T. C.
MARMARA ÜNİVERSİTESİ
AVRUPA BİRLİĞİ ENSTİTÜSÜ

AVRUPA BİRLİĞİ SİYASETİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

AVRUPA BİRLİĞİ'NİN SİBER GÜVENLİK POLİTİKASI

YÜKSEK LİSANS TEZİ

MEHMET EREN

İSTANBUL - 2016

T. C.
MARMARA ÜNİVERSİTESİ
AVRUPA BİRLİĞİ ENSTİTÜSÜ

AVRUPA BİRLİĞİ SİYASETİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

AVRUPA BİRLİĞİ'NİN SİBER GÜVENLİK POLİTİKASI

YÜKSEK LİSANS TEZİ

MEHMET EREN

Danışman: DOÇ. DR. E. MÜNEVVER CEBECİ

İSTANBUL - 2016

T.C.
MARMARA ÜNİVERSİTESİ
AVRUPA BİRLİĞİ ENSTİTÜSÜ

ONAY SAYFASI

Enstitümüz AB Siyaseti ve Uluslararası İlişkiler Anabilim Dalı Türkçe / İngilizce Yüksek Lisans Programı öğrencisi Mehmet EREN'in ***"AVRUPA BİRLİĞİ'NİN SİBER GÜVENLİK POLİTİKASI"*** konulu tez çalışması 19/09/2016 tarihinde yapılan tez savunma sınavında aşağıda isimleri yazılı jüri üyeleri tarafından ~~OYBİRLİĞİ~~ / OYÇOKLUĞU ile BAŞARILI bulunmuştur.

Onaylayan:

Doç. Dr. E. Münevver CEBECİ Danışman .....

Doç. Dr. Salih BIÇAKCI Jüri Üyesi .....

Yrd. Doç. Dr. İbrahim MAZLUM Jüri Üyesi .....

Onay
Prof. Dr. Mazaffer DARTAN
Müdür

22.09.2016 Tarih ve 2016/21 Sayılı Enstitü Yönetim Kurulu kararı ile onaylanmıştır.

ÖZET

Bilgi ve iletişim teknolojilerindeki gelişme ile önem kazanan siber güvenlik ve AB'nin geliştirmiş olduğu siber güvenlik politikası çalışmanın ana temasını oluşturmaktadır. Geleneksel güvenlik tanımına ek olarak kapsamlı siber güvenlik tanımı ile başlayan çalışmada, siber güvenlik, Barry Buzan ve Ole Wæver'ın başını çektiği Kopenhag Ekolünün gündeme getirdiği güvenlikleştirme kavramı ile teorik çerçeveye oturtulmuştur. Çalışmada oltalama, kötücül yazılım, botnet, hizmeti engelleme ve sosyal mühendislik saldırı türlerinde örneklerle siber saldırı tekniklerine değinilmiştir. Çalışmada ayrıca gelişmiş kalıcı tehdit saldırılarına (APT) da değinilmiştir. Avrupa Birliği'ni etkileyen siber saldırı örnekleri olarak Alman Parlamentosuna yapılan siber saldırılar, Estonya örneği ve TV5 Monde örneği incelenmiştir. AB'nin siber güvenlik politikasının temelini oluşturan "Avrupa Birliği için Siber Güvenlik Stratejisi" belgesi ile birliğin ortak siber güvenlik politikası kapsamında gerçekleştirdiği ve gerçekleştirmeyi öngördüğü temel politikalar ve yol haritaları çalışmanın ana konusunu oluşturmuştur. Bu kapsamda AB'nin belirlemiş olduğu "siber güvenliğin hedefleri", "stratejik öncelikler ve eylemler", ile "roller ve sorumluluklar" detaylı olarak incelenmiştir. Tezin ana argümanı, AB siber güvenlik politikalarının tüm dünyada göze çarpan ve örnek unsurları içerdiği, etkin ve kararlı bir siber güvenlik politikasının AB kurumları, üye devletlerin yetkili politika yapım mercileri ve ortak paydada buluşulmuş uluslararası ortaklıklar ile oluşturulacak koordinasyon sayesinde geliştirilebileceği, ancak bu işbirliğinin AB'de henüz sağlanmadığıdır.

Anahtar Kelimeler: Güvenlikleştirme, Siber Güvenlik, AB'nin Siber Güvenlik Politikası, ENISA, Europol, OGSP.

ABSTRACT

The subject of this thesis is the EU's cyber security policy. Cyber security gets more important with advancements in information and communications technology. The thesis starts with the traditional definition of security and gives a comprehensive explanation of cyber security. The conceptual framework of this thesis is securitization, a concept developed by the Copenhagen School, especially by Ole Wæver and Barry Buzan. In this study, phishing, malware, botnets, denial of service and social engineering attacks are discussed as cases of the types of cyber attacks. In addition, cyber attacks of APT (Advanced Persistent Threat) are examined. Cyber-attacks on the German parliament, Estonia and TV5 Monde are examined as examples of cyber attacks that affected the European Union. "Cybersecurity Strategy of the European Union" is the basis of the EU's cyber security policy. This thesis throughly examines the major goals and policies/actions that this strategy outlines. In this context, "cyber security objectives of the EU", its "strategic priorities and actions", and its "roles and responsibilities" are analyzed in detail. The major argument of this thesis that the EU cyber security policies and examples include prominent element in the whole World and the EU can only have an effective cyber security policy through a comprehensive approach which involves cooperation with the academia, member states and the private sector (NGOs and multinational companies), but this cooperation in the EU has not yet been provided.

Key Words: Securitization, Cyber Security, Cyber Security Policy of the EU, ENISA, Europol, CSDP.

İÇİNDEKİLER

ŞEKİL LİSTESİ

KISALTMA LİSTESİ

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AFID	The Air Force Intelligence Directorate
BfV	Federal Anayasayı Koruma Dairesi
BİT	Bilgi ve İletişim Teknolojileri
BM	Birleşmiş Milletler
CEF	Bağlantılı Avrupa Kuruluşu
EC3	Avrupa Siber Suçlar Merkezi
EDA	Avrupa Savunma Ajansı
EFMS	Üye Devletler için Avrupa Forumu
ENISA	Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı
EP3R	Esneklik için Avrupa Kamu-Özel Ortaklığı
EPCIP	Avrupa Kritik Altyapılarının Korunması Programı
GCHQ	Government Communications Headquarters
GSD	General Security Department
ITU	Uluslararası Telekomünikasyon Birliği
NATO	Kuzey Atlantik Antlaşması Teşkilatı
NIS	Ağ ve Bilgi Güvenliği
NSA	National Security Agency
OECD	Avrupa Ekonomik İşbirliği Örgütü
OGSP	Ortak Güvenlik ve Savunma Politikası
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
SCADA	Supervisory Control and Data Acquisition

GİRİŞ

Bilgi ve iletişim teknolojileri alanında gündemde olan gelişmeler, sağladığı olanaklar ve dünyaya sunduğu yenilikler ile revaçta olan bir konu haline gelmektedir. Bu gelişmelerle birlikte, bu alan bize işlemciler ve bunları kontrol edenlerin bulunduğu internet, iletişim ağları ve bilgisayar sistemlerini de içine alan, birbirine bağlı bilgi teknolojileri altyapılarından oluşan siber uzayın kapılarını açmaktadır.

Günümüz dünyasında bilişim sektöründeki ilerleme ve gelişmelere bağlı olarak, teknoloji ve bilimde kullanılan teçhizat ve donanımsal araçların geliştirilmesiyle dijital ortamda yapılabilecek eylemler de genişlemektedir. Dolayısıyla geliştirilen yazılımların açık noktalarından sistemlere sızmalar ve mevcut sistemleri sabote etmeler baş gösterebilmektedir. Bunların başında da siber saldırılar gelmektedir. İnternetin sosyal ve iktisadi yaşantının olmazsa olmazı haline gelmesi ve birbirinden ayrılamaz bir şekle dönüşmesi, ülkelerin de bilgi ve iletişim sahasındaki önemli seviyedeki gelişmelere ilgisiz kalmamasına sebep olmaktadır. Bunun sonucu olarak da mevcut fiziki ortamlarda gerçekleştirilen iş ve eylemlerin sanal ortamlara taşınmasına, hizmetlerin ve ihtiyaçların fiziki mekân ihtiyacı olmadan karşılanmasına yol açan, fakat bununla birlikte de farklı tehdit algılarının da oluşmasına sebep olan önemli bir sürece girilmektedir.

