekilde ele almak mümkündür. Bu şekilde sistemlerin ve kurumların daha detaylı ele alınması özel siber güvenlik önlemlerinin alınmasına kapı aralayacaktır.

Kritik altyapılara yönelik güvenlik kriterleri, yatırımlar, tanımlamalar veya diğer düzenlemeler yapılması önerilmektedir. Bu açığın kapatılması Türkiye'nin siber güvenliği konusuna önemli katkılar sağlayacaktır. Gelecek dönemin siber güvenlik stratejisi ve eylem planında kritik altyapılara yönelik yatırım miktarının belirlenmesi ve özel ek bir eylem planının hazırlanması önerilmektedir.

6.2.3. Siber güvenlik alanında ar-ge çalışmaları teşvik edilmeli

Bilgi ve iletişim teknolojilerinde gelişim trendi son yıllarda devrim niteliğine bürünmüştür. Ayrıca açıklar ve zafiyetler benzer bir gelişim trendine sahiptir. Her gün yeni bir açık ortaya çıkmakta ve ülkeler, kurumlar veya sivil toplum saldırıya uğramaktadır. Gelişmiş veya gelişmekte olan ülke olup olmaması veya bilişim altyapısının sağlam olup olmamasına bakılmaksızın her kurum siber saldırıya uğrayabilir. Bu saldırıların başarılı olması ise sistemin güncelliğine ve sağlamlığına bağlıdır.

Siber güvenlik alanında gelişim trendini yakalamak için araştırma ve geliştirme faaliyetlerine ülkeler tarafından büyük yatırımlar yapılmaktadır. Siber güvenlik sektörünün gelişmesi bu yatırımlar ve gerek üniversiteler gerek özel şirketler gerekse kamu kurumlarının işbirliği ile başarılı sonuçlar sunabilir.

Ar-Ge yatırımları sadece mevcut sistemlerin geliştirilmesini değil aynı zamanda yeni siber güvenlik sistemlerinin de oluşturulmasına katkı sağlar. Ar-Ge yatırımlarının artırılması kamu tarafından teşvik edilmeli ve yeni firmalar ile fikirlerin desteklenmesi önem

kazanmıştır. Bu açıdan yeni strateji ve eylem planında siber güvenlikte yerli teknolojilerin geliştirilmesi ana amacına bağlı olan Ar-Ge faaliyetlerinin teşvik edilmesi, siber güvenlik konusunda Ar-Ge laboratuvarlarının kurulması ve siber güvenlik konusunda Ar-Ge laboratuvarlarının kurulması alt amaçları detaylandırılmıştır. Bu açıdan Türkiye'nin Ar-Ge faaliyetlerine özel önem verdiği, yerli teknolojileri desteklediği ve kurumsal iş birliğini teşvik ettiği söylenebilir.

Yeni dönemim strateji ve eylem planında yerli teknolojilerin desteklenmesi ile Ar-Ge faaliyetlerinin yürütülmesine yönelik daha detaylı hedeflere yer verilmesi önerilmektedir. Bu amacın faaliyetler bazında detaylandırılması ve adım adım sürecin analiz edilmesi tavsiye edilmektedir. Siber güvenlik alanında yeni fikir ve firmalara destek sunulması ülkenin savunma kapasitesini artırabilir ve aynı zamanda ihraç ürünlerinin icat edilmesini de sağlayabilir.

6.2.4. Altyapı gelişen teknolojiye adapte edilmeli

Gelişen ve değişen teknoloji eski sistemler üzerindeki zafiyetlerin ortaya çıkmasına neden olmaktadır. Altyapının sürekli olarak güncel tutulması ile birlikte gelişen teknolojiye adapte edilmesi hem maliyet avantajı sağlar hem de zafiyetlerin ortaya çıkmasından önce engellenmesine katkı sağlar.

Türkiye'nin ikinci eylem planının tespitlerinden birisi kurumlarda bilgi güvenliği yönetimi altyapılarının yeterli düzeyde olmaması şeklindedir. Yapılan testler ve kontroller açıkların fazla olduğunu kurumsal farklığın yüksek olduğunu göstermektedir. Bu konuda yapılan çalışmalardan elde edilen bilgiler ile mevcut teknolojinin gelişen teknolojiye adapte edilmesi önem kazanmaktadır. Yeni veya sıfırdan bir sistem kurulması hem çok masraflı hem de yönetimi zor bir yapıdadır. Bu yüzden değişim ve gelişimin adım adım yapılması gerekmektedir.

Gelecek strateji ve eylem planının ana dayanak noktalarından birisi de mevcut altyapının gelişen ve değişen teknolojiye uyumun sağlanması olmalıdır. Kısa dönemli sonuç alınması için hedefin hızlı bir şekilde uygulanması ve envanter analizi yapılması tavsiye edilmektedir. Altyapının gelişen teknolojiye adapte edilmesi için bakanlık, sektörel, coğrafi temelli veya toplu projeler geliştirilebilir.

6.2.5. Gelişen teknolojide liderlik amaçlanmalı

Siber güvenlik ülkelerin büyük yatırımlar yaptığı ve her geçen gün ekonomik katma değeri yükselen bir sektördür. Belli başlı ülkelerin öne çıktığı bu sektörde donanım ve yazılım geliştirme faaliyetlerine yatırım yapılması ve sonucunda başarı kazanması durumunda büyük gelir kapılarını açabilmektedir.

Sektörde her ne kadar büyük firmalar piyasayı domine etse de dinamik yapısından dolayı küçük şirketler veya yeni fikirler kolaylıkla kendilerine alan açabilmektedir. Devletlerin veya girişimcilere kaynak sağlayan bankalar ile özel yapıların bu açıdan siber güvenlik şirketlerine sürekli olarak yatırım yaptığı görülmektedir.

Türkiye'nin ilk iki strateji ve eylem planında sektörde lider pozisyona erişilmesine yönelik herhangi bir hedefe yer verilmemiştir. Ancak siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilmesi ve siber güvenlikte yerli teknolojilerin geliştirilmesi ana hedeflerden biri olarak belirlenmiştir. Buna rağmen yerli teknolojilerin geliştirilmesiyle birlikte o alanda da liderlik etmek amaçlanmamıştır.

Gelecek dönemde hazırlanacak strateji ve eylem planında siber güvenlik alanında lider olmak ana amaçlardan birisi olarak belirlenmesi önerilmektedir. Bunun yanı sıra yerli ürünlerin geliştirilmesi için avantajlı alım usullerinin uygulanması, kamu kurum ve kuruluşlarının yerli ürünlerine yönlendirilmesi, şirketlerin finansal kaynaklara erişmesine yönelik farklı yöntemler belirlenmesi ve dışa açılma konusunda teşvikler verilmesi önem kazanmıştır. Bu açıdan sürecin iyi planlanması ve ayrıntılı alt faaliyetler belirlenmesi gerekmektedir.