Bilgi ve iletişim teknolojileri (Information and Communication Technologies — ICT) günümüz dünyasında iletişimin artmasını ve sistemlerin hızlanmasını sağlamaktadır. Bu, bir yandan hayatın birçok alanında yenilikler sunan bir düzen oluştururken, aynı zamanda güvenlik zafiyetlerini de beraberinde getirmiştir. Siber uzayda da tarafların çıkarlarının örtüşmediği durumlarda taraflar meşru olmayan yöntemlere başvurulabilmektedir. Ayrıca, çoğu zaman tarafların geliştirdiği siber silahlar ve teknolojiler ile karşılıklı güç mücadelesi oluşması söz konusu olabilmektedir. Siber saldırılara karşı geliştirilen politika ve araçlar siber uzayda güç mücadelesine de sebep olabilmektedir. Bu mücadele de iktisadi, ekonomik, sosyal ve siyasi hayatı büyük ölçüde zarara uğratabilecek siber savaşlara neden olabilmektedir. Dolayısıyla insanlar ve devletler tehlikeyle yüz yüze gelmekte ve farklı zamanlarda farklı tehdit algılarının oluşması gündeme gelmektedir.

Siber uzay, uluslararası ilişkilerin şekillenmesinde ve taraf olmada yeni bir alan olarak karşımıza çıkmaktadır. Bu alandaki üstünlük mücadelesi devletleri zaman zaman karşı karşıya zaman zaman da ―ortak politikalar oluşturabilmek için― bir araya getirmektedir. Uluslararası aktörler, siber uzayda da belirleyici olmak, olası tehditleri önleyebilmek için hızla büyüyen bilişim sektörüne dikkat çekmektedirler. Ekonomik ve sosyal düzenin sürekliliğini sağlayan sistemlere karşı oluşabilecek zararlı müdahalelere önlem almaya çalışmaktadırlar.

Birleşmiş Milletler, NATO, AGİT gibi uluslararası örgütler kendi bünyelerinde farklı çalışma grupları ve komiteler oluşturarak siber güvenlik çalışmalarına önem vermekte ve gelişmeleri yakından takip ederek olası tehditlere karşı alınabilecek önlemleri araştırmaktadırlar.[1] Devletlerin ulusal güvenliğini de tehdit edecek seviyeye gelen siber saldırılara karşı alınan ve uygulamaya konulmaya çalışılan önlemlerin varlığı bu çalışmaya esin kaynağı olmuştur. Çalışmada, Avrupa Birliği'nin oluşturmaya çalıştığı politikalarının niteliği değerlendirilmektedir. Bununla birlikte siber tehditlerin önüne geçmek konusunda karşılaşılan sorunlar ve AB'nin siber güvenliği sağlamaya yönelik geliştirdiği politikaların sonuçları ve müşterek bir siber güvenlik politikası meydana getirme çalışmaları incelenmektedir. Politika yapım süreci, birçok yasal ve pratik sorumluluğu da beraberinde getirdiği için bu çalışmanın temelini oluşturmaktadır. Tezin amacı, Avrupa Birliği'nin siber güvenlik politikasını güvenlikleştirme perspektifinden değerlendirerek, politikalarının hangi temellere dayanarak ve nasıl oluştuğunu tespit etmektir.

Araştırma evrenini uluslararası konjonktürdeki siber güvenlik oluştururken örneklem ise Avrupa Birliği'nden oluşmaktadır. Çalışma, daha iyi bir analiz çerçevesi sunabilmek için Avrupa Birliği'nin siber güvenlik politikası ile sınırlandırılmıştır. Tezin

[1] "Birleşmiş Milletler Genel Kurulunda siber güvenlik ile ilgilenen üç farklı komite (the Disarmament and International Security Committee; the Economic and Financial Committee; and the Social, Humanitarian and Cultural Committee) bulunmaktadır. Bu komiteler konunun farklı açılarını ele alan karar tasarıları sunmaktadırlar. NATO kendi ağına yönelik siber tehditlerin varlığını ilk olarak 2002 Prag zirvesinde kabul etmiş ve bu çerçevede NATO Bilgisayar Olaylarına Müdahale Kapasitesini (NCIRC) oluşturmuştur. 2008 Bükreş zirvesinde siber güvenlik alanında savunma politikasının genel çerçevesi oluşturulmuş, 2011 yılında kabul edilen politika belgesi siber güvenlik alanında daha etkili ve merkezi bir yapılanmanın oluşmasını sağlamıştır. Siber güvenlik alanında bir dizi güven artırıcı önlem (GAÖ) alınması amacıyla Güvenlik Komitesi altında gayrı resmi bir çalışma grubu oluşturulmuş ve 2013 yılında ülkemizin de katılım sağladığı toplantılar sonucu ilk grup GAÖ'ler listesi tespit edilmiştir. Söz konusu liste Sınır aşan tehditlerle mücadele alanında AGİT'in Çabalarının Güçlendirilmesi başlıklı deklarasyonla 2013 Kiev Bakanlar Konseyi'nde kabul edilmiştir" (Uluslararası Telekomünikasyon Birliği, 2015; Meral, 2015)

ana konusunu AB'nin siber güvenlik politikası ile buna yönelik oluşturan eylemleri ve özellikle AB'nin siber güvenlik stratejisi oluşturmaktadır. Bu bağlamda üye devletlerin siber güvenlik politikalarına bu tezde sadece yeri geldiğinde değinilmektedir.

Bu çalışmada siber güvenlik, Barry Buzan ve Ole Wæver tarafından teorileştirilen güvenlikleştirme (securitization) kavramı temelinde değerlendirilmiştir. Bu çerçevede, siber güvenlik algısının AB'de oluşumu ve politika yapım sürecine yansıması, tam bir güvenlikleştirme zemininin varlığını ifade etmektedir. Siber güvenlik, kuramsal anlamda temel olarak tek bir teori ve yaklaşımla açıklanamamakla birlikte konunun kapsamı ve politikaların uygulanma şekli bakımından güvenlikleştirme kavramı ile değerlendirilebilir durumdadır.

Çalışmanın cevap aradığı temel soruları ise şu şekilde sıralamak mümkündür:

"AB'nin siber güvenlik anlayışı nasıl şekillenmektedir?",

"AB'de siber güvenlik ile ilgili söz edimi nasıl gerçeklemektedir?",

"AB'nin siber uzayı güvenlikleştirmesine dair en önemli belge olan siber güvenlik stratejisinin hedefleri ile AB'nin geliştirdiği politikalar uyumlu mudur?",

"AB'nin siber güvenlik politikası etkili bir politika mıdır?".

Yukarıdaki sorulardan yola çıkılarak değerlendirilen strateji belgesi ve politikalar kapsamında bu tezin ana argümanı AB siber güvenlik politikalarının tüm dünyada göze çarpan ve örnek unsurları içerdiği, etkin ve kararlı bir siber güvenlik politikasının AB kurumları, üye devletlerin yetkili politika yapım mercileri ve ortak paydada buluşulmuş uluslararası ortaklıklar ile oluşturulacak koordinasyon sayesinde geliştirilebileceği, ancak bu işbirliğinin AB'de henüz sağlanmadığıdır.

Tezde Avrupa Birliği'nin siber güvenlik politikası öncelikle kavramsal ve teorik çerçeveye oturtularak, resmi belgeler ışığında, bu konuda yayınlanmış akademik çalışmalardan da faydalanılarak değerlendirilmektedir. Yöntem olarak, çalışmada kullanılan birincil ve ikincil kaynakların analizi büyük önem taşımaktadır. Özellikle komisyon raporları, Birlik bildirgeleri, yeşil kitaplar gibi birincil kaynakların çalışmada kullanılması daha iyi bir değerlendirme yapabilmek adına önem arz etmektedir.

Çalışmadaki soruları yanıtlamak ve varsayımları sınamak için, Avrupa Birliği tarafından, resmi kurumlar aracılığı ile yayınlanan raporlar, bildiriler ve akademik çalışmalar incelenmiş ve ilgili veriler derinlemesine değerlendirilmiştir. Kapsamlı bir literatür çalışması sonucunda seçilen ikincil kaynaklar da yoğun bir şekilde kullanılmıştır.

Tez, üç ana bölüme ayrılmıştır. Birinci bölümde geleneksel güvenlik kavramından yola çıkılarak, siber uzay, siber casusluk, siber terörizm ve siber güvenlik gibi kavramlar irdelenmiştir. Bu bölümde güvenlik algısının değişimi ve güvenlikleştirme kuramı açıklanarak, siber güvenliği anlamlandırmakta nasıl kullanılabileceği ortaya konulmuştur. Güvenlikleştirme etrafında temellendirilen siber güvenlik politikalarının analizi de ilk bölümün konusunu oluşturmaktadır.

İkinci bölümde siber saldırı teknikleri ve günlük hayatta karşılaşılan örnekleri sunulmuştur. Ayrıca bir siber saldırı tekniği olmamakla birlikte devletler için önemli bir tehdit olan gelişmiş kalıcı tehdit (Advanced Persistent Threat—APT) saldırılarına da yer verilmiştir. Siber suç tanımlaması yapılarak bu olgunun uluslararası düzeydeki örnekleri verilmiş ve bu bağlamda oluşan gündem incelenmiştir. Avrupa Birliği'nin siber güvenlik politikasının oluşmasında ve etkili bir gelişim göstermesinde AB üyesi devletleri doğrudan etkileyen siber saldırı örnekleri olarak, Estonya saldırıları, Alman Parlamentosuna yapılan saldırılar ve TV5 Monde örnekleri değerlendirilmiştir.

Üçüncü bölümde ise tezin ana konusunu oluşturan AB'nin siber güvenlik politikaları, AB kurumları tarafından yayınlanan raporlar, bildiriler ve eylem planları çerçevesinde analiz edilerek sunulmuştur. Burada ana kaynağı AB'nin Siber Güvenlik Strateji Belgesi oluşturmaktadır. AB'nin ortak siber güvenlik politikasının oluşumuna nasıl gidildiği ve bu sürecin nasıl şekillendiği, konuya AB'nin ve AB'ye üye devletlerin yaklaşımları ile birlikte verilmiştir. AB'nin yayınlamış olduğu dokümanlar üzerinden nasıl bir siber güvenlik politikasının oluşturulmaya çalışıldığı, atılan adımlar ve pratik hayattaki uygulamalar bu kısımda sunulmuştur. Bu bölümün alt başlıkları AB'nin siber güvenlik stratejisi belgesi alt başlıkları ile uyumlu olarak belirlenmiştir.

Sonuç bölümünde çalışmaya ilişkin olarak ulaşılan sonuçlara yer verilmiştir. Bu bağlamda ilk bulgu, Kopenhag Ekolünün güvenlikleştirme perspektifinden siber güvenlik analizinin mümkün olduğu, siber uzayın güvenlikleştirilmesindeki rollerin ve sorumlulukların AB'deki roller ve sorumluluklarla örtüştüğüdür. İkinci olarak, AB'nin

siber güvenlik stratejisinin tek başına etkin ve yeterli bir politika olmadığı, etkinliğin ve etkililiğin gerek AB içinde daha fazla tutarlılık ve uyum, gerekse uluslararası koordinasyon ve işbirliği ile gerçekleştirilebileceği sonucuna varılmıştır.

1. BÖLÜM

KAVRAMSAL VE KURAMSAL ARKA PLAN: GÜVENLİK VE SİBER GÜVENLİK

Bu bölümde çalışmanın temellerini oluşturan güvenlik, siber uzay, siber casusluk, siber terörizm ve siber güvenlik gibi kavramlar irdelenerek, çalışma güvenlikleştirme temelinde kuramsal bir zemine oturtulmuştur. İlk olarak güvenlik kavramının dönüşümü, siber güvenlik gibi yeni bir güvenlik sektöründe ortaya çıkan tehditleri daha iyi anlayabilmek için çalışmada temel teorik çerçeve olarak kullanılan güvenlikleştirme kavramına temel oluşturacak şekilde kısaca tarihsel perspektiften anlatılmıştır. Ayrıca çalışmanın kuramsal zeminin oturduğu güvenlikleştirme kavramı detaylı şekilde irdelenmiştir. Kopenhag Ekolünün güvenlik kavramının analizinde kullandığı beş sektör (askeri güvenlik, siyasi güvenlik, ekonomik güvenlik, toplumsal güvenlik ve çevresel güvenlik) siber güvenliğin günümüzde yeni bir güvenlik sektörü olarak görülüp görülemeyeceği değerlendirmelerini anlamak ve bu güvenlik alanının diğer sektörlerle iç içe geçmişliğini göstermek amacıyla örneklerle açıklanmıştır.

Çalışmaya temel oluşturması açısından siber güvenlik kavramı da bu bölüme dâhil edilmiş olup; siber güvenlik, kavramsal çerçevesi ve içerdiği gizlilik, bütünlük ve erişilebilirlik unsurları ile birlikte anlatılmıştır. Ayrıca 2. Bölüm'de anlatılan siber saldırı teknikleri ve siber güvenlik uygulama örneklerine kavramsal çerçeve sunulması açısından siber güvenliğin anlatılmasının yararlı olacağı düşünülmüştür. Bölümün sonunda ise siber güvenlik ve güvenlikleştirme ilişkisi verilerek, çalışma için kavramsal ve kuramsal zemin hazırlanmıştır. Bu bölümde Kopenhag Ekolünün siber uzaya bakışı ve ayrı bir sektör olarak değerlendirmesine yer verilmiştir.

1.1. Güvenlik Kavramının Analizi

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). Bu bağlamda güvenlik kavramının tarihsel süreç içerisindeki dönüşümünden kısaca bahsetmekte fayda olacaktır.

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). Soğuk Savaş döneminde uluslararası ilişkiler disiplininin altında bir alan olarak incelenen güvenliğe yaklaşım, askeri tehdit merkezli olmuş ve askeri güç perspektifinde değerlendirilmiştir (Baldwin, 1995: 119). Bu dönemde incelenen farklı güvenlik temalarının varlığından da söz etmek mümkündür. Güvenliğin sadece askeri güvenlik alanında değil farklı alanlarda düşünülmesi gereği duyulmuştur. Bu alanlar toplumsal, politik ve iktisadi alanlardır. Silahlanma yarışının had safhaya çıktığı bu dönemlerde devletlerin ulusal güvenliğinin askeri boyutunun yanında askeri olmayan yönlerin de göz ardı edilmeden değerlendirmeye tabi tutulması gerekliliği vurgulanmıştır. Demokratik süreçler, sivil özgürlükler, ekonomi alanında özgürlük, iktisadi bağımsızlık, iç politika ve güvenlik arasındaki ilişkilere de atıflar yapılmıştır (Baldwin, 1995: 122).

1970'ler ve 1980'lerde dünya çapında yaşanan ve küresel etkileri olan olaylar, güvenlik kavramının değerlendirilmesini ve tanımını da değiştirmiştir. Nitekim bu süreçte gerçekleşen 1979 İran Devrimi ve aynı yıl Afganistan'ın SSCB (Sovyet Sosyalist Cumhuriyetler Birliği) tarafından işgal edilmesi, SSCB ve ABD'nin Avrupa'ya orta menzilli füze sistemlerini yerleştirmesi, Reagan tarafından 1983 yılında başlatılan yıldız savaşları çerçevesinde oluşturulan Stratejik Savunma Girişimi gibi konseptlerin oluşturulmasıyla nükleer silahlanma yarışı tekrar gündeme gelmiştir. Bu gelişmeler ile birlikte uluslararası ilişkiler disiplinindeki güvenlik arayışları farklı perspektiflere yönelimlere sebep olmuştur. Richard H. Ullman ve Barry Buzan gibi güvenlik çalışan analizciler güvenliği yeniden tanımlamaya ve alanını genişletmeye başlamışlardır. Ullman (Ullman, 1983) ve Buzan (Buzan, 1983) eserleriyle güvenlik çalışmalarında yeni bir dönemin başlangıcını oluşturmuşlardır.