6.2.6. Siber uzayda güçlü ittifaklar kurulmalı

Siber güvenlik yapısı itibarıyla ülkelerin tek başına altından kalkamayacağı kadar büyük bir konudur. Uluslararası güvenlik ittifaklarındaki zorunluluk gibi siber güvenlik alanında da işbirlikleri gereklidir. Savunma sisteminin caydırıcı olması bu işbirliğinin ortaklarına ve ortaklar arasındaki bilgi düzeyinin yüksekliğine bağlıdır.

Türkiye'nin ilk iki eylem planında da siber güvenlik alanında işbirliği yapılması yönelik olarak tespit, hedef ve faaliyetlere yer verilmiştir. Bu hedefler kritik altyapıların korunması,

mevzuatın düzenlenmesi ve siber olayların takip edilmesi ile bilgi paylaşımı esasına göre düzenlenmiştir.

İncelenen tüm eylem planlarında ittifakların güçlendirilmesi, bilgi paylaşımının teşvik edilmesi ve işbirliğinin geliştirilmesine yönelik hedef ve faaliyetlere yer verilmiştir. Uluslararası işbirliği güçlü bir savunma altyapısı ve caydırıcılık için önemlidir. Ülkelerin ittifaklar kurması, ittifaklar aracılığıyla incelemeler yapılması ve sağlam bir yapının oluşturulması önerilmektedir.

Türkiye bu kriter özelinde oldukça gelişmiştir. Gelecek dönemde hazırlanacak strateji ve eylem planının uluslararası işbirliği bölümü ve hedefleri detaylı hazırlanması önerilmektedir. Ayrıca güçlü ittifakların getireceği sinerji ülkenin tüm kurum ve kuruluşlarına dağıtılmalıdır. Kurumların ayrı ayrı veya devlet düzeyinde ittifaklar kurulması teşvik edilmelidir. Oluşturulacak sinerji güncel siber tehditlere karşı hazırlıklı olunmasına yardımcı olur ve en önemlisi caydırıcılık kazanılmasını destekleyecektir.

6.2.7. Siber güvenlik insan kaynağına yatırım yapılmalı

Siber güvenliğin en önemli caydırıcılık dayanağı insan kaynağıdır. Yetişmiş insan kaynağı siber saldırıları engelleyebilir, güçlü bir sistem kurulmasını sağlayabilir, yeni teknolojilerin gelişmesine ön ayak olabilir. Devletler yetişmiş insan kaynağının güçlü bir şekilde sağlanması için büyük yatırımlar yapmaktadır. Üniversiteler ve özel kurslar insan kaynağının yetiştirilmesi için çok önemli görevler üstlenmektedir.

Türkiye'nin ilk strateji ve eylem planında ulusal siber güvenlik altyapısının güçlendirilmesi ana hedeflerden biri olarak belirlenmiştir. Bu hedef kapsamında siber güvenlik eğitim altyapısının güçlendirilmesi, üniversitelerde siber güvenlik eğitimlerinin yaygınlaştırılması ve ilk, orta, lise öğretimi ve yaygın eğitimde siber güvenlik eğitimlerine yer verilmesi faaliyet olarak açıklanmıştır.

Strateji ve eylem planları medya açısından incelendiğinde pek çok tanıtım faaliyetine yer verildiği, siber güvenlik alanında yeni üniversite bölümlerinin açıldığı, büyük projelerin geliştirildiği ve insan kaynağı kapasitesinin artırılmasına yönelik çalışmalara hız verildiği görülmektedir. Ancak son yıllarda yetişmiş insan gücünün ülke dışına çıktığı ve istenilen

sonuçların alınmadığı görülmektedir. Gelecek eylem planının insan kaynağının yetiştirilmesine yönelik daha kapsamlı faaliyetler geliştirilmesi ve tersine beyin göçüne ayrıca önem verilmesi önerilmektedir.

6.2.8. Kamu düzeyinde eğitim sağlanmalı

Siber güvenliğin tam olarak sağlanması mümkün değildir. Şüphesiz her zaman için zafiyetler veya genel olarak eksiklikler olacaktır. Ulusal güvenliğin bir yansıması olan siber güvenliğin sağlanması için insan kaynağının farkındalık düzeyinin yüksek olması gerekmektedir. Pek çok siber saldırı insanların zafiyetinden yararlanılarak ve insandan kaynaklanan eksiklikleri sömürerek başarıya ulaşmaktadır.

Türkiye'nin ikinci strateji ve eylem planının ana hedeflerinden birisi farkındalık ve insan kaynağı geliştirme olarak belirlenmiştir. Faaliyet olarak ise toplumun her kesiminde siber güvenlik bilincinin oluşturulması, eğitim kurumlarının çalışmalarına ilave olarak yazılı ve görsel medyada farkındalık çalışmalarının yapılması şeklinde açıklanmıştır.

Gelecek dönemde siber güvenlik strateji ve eylem planında daha detaylı faaliyetler geliştirilmesi, örnek afişlerin hazırlanması, eğitim programlarının oluşturulması ve reklam filmlerinin yapılması önerilmektedir. Bunun yanı sıra çalışanların da detaylı bir şekilde programlanması önem kazanmıştır. Siber saldırılar kişileri, kişilerin kullandığı sistemleri ve olası güvenlik açıklarını tanımlamak ve açıklamak gerekmektedir. Bu açıdan bilinçlendirme ve eğitim faaliyetleri strateji ve eylem planının en önemli sacayaklarından biri haline gelmektedir.

6.2.9. Devlet, iş dünyası ve sivil toplum arasında ortaklık kurulmalı

Siber güvenliğin sağlanması için uluslararası işbirliği kadar bir ülkedeki kamu kurumları, özel sektör ve sivil toplum arasındaki da güçlü ittifakların kurulması gerekmektedir. Kurumlar ve kişilerin birbirine siber uzayda bağlı olması ve bir tarafın zafiyetinin diğer tarafın sistemsel sağlamlığına zarar vermesi bu ittifakı zorunlu kılmaktadır.

İncelenen tüm strateji ve eylem planlarında aktörler arasındaki işbirliğinin geliştirilmesine ve daha ileri bir seviye olarak kamu-özel sektör işbirliği modeline göre uygulamalar tavsiye edilmiştir. Kamunun tek başına siber uzayda tüm tehditlerle başa çıkması veya caydırıcı bir

sistem geliştirmesi mümkün değildir. Özel sektörün uzmanlığı, dinamizmi ve hızlı karar verme gibi yeteneklerinden faydalanmak için kamu sektörü gerek siber güvenlik yatırımlarında gerekse yeni teknolojilerin geliştirilmesinde özel sektör ile işbirlikleri yapmaktadır.