Ullman, çalışmalarında toplam güvenliği etkileyen unsurlar olarak askeri güvenliğin dışında kalan alanları da vurgulamıştır (Ullman, 1983: 129-135). Bir devletin ulusal askeri güvenliğinin en yüksek seviyede olmasının devletlerin sadece bu alana konsantre olmasına ve ekonomik ve sosyal alanlarda çok geride kalmasında sebep olduğunu vurgulamıştır. Diğer bir deyişle sadece askeri güvenliğe önem verilmesi sonucunda devletlerin toplam güvenliğinin negatif yönlü olacağına dikkat çekilmiştir. Ayrıca aşırı silahlanmanın ve askeri güvenliğe olan yatırımların artmasının küresel

güvensizliğe sebep olacağına ve bu yarışın bir sonunun olmayacağına dikkat çekmiştir. Ullman güvenliği amaç olarak değil sonuç olarak düşünmüştür (Ullman, 1983: 133). Bu bağlamda güvenlik tehdidini iki kategoride incelemiştir. İlk kategoride, güvenlik tehdidinin bir devlette yaşam kalitesinin düşmesi olarak nitelendirmiş ve bunun sebebinin bir savaş olabileceği gibi salgın bir hastalık ya da ülke içinde çıkan bir isyanın olabileceğine vurgu yapmıştır (Ullman, 1983: 133). İkinci kategoride tehdit, hükümet dışı birimlerin hükümetlerin hareket alanını daraltması, politika seçeneklerini azaltması olarak tanımlanmıştır (Ullman, 1983: 133). Ullman, bu tehdidin devlet içindeki bireylerden ve gruplardan gelebileceğini belirtir (Ullman, 1983: 133). Burada dikkat çeken nokta, Ullman'ın güvenliği devlet üzerinden tanımlamış olmasıdır – yani güvenliğin başvuru nesnesi devlettir.

Soğuk savaş dönemindeki dünya düzeninde nükleer savaş tehdidinin varlığı ve çift kutupluluk (bipolarity), dehşet dengesi (balance of terror), güç dengesi (balance of power) ve caydırıcılık (deterrence) gibi konuları gündeme taşımıştır. Görüldüğü üzere bu konular yoğunluklu olarak askeri güvenlik konularıdır. Ancak Soğuk Savaş döneminde güvenliğin tanımının genişletilmesine sebep olacak başka gelişmeler de yaşanmıştır. Dünyanın kuzeyindeki zengin ülkeler ile güneyindeki fakir ülkelerin arasındaki uçurumun giderek açılması, özellikle 1980'lerde güvenliğin başka boyutlarıyla da ele alınmasına neden olmuştur. 1982 Palme Komisyonu Raporu'nun güvenliğin sosyo-ekonomik ve siyasi yönlerine dikkat çekmesi bu dönem güvenlik anlayışının genişlemiş olmasının örneklerinden biridir. Bu dönemde Barry Buzan da güvenlik kavramını genişleten bir yaklaşımla güvenliği yeniden değerlendirmiştir.

Buzan, 1983'te (Buzan, 1983) yayınladığı ve 1991'de (Buzan, 1991) tekrar revize edilmiş halini güvenlik çalışmalarına kazandırdığı "People, States and Fear" isimli eseri ile literatürde bir çığır açarak güvenliği devletler arasındaki askeri ilişkilerin yanı sıra bireyler ve toplumlar arasındaki refahı, ulusun kalkınmasını da kapsayacak kavramsal bir çerçeveye oturtmuştur. Buzan ve Kopenhag Ekolündeki arkadaşlarının yaklaşımı güvenlik tartışmalarında, güvenliğin sadece klasik askeri güvenlik alanını kapsamasını savunanlar ve devlet dışı aktörler çerçevesinde değerlendirilmesini savunanlar arasında 'üçüncü yol' olarak ortaya çıktığı söylenebilir (Buzan ve Wæver, 2003). Bu çerçevede, Kopenhag Ekolü beş farklı güvenlik sektöründen söz etmektedir: Askeri, siyasi, toplumsal, ekonomik ve çevresel sektörler. Kopenhag Ekolünün güvenlik yaklaşımı

sektörel analizle sınırlı kalmamış, Ekolün bir diğer üyesi Ole Wæver'ın geliştirdiği güvenlikleştirme kavramı güvenlik çalışmalarında en sık kullanılan terimlerden biri haline gelmiştir. Bu tez de güvenlikleştirme kavramı üzerinden siber güvenlik olgusunu açıklamaya çalışmaktadır. Bu bağlamda, çalışmanın teorik çerçevesini oluşturan güvenlikleştirme kuramının, Kopenhag Ekolü ve güvenlik çalışmaları kapsamında değerlendirilmesinde fayda olacaktır.

1.2. Kopenhag Ekolü ve Güvenlik Çalışmaları[2]

Güvenliğin 'esası tartışılan' bir kavram olarak nitelendirilmesi, aynı zamanda bu kavramın öznelliğine ve farklı şekillerde anlaşılmasına da mahal vermektedir. Buzan ve Wæver'ın başını çektiği Kopenhag Ekolüne göre güvenlik kavramı sadece öznellik değil, karşılıklı öznellik üzerinden de açıklanabilir. Kopenhag Ekolü savunucularına göre güvenlik kavramı, iletişim ve etkileşimler sonucu ortaya çıkar (Buzan, Wæver ve Wilde: 29-30). Bu sebeple güvenliğin karşılıklı öznel olduğu ve sosyal bir şekilde yapılandırıldığı savunulur (Aras ve Polat, 2008: 497).

Kopenhag Ekolü, güvenlikleştirme yaklaşımında epistemolojideki söz edimi[3] (speech act) teorisinden faydalanılır. Burada herhangi bir meselenin tehdit olarak algılanmasında ve meselenin bir güvenlik meselesine dönüşmesinde aktörlerin söylemleri önem arz etmektedir. Kopenhag Ekolü temsilcilerine göre tehdidin gerçekte var olması gerekmez. Bir durumun gerçek anlamda bir tehdit olup olmadığının tecrübe edilmeden anlaşılamayacağını savunurlar. Bu bağlamda bir konunun, ancak aktörler tarafından tehdit olarak adlandırılmasıyla onun tehdide dönüştüğü söylenebilir. Başka bir deyişle, tehdidin ne olduğunun bilinemeyeceği varsayılır ve konuşma eylemi aracılığı ile tehdit

[2] Bu bölümde, kullanılan referansların yanı sıra yoğunluklu olarak Münevver Cebeci'nin Marmara Üniversitesi AB Enstitüsü'nde verdiği "AB'nin Uluslararası Politikaları" dersi notlarından faydalanılmıştır.

[3] "İngilizce karşılığı "speech act" olarak belirtilen söz edimi kuramı, anlam sorunlarına, dilin kullanımına bakılarak çözüm bulunması gerektiğini belirten, gündelik dil felsefesi geleneğinin öncü filozoflarından Austin'in 1930'larda geliştirdiği ve ayrıntılarını 1955'de Harvard'da verdiği derslerde açıkladığı bir kuramdır. Düşünürün ölümünden sonra 1962'de yayınlanan "How to Do Things with Words" adlı kitabıyla da düşünce dünyasına sunulmuştur. J. L. Austin'in geliştirdiği söz edimi kuramı, dilin farklı kullanım biçimleri ve işlevlerini öne çıkarması açısından, özellikle döneminin dar bakış açılı dil görüşüne göre, kapsamlı bir dil kuramı olma özelliğine sahiptir. Söz edimi kuramının kullanım açısından anlamlı bir değerlendirme yaklaşımı olduğu söylenebilir. Söz edimi kuramı dil üzerinde yapılan felsefi bir çalışmadan meydana gelir. Bu çalışma konuşmacı ve dinleyicinin söyledikleri ve davranışları, kişiler arası bir konuşmada kişilerin deneyimlediği edim, hareket ve olaylar arasındaki ilişkiyi gösteren mantıksal kuralların saptanmasına ilişkin bir girişimdir. Söz edimi kavramında edim eyleme, söz ise dile gönderme yapmaktadır (Çelebi, 2014: 74-75; Altınörs, 2003: 135-138)". Teori ile ilgili detaylı analiz için bkz. (Austin, 1975)

oluşturulmuş olur (Wæver, 1995: 44-45). Bu nedenledir ki Kopenhag Ekolü için güvenlik öncelikle bir söz edimidir.