Türkiye'nin tüm strateji ve eylem planlarında da özel sektör ile işbirliğinin geliştirilmesine yönelik hedef ve faaliyetlere yer verilmiştir. Ancak diğer eylem planlarıyla kıyaslandığında oluşturulan hedeflerin kapsamının dar olduğunu söylemek mümkündür. Bu açıdan gelecek eylem planının daha kapsamlı bir şekilde aktörlerin ittifak geliştirilmesine yönelik ana hedef, alt amaç ve faaliyetlere yer verilmesi önerilmektedir.

6.2.10. Siber saldırılara karşı yasal önlemlerin geliştirilmesi

Kamu sektörü diğer alanlarda olduğu gibi siber güvenlik ve siber uzay kapsamında yasal çerçeve içinde hareket etmek zorundadır. Bu çerçeve saldırıların önlenmesi, teknolojik gerekliliklerin belirlenmesi, uzmanlığın yeterlilikleri gibi pek çok farklı konuları içermelidir. Yasal yapının oluşturulması bir ülkede tüm vatandaşların uyması gereken kuralların ortaya koyulmasını sağlar. Ayrıca mevzuat düzenlemeleri ile siber güvenlik politikalarının yetkili kurumu, görevi, yetkileri ve yapısı da ortaya koyulur.

İncelenen eylem planlarının çoğunda yasal mevzuatın oluşturulmasına yönelik hedeflere ve faaliyetlere yer verilmiştir. Türkiye'nin ilk eylem planında yasal düzenlemelerin hayata geçirilmesi ana hedeflerinden biri olarak belirlenmiştir. Bu hedefin gerçekleştirilmesine yönelik iki adet alt faaliyet oluşturulmuştur. İlk faaliyet Siber Güvenlik Kurulunun oluşturulmasıdır. Kurul oluşturulmuş ama daha sonra işlevsiz kalmıştır. Bir sonraki faaliyet ise siber güvenlik konusunda mevzuat çalışmalarının yapılmasıdır. Faaliyete yönelik pek çok uygulama hayata geçirilmiştir.

Gelecek eylem planında yasal yapıya yönelik hedeflerin daha spesifik olması ve faaliyetlerin daha fazla sayıda belirlenmesi önerilmektedir. Diğer ülkelerin mevzuat çalışmaları incelenerek örnekler Türkiye'ye adapte edilebilir. Bunun yanı sıra iyi uygulama örneklerinin benzer sistemler içinde ele alınması tavsiye edilmektedir. Özellikle caydırıcılık, teknolojik teşvik, siber savunmama gerekliliği ve kural temelli yaklaşımlar siber uzayda sağlam bir yapının oluşturulmasına katkı sağlayabilir.

6.2.11. Siber caydırıcılığın oluşturulması

Siber caydırıcılık bir ülkenin en önemli silahıdır. Sağlam bir siber altyapı, yetişmiş insan kaynağı ve karşılık verebilme kapasitesine bağlı olan caydırıcılık gücü yükselecektir. Bir ülkenin caydırıcılık seviyesi ne kadar yüksekse o kadar siber uzayda başarılı demektir. Bu yüzden ana hedeflerden biri siber caydırıcılığın kazanması olmalıdır.

Günümüzde ülkeler siber güvenliğe ne kadar yatırım yaparlarsa yapsınlar veya ne kadar güçlü bir konum elde etmiş olurlarsa olsunlar her zaman saldırıya uğrama riskiyle karşı karşıyadır. Bu açıdan bakıldığında siber caydırıcılığın tam olarak herkesi engellemesi mümkün değildir.

Siber caydırıcılık, ülkelere yapılan saldırıların karşılık verileceğini ve cezalandırılacağını açıklayan bir kavramdır. Siber caydırıcılığın kazanılması için yatırımların yapılması, siber güvenlik politikalarının geliştirilmesi ve ulusal/ uluslararası işbirliğinin güçlendirilmesi gerekmektedir. Bu atılan adımlar ile devletler siber saldırılara daha dayanıklı hale gelir. Siber korsanlar ise sonuca ulaşamadığı için siber caydırıcılığa sahip olan ülkelere saldırıyı tercih etmeyebilir.

Siber caydırıcılığın sağlanmasına yönelik bazı ülkeler hedef ve faaliyet geliştirilmesi rağmen çoğu ülke bu konuya değinmemiştir. Türkiye'de ise BTK'nın stratejik hedeflerinden birisi "*ulusal siber güvenliğe yönelik faaliyetler kapsamında siber saldırılara karşı korunma ile bu saldırılara karşı caydırıcılık sağlamak için gerekli tedbirlerin alınmasını sağlamak ve bu konuda gerekli yaptırımları uygulamak*" şeklinde belirlenmiştir. Ancak tüm strateji ve eylem planlarında konu hakkında herhangi bir özel hedef veya faaliyete yer verilmemiştir. Gelecek dönemde hazırlanacak strateji ve eylem planında siber caydırıcılığın kazanılması ana tema olarak belirlenmelidir.

6.2.12. Siber güvenlik bütçesi oluşturulmalı

Siber güvenlik yatırımları büyük tutarlara neden olmaktadır. Sürekli değişen teknolojiye uyum sağlamak için ise bu yatırımların da sürekli olması gerekmektedir. Siber güvenlik strateji ve eylem planlarında yer alan hedef ve faaliyetlerin büyük çoğunluğuna bütçe tahsis

edilmemiştir. Böyle bir yolun izlenmesi şüphesiz strateji ve eylem planlarının önemli bir eksikliğidir.

Türkiye'nin hazırlanan tüm strateji ve eylem planlarında da maliyet tahmini ve bütçe tahsisi yapılmamıştır. Hedeflerin ne derece tutturulduğu veya faaliyetlerin yerine getirilip getirilmediği kontrol edilmemesinin bir nedeni şüphesiz parasal tahminlere yer verilmemesidir. Çünkü eğer maliyet tahmini yapılsaydı veya bütçe tahsisi gerçekleştirilesiydi gerek faaliyetler kontrol edilecekti gerekse hedeflere ne derece ulaşıldığı öğrenilebilecekti.

Gelecek dönemde hazırlanması planlanan strateji ve eylem planının bütçesinin belirlenmesi, faaliyetler için ayrı ayrı kaynak tahsis edilmesi ve kurumsal yetki ile birlikte ekonomik kuvvetin de sunulması tavsiye edilmektedir. Tanıtım faaliyetlerinden eğitimin programlanmasına kadar tüm ana hedeflerin ve faaliyetlerin bütçesel olarak ele alınması önerilmektedir.

7. SONUÇ VE ÖNERİLER

Bir ülkenin varlığını devam ettirmesi genel olarak güvenliğini sağlamasına başlıdır. Ulus devletlerin yaygınlık kazanması ulusal güvenlik kavramının gündeme ve literatüre yerleşmesini sağlamıştır. Bilgi ve iletişim teknolojilerindeki gelişmeler ile birlikte ulusal güvenlik kavramının bir dalı olarak siber güvenlik kavramı doğmuştur. Ulusal güvenliği bir ülkenin kendisini ve vatandaşlarının her türlü güvenliğinin sağlanması olarak tanımlamak mümkünken siber güvenliği bir ülkenin tüm aktörlerinin siber uzaydaki tehditlere karşı koymak için araç, politika, kılavuz, risk yönetimi ve eğitim ile teknolojileri ifade etmektedir.

Siber güvenlikte tehditler ve tehdit sahipleri sürekli olarak değişmektedir. Siber saldırılar her an ortaya çıkabilmekte, siber teröristler organize bir şekilde sistemlere sızabilmekte, kritik bilgiler siber casuslar tarafından ele geçirilebilmekte, son otuz yılda pek çok siber suç olarak tanımlanan faaliyetler ortaya çıkabilmekte ve ülkeler arasında siber savaşlar ortaya çıkabilmektedir. Bu kadar karmaşık ve puslu bir ortamda ülkelerin dost veya düşman diğer ülkelere karşı sürekli olarak hazırlıklı olması gerekmektedir. Hazır olmanın en iyi yolu ise güçlü strateji ve eylem planları hazırlamak ve uygulamaktır. 2000'li yıllardan itibaren pek çok ülke siber güvenlik alanında planlar hazırlamakta ve stratejiler geliştirmektedir. Türkiye ise söz konusu alanda geç kalmış ve ilk strateji ve eylem planını 2013 yılında hazırlayabilmiştir.

Siber Güvenlik Kurulu'nun 2012 yılında kurulması ve ilk strateji ve eylem planının 2013 yılında yürürlüğe koyulması önemli bir başarıdır. Ancak yeni hükümet sistemi ile birlikte Siber Güvenlik Kurulu'nun işlevsiz kalması, yeni sisteme adapte edilememesi ve iki yıldan uzun süredir herhangi bir düzenleme yapılmaması konunun koordinasyonuna zarar vermektedir. Son toplantısını 2013 yılının sonunda yapması ise daha büyük bir sorun olarak önümüzde durmaktadır. BTK, Güvenlik ve Dış Politikalar Kurulu, Dijital Dönüşüm Ofisi gibi yapıların siber güvenlik alanına dair yetkileri olmasına rağmen bu durum çok başlılığa neden olmaktadır.

20/06/2013 tarih, 28683 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı kapsamlı ve sağlam temellere dayandırılmıştır. İngiltere ve diğer ülkelerin aksine 2013-2014 Strateji ve Eylem Planı yıllık veya dönemlik olarak takip edilmemiş, gerçekleşmeler izlenmemiştir. Strateji ve eylem

planının başarısının ölçülmemesi veya ölçülmeden iki yıl aradan sonra 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının yürürlüğe koyulması büyük bir eksikliğe neden olmuştur. Daha sonra bir yıl aradan sonra ve bir yılın da geç yayından dolayı toplam iki yıl kayıp ortaya çıkarak 2020-2023 dönemi için Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlanmış ve yürürlüğe koyulmuştur. Çünkü strateji ve eylem planlarında benzerlikle olduğu gibi bu benzerliklerin başarısızlıktan kaynaklanıp kaynaklanmadığı belli değildir. Planların maliyetlendirilmesinin yapılmaması ile yatırım planının hazırlanmaması diğer eksikliklerden daha önemlidir. Siber güvenlik alanı büyük yatırımlara ihtiyaç duyulan ve sürekli olarak geliştirilmesi gereken bir sektördür. Buna rağmen 2013-2014 Strateji ve Eylem Planı döneminde yasal düzenlemelerin hayata geçirilmesi, USOM ve SOME ekiplerinin kurulması, insan kaynağının yetiştirilmesi ve bilinçlendirilmesi vb. amaçlarına ulaşıldığını söylemek mümkündür. Yine de yapılması gereken pek çok faaliyet bulunmaktadır.

2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ise uzun bir hazırlık sürecinden sonra kamuoyuna 23 Kasım 2016 tarihinde duyurulmuştur. Strateji ve eylem planının yürürlük tarihine ise ulaşılamamıştır. Bu durum planın sahipsiz kalmasına ve BTK ile Ulaştırma ve Altyapı Bakanlığı arasında yetki karmaşasına neden olmuştur. Strateji ve eylem planı daha önceki planla benzer amaçlara sahip olup yatırım maliyeti hesaplanmamış veya takibi yapılmamıştır. 2019 yılı sonu itibarıyla yeni bir strateji ve eylem planının hazırlıklarına veya çalışmalarına yönelik kamuoyuna herhangi bir haber yansımamıştır. Daha sonra 2020 yılının sonunda Ulusal Siber Güvenlik Stratejisi ve Eylem Planı Resmi Gazete'de yayımlanarak yürürlüğe koyulmuştur.

Almanya diğer alanlarda olduğu gibi siber güvenlik alanında da sürekli bir ilerleme içindedir. AB'nin liderliğine gönülsüz olarak sahip olan Almanya gerek ülkesinin gerekse birliğin siber güvenlik alanında öncü bir rol üstlenmesi için çalışmaktadır. Bu yapının bir benzeri diğer birlik üyesi Fransa için de geçerlidir. Danimarka ve İrlanda kapsamlı strateji ve eylem planı hazırlayan ülkelerden olup AB ve dünya özelinde liderliği amaçlayan ülkelerdir. Birliğin yeni üyelerinden olan Hırvatistan'da sürekli bir gelişim içinde olmayı hedeflemektedir.

İngiltere siber güvenlik stratejisi ve eylem planı konusunda en kapsamlı ve gerçekçi ülkelerden birisidir. Strateji ve eylem planlarını sürekli olarak takip etmesi, hükümete

sonuçların rapor edilmesi, yatırım tutarının belirlenmesi ve amaçlara göre bölüştürülmesi planın sadece sözde kalmamasını sağlamıştır. Ülkemiz tarafından büyük oranda İngiltere'nin stratejisi ve eylem planından esinlenmiştir. Başarılı bir uygulama ve sistemin örnek alınması ise doğru bir yaklaşım olmuştur. Polonya, AB üyesi olup genel olarak strateji ve eylem planında İngiltere ekolünü takip etmiştir. İncelenen ülkelerle kıyaslandığında İngiltere'den sonra maliyetlendirme yapan tek devlettir. Uzun bir dönemi kapsaması ve genel bir alanı içine alması planın bir diğer dikkat çeken özelliğidir.