Kopenhag Ekolü savunucularının öne sürdüğü güvenlikleştirme yaklaşımında iki unsurun varlığı önem arz etmektedir. Bunlardan birincisi tehdit tanımlaması yapacak bir anlatıcının olması bir diğer unsur ise bunların kabul göreceği alımlayıcı kitlenin (audience)[4] varlığıdır. Buradaki anlatıcı güvenlik aktörü olarak karşımıza çıkmaktadır. Nitekim herkesin her söylediği bir tehdit olarak kabul görmeyebilir. Bu durumda güvenlikleşme gerçekleşmez. Güvenlikleştirmenin en önemli yönü bir alıcı kitle tarafından ilgili söz ediminin kabulüdür. Güvenlik aktörüne ihtiyaç duyduğu yetkiyi veren de bu kabuldür. Yani güvenlik aktörünün söylemlerinin kabul görmesi ile bu aktöre zımni olarak bir tehdit tanımlama ve o tehditle çeşitli yollarla (önlemlerle) başa çıkma yetkisi verilmiş sayılır. Burada bahsedilen yetkinin resmi bir yetki olması gerekmez; uluslararası örgütlerin, sivil toplum kuruluşlarının, etkili şirket ortaklıklarının ve hatta bazı bireylerin birer güvenlik aktörü olarak karşımıza çıkması muhtemeldir. Resmi yetki ise, daha çok, önceden verilmiş yetkidir. Örneğin, demokratik ülkelerde tehditleri ve güvenlik politikalarını belirleme yetkisi önceden seçimler yoluyla hükümetlere verilir.[5] Bununla birlikte güvenlik meseleleri hakkında karar verme yetkileri de bu yollarla devredilebilir (Aras ve Polat, 2008; Wæver, 1995: 44-45).

Kopenhag Ekolüne özgü bakış açısında; güvenlik aktörüne göre, karşılaşılan tehdit söz konusu başvuru nesnesi için yaşamsal (existential) bir tehdittir – yani beka (survival) ile ilgilidir – ve eğer onunla ilgili olarak anında aksiyon alınmazsa çok geç olabilir (Buzan, Wæver ve Wilde: 39). Bu nedenle, o tehditle en kısa zamanda ve olağan olmayan, yani istisnai, önlemlerle mücadele etme gerekliliği duyulur. Bu istisnai önlemler, çoğu zaman mevcut siyasi normlarının bozulması anlamına gelir (Aras ve Polat, 2008: 497). Yeni vergiler konulması, olağanüstü hal ya da sıkıyönetim ilanı, asker alımı gibi önlemler bu duruma örnek olarak verilebilir (Buzan, Wæver ve Wilde: 29-30). Bu önlemlerin ortak paydası, insanların temek hak ve özgürlüklerini sınırlandırmalarıdır. Örneğin, terör ile ilgili olarak uçuşlarda yolcuların yanına alacakları eşyaların sınırlandırılması temel hak ve hürriyetlere getirilmiş bir kısıtlamadır. Aynı şekilde

[4] İngilizce karşılığı "audience" olarak belirtilen ve teoride kullanılan kelime alımlayıcı kitle ya da dinleyici kitle olarak kullanılmaktadır. Alımlayıcı olarak kullanılmasının temel nedeni dinleyen kesimin söylenenleri anlayarak kabul etmesidir. Söz konusu dinleyiciler güvenlikleştirme eyleminin gerçekleştirilmesinde aktif bir rol oynamaktadır. (Kaliber, 2005)

[5] Bu paragraf, Münevver Cebeci'nin dipnot 2'de bahsedilen dersinden derlenmiştir.

olağanüstü hal ve sıkıyönetim durumlarında uygulanan sokağa çıkma yasağı da yine bu türde sınırlandırıcı bir önlemdir. Böylelikle güvenlikleştirme ile güç kullanımı meşru zemine oturtulmaya çalışılır. Daha da ötesini düşünmek gerekirse güvenlikleştirme, normal meşru siyaset zemininin dışına çıkılmasına ve panik siyasetinin ortaya çıkmasına sebep olur (Buzan, 1997: 13-14).

Güvenlik söylemi, toplumu herhangi bir tehdide karşı uyarmak ve toplumu bu konuda harekete geçirmek amacı ile kullanılabilir. Çoğu zaman beka (survival) ile ilgili ciddi tehditlere yönelik kullanılsa da, güvenlik söylemi, belirli kişilerin toplumdaki mevcut pozisyonlarını korumaları için- ya da başka amaçlara erişmek[6] için suistimal edilebilir. Bu anlamda, güvenlik, her zaman sonuçları fayda sağlayıcı bir kavram değildir. Pozitif olmaktan çok negatif sonuçlar verilmesi de muhtemel bir durumdur (Wæver, 1995: 45; Kaliber, 2005: 38). Hak ve özgürlüklerin sınırlandırmasında uç sayılabilecek istisnai uygulamalara gidilmesi suistimallere açık olduğu için olumsuz yönler de taşır. Kopenhag Ekolü, güvenliğin negatif bir değer olduğunu vurgular ve güvenlikleştirmeyi, problemlerin çözümü konusunda normal siyasi yollarla ilgilenilmesi konusunda başarısızlık olarak belirtilir. (Buzan, Wæver ve Wilde, 1998: 27,208; Wæver, 1995: 51)

Bir söz edimi ile başlayan ve olağanüstü önlemler kullanılması ile sonuçlanan sürece Kopenhag Ekolü "güvenlikleştirme" (securitization) adını vermiştir (Buzan, Wæver ve Wilde, 1998: 24) Daha kolay bir analiz çerçevesi sunmak amacıyla Kopenhag Ekolü güvenliği sektörlere ayırmıştır. Gerçek hayatta bu sektörlerin iç içe geçmiş olduğunun altını çizmek gerekir. Nitekim Kopenhag Ekolü, sadece analiz çalışmasının daha kolay yapılabilmesi için bu ayrıma gitmiştir. Bu beş sektörden kısaca bahsetmek siber güvenlik için çizilecek olan kuramsal temel için yerinde olacaktır.

Askeri güvenlik sektöründe başvuru nesnesi (referent object)[7] genellikle devlettir. Ancak, askeri güvenlik barışı koruma faaliyetleri ile ilgili alanları da içerdiği için başvuru

[6] ABD'nin Irak'ta kitle imha silahları bulunduğunu öne sürerek, ülkesinin bölgedeki enerji çıkarlarını korumaya çalışması buna örnek olarak verilebilir. Bush'un 29 Ocak 2002'de vermiş olduğu demeçte kullanmış olduğu dili örnek olarak incelemek faydalı olacaktır. Kitle imha silahı kullandıklarını öne sürdüğü ve "şer ekseni" olarak tanımladığı İran, Irak ve Kuzey Kore'nin bu silahları geliştirerek terörizme destek verdiği ve hem ABD için hem de dünya için bir tehdit oluşturduğunu belirttiği söylemi ile bir güvenlik tehdidi gündemi oluşturmuştur. Bush'un yaptığı konuşma detayları için bkz. (The Washington Post, 2002)

[7] İngilizce karşılığı "referent object" olarak belirtilen "başvuru nesnesi" varoluşsal anlamda tehdit ediliyor olarak görülen nesnedir. Buzan'a göre yeni güvenlik sisteminde devlet, esas başvuru nesnesi olması özelliğini yitirmiştir. Yeni başvuru nesnelerine devletin üstündeki uluslararası rejimleri, altında ise temel hak ve özgürlükler kapsamında bireyleri, yanında da küresel ekonomi, çevresel sistemler gibi alanları

nesnesi bu gibi durumlarda herhangi bir insan topluluğu da olabilir (örneğin; Bosnalı Müslümanlar). Güvenlik meselelerinin askeri yöntemlerle çözülmeye çalışıldığı durumlara dikkat çekilir. Devletlerarasındaki bir savaş, bir devletin içindeki herhangi bir iç savaş, ya da barışı koruma amacıyla yapılan operasyonlar bu sektöre örnek olarak verilebilir. Bu sektörde ana aktör devletlerdir. Ayrıca, NATO ve AB gibi uluslararası örgütlerin de aktörlüğünden bahsedilebilir. Özellikle son yıllarda devlet dışı aktörlerin (terörist gruplar) gayri meşru bir şekilde ağır silahlar ele geçirerek askeri güvenlik alanında varlık gösterdikleri de görülmektedir.

Siyasi güvenlik sektöründe tehditler genellikle dayanılan ilke çerçevesinde tanımlanır. Başka bir deyişle bu sektörde tehditler egemenlik ve bazı zamanlar da buna eşlik eden bir ideoloji temelinde tanımlanır (Buzan, Wæver ve Wilde, 1998: 42). Siyasi güvenlik sektörünün başvuru nesnesi devlet olabileceği gibi, etnik ya da dini bir grup ya da bir birey olabilir. Bir devletin yönetim şekline (rejimine) yönelik tehditler bir siyasi güvenlik sorunu oluşturabilir. Öte yandan devletin kendisi kendi vatandaşlarına ya da onların bir kısmına yönelik tehdit oluşturabilir. Bu, genellikle demokratik olmayan rejimler ile yönetilen ülkeler için geçerlidir. Bir ülkede insan haklarının ya da azınlık haklarının yeterli derecede sağlanamaması, demokratik şartların oluşturulamaması, adaletin üstünlüğü kuralının yok sayılması ya da yönetişimin (governance) çok zayıf veya tamamen yok olması siyasi güvenlik sektörünün problemlerini oluşturur (Buzan, Wæver ve Wilde, 1998: 141-142). Buna ek olarak, AB gibi siyasi oluşumlu örgütlerin sürekliliğine ilişkin tehditler de bu sektör içinde değerlendirilebilir.

Giderek küreselleşen dünyada ekonomi sadece devletlerin sürekliliği için değil dünyanın sürdürülebilirliği için gerekli bir unsur olarak karşımıza çıkmaktadır. Nitekim dünyanın herhangi bir yerinde meydana gelen bir kriz dünyadaki tüm toplulukları, ülkeleri ve farklı sektörleri etkileyebilmektedir. Bu anlamda ekonomik istikrar hem devletlerin, hem insan topluluklarının, hem de bireylerin ve aslında tüm dünyanın sürekliliği açısından son derece önemlidir. Bu sektör, neredeyse tamamen farklı olarak kaynaklara erişim, finans ve piyasa gibi devletin kabul edilebilir bir refah ve güç seviyesine gelmesi için gerekli olan konulara odaklanır (Buzan, 1991: 19-20). Başka bir ifade ile bu sektör ticaret ve üretim ilişkileri ile ilgilenmektedir. Kopenhag Ekolü

işaret etmektedir (Buzan, 1997: 11-12). Balcacq, başvuru nesnesinin dengeleyicisi olarak "başvuru öznesi"ni (referent subject) eklemektedir. Bunu da güvenliğin sağlanması gereken şey olarak tanımlamaktadır (Balzacq, 2005: 177).

temsilcilerine göre bunların hepsi güvenlik tehdidi olarak inşa edilebilir. Ayrıca, ekonomik güç, devletlerin diğer alanlarda, özellikle askeri güvenlik alanındaki gücü ile de yakından ilişkilidir (Buzan, 1998: 38,95).

Toplumsal güvenlik sektörü kolektif kimlik konuları ile ilgilenmektedir. Bu sektörde başvuru nesnesi herhangi bir topluluktur. Bu bir etnik ya da dini azınlık olabileceği gibi, bir ulus da olabilir. Söz konusu grubun kimliğine yönelik bir tehdidin ortaya çıkması ile oluşur. Batı Trakya'daki Türk azınlığın belirli sosyal ve kültürel haklarının sınırlanması, Çin'deki Uygur Türkü olan Müslümanların yaşama haklarının ellerinden alınmaya çalışılması bu tür tehditlere örnek olarak verilebilir. Diğer yandan, Avusturyalıların Türk ve Müslüman göçmenleri kendi kimliklerine tehdit olarak algılaması çoğunluğun da azınlıklar kadar toplumsal güvenlik alanında başvuru nesnesi olarak inşa edilebileceğine örnektir. Toplumsal güvenlik sektörünün başvuru nesnesini, geniş grupların taşıdığı aidiyet ve bağlılık hissi sonucunda "biz" duygusunun tehdit edildiği konusunda erişilen fikir birliğinin belirlediği söylenebilir (Buzan, Wæver ve Wilde, 1998: 123).

Çevresel güvenlik sektörü insan eylemleri ve biyosfer arasındaki ilişki üzerinde durmaktadır. En basit haliyle, çevresel güvenlik sektörünün başvuru nesnesi çevrenin kendisidir. Fakat bunun yanında medeniyetin sağlamış olduğu ilerlemeyi kaybetmesi riskiyle de ilgilenmektedir. Küresel ısınma, karbondioksit salınımı, iklim değişikliği gibi çevresel sorunlar giderek insan yaşamını tehdit eder hale gelmektedir. Diğer taraftan, doğal kaynakların tükenmek üzere olması, hem zorunlu göçlere hem de savaşlara neden olmaktadır. Bu da gerçek yaşamda güvenlik sektörlerinin bir birleriyle ilişki içinde olduğunun ve sektörlerin bir arada değerlendirilmesi gerektiğinin önemli bir göstergesidir. (Buzan, Wæver ve Wilde, 1998: 75) Öte yandan, depremler, sel, erozyon gibi doğal afetler de çevresel güvenliğin konuları olabilmektedir. Bu gibi durumlarda başvuru nesnesi insanlar ve/veya insan gruplarıdır. Bu bölümde değerlendirilen sektörlerin siber güvenliğin kapsadığı alanlara veri oluşturduğu söylenebilir. Zaman zaman bir sektör başlıca siber güvenliğe konu olabilirken zaman zaman da farklı sektörlerin bir arada olduğu karma bir sektörü ihtiva eden bir olgu olarak karşımıza çıkabilmektedir. Ayrıca, siber güvenliğin kendisinin bir güvenlik sektörü olarak değerlendirilip değerlendirilemeyeceği de tartışılması gereken bir konudur. Bu bağlamda

siber güvenlik ve güvenlik sektörlerinin ilişkisinin anlaşılabilmesi için siber güvenlik ve güvenlikleştirme kavramının birlikte değerlendirilmesi yerinde olacaktır.

1.3. Siber Güvenlik Kavramının Analizi

Bilgi teknolojilerine ilişkin birçok kavramda olduğu gibi siber güvenlik kavramına ilişkin olarak da net bir tanım yapmak mümkün olmamaktadır. Bu sebeple siber güvenlik kavramından önce siber (cyber) kavramının tanımlanması faydalı olacaktır. Ayrıca siber kelimesi ile ilintili olarak siber casusluk ve siber terörizm kavramları da bu bölümde irdelenmiştir. Siber suç kavramı ise bu tezin 2. Bölümünde detaylı bir şekilde anlatılmıştır.

1.3.1. 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 İngilizcedeki anlamı "cyber"[8] 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) "Siber uzay" terimi de ilk olarak 1984 yılında "Neuromancer" (Gibson, 1984) adlı bilim kurgu romanının içinde geçerek gündeme gelmiş, siber ve uzay ifadelerinin birleşmesinden bir bünyeyi oluşturması ile sonraları da akademide kullanılmıştır (Whittekar, 2004: 4).