Strateji ve eylem planlarının sürekliliği gelişim ve sürdürülebilir kalkınma için son derece önemlidir. Arada kopukluk olmasına rağmen ülkemizin sürekliliğe sahip olduğunu söylemek mümkündür. Siber Güvenlik alanında Ar-Ge çalışmalarının yapılması teknolojik ilerlemeler ve ulusal yapılar için son derece önemlidir. Büyük insan kaynağı yatırımlarına ve teknolojilere ihtiyaç duymaktadır. Tüm strateji ve eylem planlarımızda bu durumun ciddiyetine vurgu yapılmıştır.

Kritik altyapıların belirlenmesi ve söz konusu kritik altyapılara farkı korunma önlemlerin alınması son dönemde tüm mecralarda dile getirilmektedir. Kritik altyapılar genellikle toplumun genelinin hayat koşullarını etkileyecek yapılardır. Bu yapılara yapılan siber saldırılar sosyal hayatı büyük bir kesintiye uğratabilir. Veya sağlık sektöründeki sistemindeki yapılara yapılan saldırıların sonuçları ölümcül olabilir. Bunun yanı sıra ekonomik sistemleri hedef alan siber saldırıların büyük mali kayıplara neden olması mümkündür. Kritik altyapıların korunması söz konusu nedenlerden dolayı strateji ve eylem planlarında daha detaylı yer almalı ve kapsamlı hedefler belirlenmelidir.

Altyapının gelişen teknolojiye adapte edilmesi konusunda ise neredeyse bütün ülkeler hedef belirlemiştir. Değişen teknolojiye uyum sağlanamaması büyük açıklara neden olabilmekte ve sorunlar çıkabilmektedir. Bunun için gerek güncelleme gerekse yeni teknolojilere uyum hem kritik altyapıların korunması hem de trendi takip edilmesi için son derece önemlidir. Eski teknolojiler ve sistemler pek çok açığa ve soruna neden olmaktadır.

Siber uzayda güçlü ittifak kurmayı hedefleyen ülkeler tek başlarına dünya sahnesinde yer bulmanın zorluğunun farkındadırlar. Çünkü globalleşme ile birlikte sistemler iç içe girmiş ve birbirlerine daha fazla bağlı hale gelmiştir. Bu durum zorunlu olarak birliklerin kurulması ve yakınsamanın hızlanmasına neden olmuştur. Neredeyse tüm ülkeler uluslararası

birlikteliği hedefleri içine koymuştur. Siber güvenliğin sağlanması büyük oranda insan kaynağına bağlıdır. Teknolojiler sürekli olarak geliştirilmesine rağmen bu teknolojileri kullanacak insan kaynağının olmaması veya yetersizliği ülkelerin zarar görmesine neden olabilmektedir. Tüm ülkeler söz konusu durumun farkında olup strateji ve eylem planlarında hedefleri içinde insan kaynaklarını dahil etmiştir. Kamu düzeyinde eğitim sağlanması ise siber güvenlik insan kaynağının geliştirilmesi ile yakın bir bağlantı içinde olup ülkeler benzer hedefler belirlemiştir.

Ülkelerin ulusal güvenliklerini sağlamaları tüm aktörlerin katılımına ve işbirliğine bağlıdır. Siber güvenlik ise ulusal güvenlikten daha yakın bir işbirliğine ihtiyaç duymaktadır. Bu yüzden Fransa hariç tüm ülkeler devlet, iş dünyası ve sivil toplum arasında ortaklığın sağlanmasına son derece önem atfetmişlerdir. Siber güvenlik ihlallerinin yasal zemine oturtulması, cezaların belirlenmesi, sistemin korunması ve gelişmelere uyum sağlanması kanuni düzenlemeler ile sağlanabilir. Bu yüzden siber saldırılara karşı yasal önlemlerin geliştirilmesi tüm ülkelerce strateji ve eylem planlarına eklenmiştir.

Saldırıların ve ihlallerin olmadan önce engellenmesi sağlam bir yasal ve teknoloji altyapısına bağlıdır. Bu durum siber güvenlik alanında caydırıcılık kavramıyla açıklanmaktadır. Caydırıcılığın ölçülmesi için çalışmada siber caydırıcılığın oluşturulması kriteri oluşturulmuş ve ülkeler kıyaslanmıştır. Siber caydırıcılık konusunda yatırım yapılması önemli görülmektedir. Siber saldırılara karşı korsanları işin başında vazgeçmeyi amaçlayan caydırıcılık tüm ülkelerin ana hedefi olmalıdır. Yine de ne kadar caydırıcılık seviyesi yüksek olursa olsun siber saldırı olasılığı her zaman için olacaktır. Gelecek çalışmalarda araştırmacılar daha fazla ülkeyi inceleyerek ve kıyaslama kriterlerini artırarak literatüre katkı sağlayabilirler.

KAYNAKLAR

Ada, M. (2018). *Nato Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi.* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.

Ak, T., (2013) *Ulusal Güvenlik-Çevresel Güvenlik Ekseninde Silahlı Kuvvetler Çevre İlişkisi*. Yayımlanmamış Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Anas M. K. (2014), *National Cyber Security Strategy (NCSS): A Model For Nigeria*, Yaşar University Graduate School of Natural and Applied Sciences (Master Thesis), Bornova İzmir.

Aydın, H. (2008), *Toplumsal Güvenlik ve Yerel Siyaset*, Yerel Siyaset Dergisi, (28), 8-17.

Bailey, K. D. (1982). *Methods of Social Research*. New York: Free Press.

Balcı, A. (2016). Sosyal Bilimlerde Araştırma Yöntem, Teknik ve İlkeler. Pegem Akademi.

Baş, T., ve Akturan, U. (2017). Sosyal Bilimlerde Bilgisayar Destekli Nitel Araştırma Yöntemleri. Seçkin Yayıncılık.

Bektaş, Ö. ve Zabun, E. (2019). *Vatandaşlık Eğitiminde Değerler Karşılaştırması: Türkiye ve Fransa*. Değerler Eğitimi Dergisi, 17 (37), 247-289.

Bilici, N. (2005). *Türkiye-Avrupa Birliği İlişkileri*, Seçkin Yayınları, Ankara.

Bilici, N. (2006). *AB'de Ekonomik Bütünleşme ve Türkiye'nin Entegrasyonu*, Ankara Avrupa Çalışmaları Dergisi, 5,(2), Ankara.

Buzan, B., Wæver, O. ve Wilde, J. D. (1998). *Security: A New Framework for Analysis*. Boulder, London: Lynne Rienner Publishers.

Canbek, G., ve Sağıroğlu, Ş. (2007). *Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma*. Gazi Üniv. Müh. Mim. Fak. Der., 22(1), 121-136.

Cartwright J. E. (2011). *Memorandum for Chiefs of the Military Servs*., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5.

Chen, P. Desment, L. ve Huygens, C. (2014). *A Study on Advanced Persistent Threats*. Communications and Multimedia Security, 63-72.

Clarke, R.A., and Knake, R.K. (2010). Cyber War. HarperCollins e-books. 11.

Collin, B. C. (2004). *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*, 11th Annual International Symposium, Institute for Security and Intelligence.

Corbin, J. ve Strauss, A. (2008). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks: Sage.

Dedeoğlu, B. (2003). *Uluslararası Güvenlik ve Strateji*,. İstanbul: Derin Yayınları.

Denning, E. D. (2000). *Cyberterrorism*, Global Dialogue [abstract].

Dinan, D. (2014). *Europe Recast: A History Of European Union*. USA. Lynne Rienner Publishers.

Dönmez, S. (2010), *Güvenlik Anlayışının Dönüşümü: İttifak Kavramı ve NATO*. Yayınlanmamış Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Eren, M. (2016), *Avrupa Birliği'nin Siber Güvenlik Politikası*. Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, Avrupa Birliği Enstitüsü, İstanbul.

European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. European Commission, Brussels.

Evans, D. (2011). *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*. Cisco Internet Business Solutions Group (IBSG).

Fei, G. (2011). *China's Cybersecurity Challenges and Foreign Policy*. Georgetown Journal of International Affairs, 185-190.

Friedberg, I. Skopik, F. Settani, G., and Fiedler R. (2015). *Combating advanced persistent threats: From network event correlation to incident detection*. Computers & Security 48, 35-57.

Gibson, R. ve Erle, S. (2006). *Google Maps Hack*. Sebastopol: O'reilly Media.

Goodrich, M. ve Tamassia, R. (2010). *Introduction to Computer Security*. Essex: Pearson.

Göçoğlu, V. (2018). *Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi*. Yayımlanmamış Doktora Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Hamdi A. (2008). *Toplumsal Güvenlik ve Yerel Siyaset*. Yerel Siyaset, Okutan Yayıncılık, İstanbul.

Hansen, L. ve Nissenbaum, H. (2009). Dij*ital disaster, Cyber Security, and the Copenhagan School*. International Studies Quarterly, 53, 1155- 1175.

Hogben, G. (2011). Botnets: Detection, Measurement, Disinfection & Defence. ENISA. Web: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence, Son Erişim Tarihi: 28.11.2020.

İnternet: Çekya, National Cyber Security Strategy Of The Czech Republic For The Period From 2015 To 2020, Web: https://www.enisa.europa.eu/about-enisa/structure-

organization/national-liaison-office/news-from-the-member-states/czech-republic-national-cyber-security-strategy-2015-2020, Son Erişim tarihi: 18.11.2020.

İnternet: European Commission (EC) (2013). Web: https://ec.europa.eu/info/law_en, Son Erişim Tarihi: 05.05.2020.

İnternet: Granger, S. Social Engineering Fundamentals, Part I: Hacker Tactics. Security Focus, Web: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1050.4098&rep=rep1&type=pdf, Son Erişim Tarihi: 18.12.2020

İnternet: Letonya, Cyber Security Strategy of Latvia 2014-2018, Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss, Son Erişim Tarihi: 09.11.2020.

İnternet Hürriyet, Türkiye'de 1.6 milyon siber saldırı gerçekleşti, Web: https://www.hurriyet.com.tr/sosyal/tekno/turkiyede-1-6-milyon-siber-saldiri-gerceklesti-41711458, Son Erişim Tarihi: 12.02.2021.

İnternet: 1 sayılı Cumhurbaşkanlığı Kararnamesi, (2018/10/7) . Resmi Gazete (Sayı: 30474). Web: https://www.mevzuat.gov.tr/MevzuatMetin/19.5.1.pdf, Son Erişim Tarihi: 8.12.2021.

İnternet: 5809 sayılı Elektronik ve Haberleşme Kanunu, (2008/5/11). Resmi Gazete (27050 (Mükerrer)). Web: https://www.mevzuat.gov.tr/MevzuatMetin/19.5.1.pdf, Son Erişim Tarihi: 8.12.2021.

İnternet: AB Bakanlığı (Avrupa Birliği Bakanlığı) (2020). https://www.ab.gov.tr/65.html, Son Erişim Tarihi: 28.02.2020.

İnternet: AKÇTKA (Avrupa Kömür Çelik Topluluğunu Kuran Antlaşma) (1951). https://Europa.Eu/European-Union/Law/Treaties_En, Son Erişim Tarihi: 28.02.2020

İnternet: Almanya, Cyber Security Strategy for Germany (2016), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany Son Erişim Tarihi: 8.12.2020.

İnternet: Avusturya, Austrian Cyber Security Strategy (2013), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy, Son Erişim Tarihi: 12.11.2020.

İnternet: Belçika, Cyber Security Strategy .be (2012), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-

map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/view, Son Erişim Tarihi: 15.11.2020.

İnternet: Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı 2019-2023 Stratejik Planı, Web: https://www.btk.gov.tr/uploads/pages/yayinlar-stratejik-planlar/bilgi-teknolojileri-ve-iletisim-kurumu-2019-2023-stratejik-plani-published-revised-at-27-05-19.pdf, Son Erişim tarihi: 16.11.2020.

İnternet: Birleşmiş Milletler. (2019). Cyberspace. UNTERMS, Web: https://unterm.un.org/UNTERM/display/Record/UNHQ/NA/c328692 Son Erişim Adresi: 12.11.2010.

İnternet: Bulgaristan, National Cyber Security Strategy "Cyber Resilient Bulgaria 2020" Sofia, 2016, Web: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf, Son Erişim Adresi: 22.11.2020.

İnternet: CISCO. (2013). A Cisco Guide to Defending Against Distributed Denial of Service Attacks. Cisco Security Intelligence Operations, Web: http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html, Son Erişim Tarihi: 22.11.2020.

İnternet: Danimarka, Danish Cyber and Information Security Strategy (2018), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategy-for-cyber-and-information-security, Son Erişim Tarihi: 22.11.2020.

İnternet: Erdem, M. (2011). Anonymous ve Siber Ataklara Hukuksal bir Yaklaşım. Bilişim Hukuk, Web: http://www.bilisimhukuk.com/2011/06/anonymous-ve-siberataklara-hukuksal-bir-yaklasim/, Son Erişim Tarihi: 09.11.2020.

İnternet: Estonya, Cybersecurity Strategy Republic of Estonia (2019), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy, Son Erişim Tarihi: 9.11.2020.

İnternet: *Father of Cyberspace*, Web: http://www.wired.com/science/news/2009/03/dayintech_0317, Son Erişim Tarihi: 01.11.2020.

İnternet: Finlandiya, Finland's Cyber security Strategy (2013), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/finlands-cyber-security-strategy, Son Erişim Tarihi: 10.11.2020.

İnternet: Fransa, French National Digital Security Strategy (2015), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/information-systems-defence-and-security-frances-strategy, Son Erişim Tarihi: 10.11.2020.