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,

[8] "Cyber" kelimesi Türkçeye "siber" olarak çevrilmekle birlikte, Türkçede tam olarak bir karşılığı bulunmadığı için burada İngilizce karşılığı üzerinden kavram açıklaması yapılmıştır.

insanların her türlü elektronik bilgi hizmetine erişimini mümkün kılan ve "siber uzay" olarak tanımlanan yeni bir dünya oluşmuştur. (Gibson ve Erle, 2006: 97) Siber uzay, internete bağlı bilgisayar sistemlerini, iletişim altyapılarını, veri tabanlarını ve bilgi araçlarını barındıran, genellikle ağ (net) olarak bilinen küresel sistem olarak tanımlanabilmektedir. (Birleşmiş Milletler, 2016) Bu tanımlardan yola çıkarak günümüzde siber uzayın tek bir uzaydan oluşmadığı, her biri farklı sayısal etkileşim ve iletişim yöntemi sağlayan bir biri ile iç içe geçmiş bir alan olduğu sonucuna ulaşabiliriz. Hızla gelişen ve homojen olmayan küresel bir sistemin varlığından söz edebiliriz.

Siber uzayda internete bağlı bilgisayarlar için fiziksel olarak hangi konumda bulunursa bulunsun iletişim ve veri akışı açısından herhangi bir zaman ve mekân farkı gözetmeksizin anlık iletimler sağlanması mümkün olmaktadır. Bununla birlikte bilgisayar güvenliği fiziksel bir olgu olmanın ötesinde siber uzay bağlamında tartışılan bir konu haline gelmiştir. Nitekim zararlı yazılımlar aracılığı ile bilgisayarların hem yazılımsal hem de donanımsal olarak zarara uğrama ihtimali ortaya çıkmıştır. Bununla birlikte bu bilgisayarlarda ve sistemlerde depo edilen verilerin zarara uğraması ya da sistemlerin ve bilgisayarların yetkisiz erişimler sonucunda amacı dışında suç teşkil edebilecek eylemlerde kullanılması yeni sorunlar olarak ortaya çıkmıştır. Tam bu noktada siber uzayın güvenlikleştirilmesi ve bu alanda gerçekleştirilen eylemlerin niteliklerinin tartışılması ihtiyacı doğmaktadır. Bu bağlamda bilgisayar suçları ve siber uzayın ayrılmaz parçaları olarak devletler ve uluslararası örgütler için önemli bir sorun olan casusluk ve terörizm kavramları da bu alana taşınmış ve siber uzayda da bu faaliyetler mümkün olmuştur. Bu açıdan AB'nin siber güvenlik politikasının oluşturulmasında siber casusluk ve siber terörizm faaliyetlerinin de etkilerinin olduğunu söylemek yerinde olacaktır.

Casusluk, insanlık tarihinin oluşumundan günümüze değin varlığını sürdüren bir kavramdır. Devlet güvenliğine karşı işlenen suçların en önemli, en eski ve en tehlikeli olanlarından biri olarak değerlendirebileceğimiz casusluk faaliyeti, günümüzde teknolojinin gelişmesi, bilgi ve iletişim teknolojilerindeki yenilikler ile birlikte siber uzayda da kullanımına fırsat bulunan bir alan olarak karşımıza çıkmaktadır. Geçmişte sadece askeri ve siyasi alanlara yönelmiş olan casusluk faaliyetlerinin günümüzde teknolojiden sanayiye, eğitimden genetiğe, havacılıktan telekomünikasyon sektörüne kadar birçok alana yayıldığını söylemek mümkündür. 2002 yılında başlayan, ABD Savunma Bakanlığı'nı hedef alan, Çin tarafından gerçekleştirildiği belirtilen ve "Titan

Rain" olarak anılan siber casusluk olayları bu alanın en belirgin örneklerindendir. Bu saldırılarda Çinliler tarafından NIPR Net sunucularından 10-20 terabayt veri indirildiği düşünülmektedir (Carr ve Shepherd, 2010: 4). Bu faaliyetlerin sonrasında gerçekleşmiş olan siber casusluk olayları da bu isimle anılmaya devam edilmiştir.

Bilgi ve iletişim teknolojilerindeki yenilikler ile birlikte verilerin depolanması ve saklanması kolaylaşırken aynı zamanda siber casusluk faaliyetlerinin de kolaylaşmasına olanak sağlamaktadır. İnternet ile iç içe geçmiş günümüz dünyasında internet aracılığı ile kişilere, işletmelere, devlet kurumlarına ait kullanıcı hesaplarına ait bilgilerin ele geçirilmesi çok yaygın karşılaşılan eylemler olarak karşımıza çıkmaktadır. AB'nin siber güvenlik politikasının oluşturulmasında bu tür eylemlerin de etkisinin olduğunu söylemek mümkündür.

Terörizm de, uluslararası ve ulusal güvenlik ortamını tehdit eden bir olgu olarak karşımıza çıkmaktadır. Terörizm konusunda mutabık kalınmış bir tanım olmamakla birlikte her analizci ve çoğu zaman her resmi kurum (devlet veya uluslararası örgüt) kendi dünya görüşü ve siyasi bakış açısına göre tanım yapabilmektedir. Terörizm olarak adlandırılabilecek faaliyetler bir toplum için özgürlük mücadelesi olarak değerlendirilebilirken, karşı toplum ya da devlet tarafından terörist bir eylem olarak algılanabilmektedir. (Çitlioğlu, 2008: 17) Bu açıdan tek bir terörizm tanımından söz etmek mümkün olmamaktadır. Siber terörizm ise, genel olarak, terörist eylemlerin siber alan kullanılarak gerçekleştirilmesi olarak ya da terör örgütlerinin siber uzayı araç olarak kullanmaları olarak tanımlanabilir. (Jancewski ve Colarik, 2008: 7) Daha kapsamlı olarak ise bilgisayar ve iletişim teknolojisi yeteneklerinin siyasi olarak motive olmuş devlet dışı gruplar veya gizli ajanlar tarafından şiddet, bir toplumu etkilemek ya da bir hükümetin politikalarını değiştirtmek amaçlı olarak silah veya hedef olarak kullanılması şeklinde tanımlanabilir. (Andress ve Winterfeld, 2011: 198)

Bu çalışma kapsamında değerlendirilen Estonya saldırıları siber terörizm faaliyeti olarak değerlendirilmektedir. (Bloomfield, 2007) Siber uzayın güvenlikleştirilmesinde ve siber tehditlerin güvenlikleştirme alanına dâhil edilmesinde bu tür olayların öneminin büyük olduğunu söylemek yerinde olacaktır. Nitekim terörist faaliyetler sonucu zarar gören sadece devlet ya da herhangi bir kurum olmamakla birlikte toplumsal hayatın her aşamasında olumsuzluklar yaşanabilmektedir.

1.3.2. Siber Güvenlik Kavramı

Çalışmanın ana temasını oluşturan 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), bilginin 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)

Şekil 1 Siber Güvenliğin Hedefleri

Kaynak: (Bisson ve Saint-Germain, 2005: 3)

Şekil 1'de de görüldüğü üzere, bilginin güvenliğinin sağlanabilmesi için gizliliğinin, bütünlüğünün ve erişilebilirliğinin birlikte sağlanması gerekmektedir. Nitekim bu üç bileşenden birinde zayıf halkanın olması bilgiye sızmaları ve yetkisiz kişilerin ulaşımına zemin hazırlayacaktır. Siber güvenlik de bu noktada devreye girmekte ve bu bileşenlerin ayrı ayrı sağlanması için önlemler geliştirmektedir. Siber güvenliği

anlayabilmek için siber güvenliğin üç temel hedefi olan unsurların tek tek incelenmesinde fayda olacaktır. Bu unsurlar; gizlilik, bütünlük ve erişilebilirliktir.