İnternet: Güney Kıbrıs, Cybersecurity Strategy of the Republic of Cyprus (2012), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf/view, Son Erişim Tarihi: 7.11.2020.

İnternet: Hırvatistan, The National Cyber Security Strategy Of The Republic Of Croatia (2015), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/croatian-cyber-security-strategy, Son Erişim Tarihi: 28.11.2020.

İnternet: Hollanda, National Cyber Security Agenda A cyber secure Netherlands (2018), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1, Son Erişim Tarihi: 17.11.2020.

İnternet: Hürriyet, Türkiye siber saldırıların en çok artış gösterdiği ülkelerden biri, Web: https://www.hurriyet.com.tr/teknoloji/turkiye-siber-saldirilarin-en-cok-artis-gosterdigi-ulkelerden-biri-41711503, Son Erişim Tarihi: 12.02.2021.

İnternet: İngiltere, National Cyber Security Strategy 2016-2021, Web: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, Son Erişim Tarihi: 12.02.2021.

İnternet: İrlanda, National Cyber Security Strategy 2015-2017, Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf, Son Erişim Tarihi: 12.02.2021.

İnternet: İspanya, Natıional Cybersecurity Strategy (2019), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy, Son Erişim Tarihi: 12.02.2021.

İnternet: İsveç, A National Cyber Security Strategy (2017), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy, Son Erişim Tarihi: 09.11.2020.

İnternet: İtalya, The Italian Cybersecurity Action Plan (2017), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security, Son Erişim Tarihi: 09.11.2020.

İnternet: Letonya, Cyber Securıty Strategy Of Latvıa (2014), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss, Son Erişim Tarihi: 09.11.2020.

İnternet: Litvanya, National Cyber Security Strategy (2018), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/programme-for-the-development-of-electronic-information-security-cyber-security-for-2011-2019-2011, Son Erişim Tarihi: 09.11.2020.

İnternet: Lüksemburg, Luxembourgish National Cyber Security Strategy (2018), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite, Son Erişim Tarihi: 09.11.2020.

İnternet: Macaristan, Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary (2013), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf, Son Erişim Tarihi: 05.12.2020.

İnternet: Malta, Malta Cyber Security Strategy (2016), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta, Son Erişim Tarihi: 05.12.2020.

İnternet: OECD. (2009). Computer Viruses and Other Malicious Software: A Threat to the Internet Economy. OECD Publishing. Web: https://www.oecd.org/sti/ieconomy/computerviruses andothermaliciousoftwareathreattotheinterneteconomy.htm, Son Erişim Tarihi: 22.12.2020.

İnternet: Polonya, National Framework Of Cybersecurity Policy Of The Republic Of Poland For 2017-2022, Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013 Son Erişim Tarihi: 12.12.2020.

İnternet: Portekiz, National Capabilities Assessment Framework (2019), Web: https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf+&cd=3&hl=tr&ct=clnk&gl=tr, Son Erişim Tarihi: 14.12.2020.

İnternet: Romanya, Cyber Security Strategy of Romania (2013), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania, Son Erişim Tarihi: 14.12.2020.

İnternet: Sabah, Türkiye'ye 110 bin siber saldırı yapıldı! Peki ne kadarı başarı oldu?, Web: https://www.sabah.com.tr/ekonomi/2021/01/30/turkiyeye-110-bin-siber-saldiri-yapildi-peki-ne-kadari-basari-oldu, Son Erişim Tarihi: 18.12.2020.

İnternet: Slovakya, Cyber Security Concept of the Slovak Republic for 2015 – 2020 ,Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1, Son Erişim Tarihi: 18.12.2020.

İnternet: Slovenya, Cyber Security Strategy Establishing A System To Ensure A High Level Of Cyber Security (2015), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic, Son Erişim Tarihi: 17.12.2020.

İnternet: Statista, (2016). *Countries with the highest rate of malware infected computers as of 1st quarter 2016*. Statista.com, Web: http://www.statista.com/statistics/266169/highest-malware-infection-ratecountries/, Son Erişim Tarihi: 17.12.2020.

İnternet: Techinasia. (2017). *China Now Has 731 Million Internet Users, 95% Access From Their Phones*. Web: https://www.techinasia.com/china-731-million-internet-users-end-2016 Son Erişim Tarihi: 17.12.2020.

İnternet: Threatmap, Live Cyber Threat Map, Web: https://threatmap.checkpoint.com/, Son Erişim Tarihi: 17.12.2020.

İnternet: Türkiye (1), Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Web: https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, Son Erişim Tarihi: 17.12.2020.

İnternet: Türkiye (2), 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, Web: https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, Son Erişim Tarihi: 17.12.2020.

İnternet: Türkiye (3), Ulusal Siber Güvenlik Stratejisi 2020 – 2023, Web: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/NationalCybersecurityStrategyOfTURKEY.pdf, Son Erişim Tarihi: 17.12.2020.

İnternet: Uluslararası Telekomünikasyon Birliği (2008). ITU Botnet Mitigation Toolkit. Cenevre: Uluslararası Telekomünikasyon Birliği, Web: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html, Son Erişim Tarihi: 18.12.2015.

İnternet: Yıldırımoğlu, M. (2015). Yarattığı Virüs ile Internet'i Felç Eden Adam. Muratyildirimoglu, Web: http://muratyildirimoglu.com/makaleler/hacker1.htm, Son Erişim tarihi: 10.01.2021.

İnternet: Yunanistan, Greek National Cyber Security Strategy (2017), Web: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view, Son Erişim tarihi: 10.01.2021.

Kahraman S.; Kutlu, Ö. ve Dinçer, S. (2019). *Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Politikalarının Analizi*. ASSAM Uluslararası Hakemli Dergi, 1 – 14.

Kara, M. (2013). *Siber Saldırılar – Siber Savaşlar ve Etkileri*. Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 40-41.

Karaarslan, E. (2013). *Siber Güvenlik Deneyleri için Ağ Benzetici ve Ağ Sınama Ortamlarının Kullanımına Dair Ön İnceleme*. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisleri Dergisi, 6 (1), 1-9.

Karluk, S. R. (1996), *Avrupa Topluluğu ve Türkiye*, 4. Baskı, İstanbul Menkul Kıymetler Borsası Yayınları, İstanbul.

Kaya, H. P. (2019). *Türkiye'de denetim alanında yazılmış olan doktora tezlerinin değerlendirilmesi (1995-2018)*. Karabük Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 9 (2). 556-576.

Kıral, B. (2020). *Nitel Bir Veri Analizi Yöntemi Olarak Doküman Analizi*. Siirt Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 8 (15), 170-189.

Kıral, B. ve Çilek, A. (2020). *2023 Vizyon Belgesi'nin karakter eğitimi bakımından değerlendirilmesi*. Milli Eğitim Dergisi. 49(225), 5-22.

Kıratlı, O. S. (2016). *Avrupa Dış İlişkiler ve Güvenlik Politikası ve Üç Büyükler: Almanya, Fransa ve İngiltere*. Akademik İncelemeler Dergisi, 11(1), 207-224.

Klimburg, A. (2012). *National Cyber Security Framework Manual*. Tallin: NATO CCD COE Publications.

Korkmaz, M. (2018). *Avrupa Merkez Bankası Politikalarının Seçilmiş Avrupa Birliği Üyesi Ülkelere ve Türkiye'ye Etkisi*. Yayımlanmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.

Labuschagne, A. (2003). *Qualitative research: Airy fairy or fundamental?* The Qualitative Report, 8(1).

Levine, J. R. (2016). Written Comments of Dr. John R. Levine. commerce.senate, Web: http://www.commerce.senate.gov/pdf/levine032304.pdf, Son Erişim Tarihi: 09.11.2020.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. United States of America: RAND Corporation, 12-13.

Lord, K. M. (2011). *America's Cyber Future: Security and Prosperity in the Information Age (Volume II)*. Zurich: Center for New American Studies.

Mahmutoğlu, F. S. (2002). *Karşılaştırmalı Hukuk Bakımından İnternet Sürelerinin Ceza Sorumluluğu*. İ.Ü. Hukuk Fakültesi, Ceza Hukuku ve Kriminoloji Araştırma ve Uygulama Merkezi'nde yapılan, "İnternet Ortamında Ceza Sorumluluğu" konulu panelde sunuldu. İstanbul.

Merriam, S. B. (2009). *Qualitative research. A guide to design and implementation*. San Francisco: John Wiley-Sons.

Mills, J., Bonner, A. ve Francis, K. (2006). T*he development of constructivist grounded theory*. International Journal of Qualitative Methods, 5(1), 25– 35.

Nickolov, E. (2008). *Modern Trends in the Cyber Attacks against the Critical Information Infrastructure*. Modern Trends in the Cyber Attacks against the Critical Information Infrastructure ss. 1-95.

O'Hara, G. (2010). *Cyber-Espionage: A Growing Threat to the American Economy*, 19 Comlaw Conspectus, 241.

Özbay, R. (2015). *Aktif Siber Savunma Teknikleri ve Performans Analizi*. Yayınlanmış Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü Afyon Kocatepe Üniversitesi, Afyon.

Page, E. (2000). *Theorizing The Link Between Environmental Change and Security.* Rewiew of European Community & İnternational Environmental Law, 9 (1): 33-43.

Park, M. (2018). *Let's learn about enemy through various IoCs of real APT cases*. In DragonCon 2018, Dec 8, 2018. Dragon Threat Labs.

Qasimov, C. ve X. Bağırov (2008). *Azərbaycan Təhlükəsizlik Orqanlarının Qısa Tarixi* – Dərslik, Azərbaycan Respublikası Milli Təhlükəsizlik Nazirliyinin Heydər Əliyev Adına Akademiyası, Bakı: MTN`in Nəşriyyatı.

Rehber, (2020), *Bilgi ve İletişim Güvenliği Rehberi,* Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Ankara.

Rehber, (2021), *Bilgi ve İletişim Güvenliği Denetim Rehberi,* Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Ankara.

Roy, J. (2007). *Reflections On The Treaty Of Rome And Today's EU*. Jean Monnet/Robert Schuman Paper Series. S.1-10

Schreier ,F. (2015). *On Cyberwarfare*. DCAF Horizon 2015 Working Paper No.7, 61.

Stafford, T. F. ve Urbaczewski, A. (2004). *Spyware: The Ghost in the Machine*. Communications of the Association for Information Systems, 14, 291-306.

Stake, R. E. (1995). *The art of case study research*. Thousand Oaks: Sage

Şahin, Y. (2017). *Brexit ve Trump Çağında AB Güvenlik ve Savunma Politikaları*. İstanbul: İktisadi Kalkınma Vakfı.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2013). U*lusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*, Ankara.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2016). *2016-2019 Ulusal Siber Güvenlik Stratejisi*, Ankara.

TBD (2015). *Siber Güvenlik ve Kritik Altyapı Güvenliği Çalışma Grubu Nihai Raporu*, Türkiye Bilişim Derneği, Ankara.

TBMM (2016. *Bilgi Güvenliği ve Bilişim Suçları Üçüncü Kısım*. TBMM, Ankara.

Terriff, T., Croft, S., James, L., and Morgan, P. M. (1999). *Security Studies Today*.Cambridge: Polity Press.

Uluslararası Telekomünikasyon Birliği (2008). X.1205: Overview *of cybersecurity*. Cenevre: Uluslararası Telekomünikasyon Birliği.

Ünver, M., Canbay, C., ve Mirzaoğlu, A. G. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Bilgi Teknolojileri Üst Kurulu, Ankara.

Varlık, A. B. (2015). *Ulusal Güvenlik. Milli Güvenlik Teorisi*, Ed.: Ümit Özdağ, Ankara: Kripto Yayınları.

Wach, E., and Ward, R. (2013). *Learning about qualitative document analysis*. IDS Practice Paper in Brief, 13, 1-11.

Wiener, N. (1965). Cyb*ernetics, Second Edition: or the Control and Communication in the Animal and the Machine*. Cambridge: The MIT Press.

WP (2016). *White Paper on German Security Policy and The Future of the Bundeswehr*. The Federal Government, Germany.

Yin, R. K. (1994). *Case study research: Design and methods*. Thousand Oaks: Sage.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	:	ARINMIŞ UZUN, Sündüs
Uyruğu	:	T.C.

Eğitim Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Yüksek lisans	Gazi Üniversitesi/ Adli Bilişim	Devam ediyor
Lisans	Karadeniz Teknik Üniversitesi/ Elektrik-Elektronik Mühendisliği	2014
Lise	Etimesgut Lisesi / Fen Bilimleri	2006

İş Deneyimi

Yıl	**Yer**	**Görev**
2019-Halen	Özel Sektör	Siber Güvenlik Uzmanı
2017-2019	Özel Sektör	Siber Güvenlik Teknolojileri Uzmanı

Yabancı Dil
İngilizce

Yayınlar

Uzun, S. A. Türkiye'de Kişisel Verilerin Korunması ve Vatandaş Algısının Ölçülmesi. *Bilişim Teknolojileri Dergisi*, 14(3), 207-221.

Tezden Üretilen Yayınlar

Çakır, H. ve Uzun, S. A. (2021). Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi*, 7(2), 355-381.

Hobiler

Kayak yapmak, yürüyüş yapmak, voleybol oynamak, yüzmek, müzik dinlemek, kitap okumak

GAZİLİ OLMAK AYRICALIKTIR...