Gizlilik, bilgi ve iletişim ağlarındaki bilgilere yetkisiz kişilerin erişiminin kısıtlanmasının sağlanmasını ifade etmektedir. (Avrupa Komisyonu, 2013a) Kişisel verilerin gizliliğinin sağlanması ve haberleşme etkinliğinin özgür bir şekilde yapılabilmesi için bilgilerin gizliliğine önem atfedilmektedir.

Bütünlük; iletilen, gönderilen veyahut alınan bilginin eksiksiz ve üzerinden oynanmamış olmasının sağlanmasını ifade etmektedir (Avrupa Komisyonu, 2013a). Bütünlük, sözleşmelerin yapılması sırasında kimlik doğrulamasının sağlanması için önem arz etmektedir (Avrupa Komisyonu, 2013a). Ayrıca verilerin doğruluğunun yüksek öneme sahip olduğu sağlık uygulamaları ve sanayi tasarımları gibi alanlar için de önemli bir unsur olarak karşımıza çıkmaktadır (Avrupa Komisyonu, 2013a). Bilişim sistemlerinde depolanan bilgilerin kısmen veya tamamen silinmiş ya da yok edilmemiş olması da bütünlük bağlamında değerlendirilebilir (Avrupa Komisyonu, 2013a).

Erişilebilirlik, bilginin her koşulda ulaşılabilir ve erişebilir olmasıdır (Avrupa Komisyonu, 2013a). Doğal afet durumları başta olmak üzere, kazalar ve saldırılar gibi olağanüstü durumlarda da hizmetlere devam edilmesinin sağlanmasını ifade etmektedir (Avrupa Komisyonu, 2013a). Bilgi ve iletişim ağlarında kesintinin yaşanması haberleşme, hava yolu taşımacılığı gibi sistemlerin sürekliliğinde kesintiye sebep olabileceği için erişilebilirlik bilgi için önemli bir unsur olarak karşımıza çıkmaktadır (Avrupa Komisyonu, 2013a). Erişilebilirlik aynı zamanda saklanan bilginin gerekli durumlarda yetkili kişilerce ulaşılabilir olmasının gerekliliğini de bünyesinde barındırmaktadır (Avrupa Komisyonu, 2013a).

Siber güvenliğin hedeflerini de esas alarak siber güvenliği şu şekilde tanımlayabiliriz: 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)

1.4. Siber Güvenlik ve Güvenlikleştirme İlişkisi

Siber güvenlik, düşük maliyetlerle kısa sürelerde farklı sektörlere yönelik gerçekleştirilen siber saldırılar neticesinde ülkelerin askeri ve siyasi yapılanmalarını içeren gizli bilgilerin deşifre edilebilmesi, toplumsal yapı ve kimliklere ilişkin algılar oluşturulması, ülke ekonomilerinin zarar görmesi, altyapı sistemlerini düzenleyen sistemlere yapılan saldırılar ile çevresel problemlerin ortaya çıkması açısından önemli bir güvenlik alanı – bir anlamda güvenlik sektörü – haline gelmiştir. Ayrıca, güvenlik sektörlerinin iç içe geçmişliğini göstermesi açısından da son derece önemlidir. Buradan yola çıkarak, siber güvenliği ve siber güvenliğin ortaya çıkış sürecini güvenlikleştirme süreci üzerinden açıklamak yerinde olacaktır.

Kuramsal temel olarak güvenlikleştirmenin seçilmesinde güvenlik çalışmalarındaki geleneksel ve eleştirel teorilerin kapsamlarının tam olarak siber uzay ile örtüşmemesi önemli bir sebep olmuştur. Ulusal bağımsızlık, toprak bütünlüğünün korunması ve egemenlik, geleneksel güvenlik teorisyenlerinin devlet temelli anlayışının merkezi değerlerini oluşturmaktadır (Miller, 2001: 17). Siber güvenliği bu alanda açıklamaya çalışmak devlet-dışı aktörlerin varlığını göz ardı etmek anlamına gelmektedir. Bu bağlamda, siber güvenliğin sadece devlet merkezli bir alan olmaması, aksine devlet-dışı birçok birim ve aktörü de bünyesinde barındırıyor olması Kopenhag Ekolünün güvenlik yaklaşımının bu alanı daha kolay açıklayabileceğini göstermektedir. Ayrıca, geleneksel güvenlik anlayışı, güvenliğin nesnelci bir algısını temsil etmektedir. Realistler, dışarıda, gözlemleyen bireylerden bağımsız, nesnel ve bilinebilir bir dünyanın var olduğunu öne sürmektedirler (Mearsheimer, 1994-95: 37-41). Bu yaklaşım, tehditlerin de nesnel olduğu görüşündedir ve güvenliğin tanımlanmasında söz edimini tamamen göz ardı etmektedir. Ancak siber uzayın bilinmezliği ve belli sınırlarının olmayışı siber tehditlerin belirlenmesinde söz ediminin önemli bir yer tuttuğunun da göstergesidir. Bu bağlamda, siber güvenliğin geleneksel teoriler üzerinden tanımlanması çok açıklayıcı değildir. Kopenhag Ekolünün yaklaşımı, gerek devleti göz ardı etmememesin, gerekse diğer aktörleri ve güvenliğin başvuru nesnelerini tanımına dâhil etmesi ve söz edimi vurgusu açısından bu tezde tercih edilen kuramsal çerçeve olmuştur. AB'nin siber güvenlik politikasını oluşturmasında geçen süreçte gerek Avrupa Komisyonu Başkanının,

gerekse Avrupa Parlamentosu yetkililerinin söylemleri, demeçleri[9] söz edimi olarak karşımıza çıkmaktadır. Küresel gündeme paralel olarak siber uzayın, güvenlik alanına dâhil edildiği söylenebilir. Güvenlik tehdidi algılarının oluşturulmasında bu süreçlerin göz ardı edilmesi mümkün değildir.

Kopenhag Ekolünün güvenliğe yaklaşımının farklı güvenlik teorilerinden beslenerek eklektik bir yapıdan oluştuğu söylenebilir. Nitekim Kopenhag Ekolünün yaklaşımı, gücünü de bu kapsayıcı perspektiften almaktadır. Ancak Kopenhag Ekolünün çevre gibi yan konuların bile güvenlik meselesi haline getirilmesine karşı çıktığı ve bireysel güvenliği bir güvenlik sektörü olarak ele almadığı gözden kaçırılmamalıdır. Bu, onların yaklaşımını eleştirel teorilerden uzaklaştırırken, devleti de analiz birimi olarak kullanmaları onları realist teoriye yakınlaştırmaktadır. Diğer taraftan, etkileşim ve karşılıklı öznellik vurguları, bakış açılarının en fazla sosyal yapılandırmacılık (social constructivism) teorisinden etkilendiğini göstermektedir. Kopenhag Ekolüne göre güvenlik bir eylemdir. Bu eylem, bir konunun belirli bir şekilde çerçevelenmesidir. (Açıkmeşe, 2008: 208-210) AB kurumları ve temsilcileri tarafından siber güvenlik de bu anlamda çerçeve içine alınan ve zamanla söz edimleri ile güvenlik tehdidinin belirlediği ve bu çerçevede önlemler alınmasının beklendiği bir alan olarak karşımıza çıkmaktadır.

Siber güvenliğin Kopenhag Ekolündeki en kapsamlı çalışması Hansen ve Nissenbaum tarafından 2009 yılında yapılmıştır. (Hansen ve Nissenbaum, 2009) Siber uzayın güvenlikleştirilmesi konusunda yapılmış kapsamlı bir çalışmadır ve Kopenhag Ekolünden yola çıkılarak siber uzayın güvenlikleştirilmesi konusunda metodolojisi ve argümanlar ortaya konulmuştur. Makalede, Soğuk Savaş sonrası meydana gelen teknolojik yenilikler ve jeopolitik değişimlerin karışımına cevaben doğmuş olarak nitelendirilen siber güvenlik kavramı etraflıca değerlendirilmiştir. Tehditleri ve başvuru nesneleri ile siber güvenlik güvenlikleştirme perspektifinden farklı bir sektör olarak analiz edilerek, Estonya kamu ve ticari kuruluşlarına gerçekleştirilen siber saldırılar üzerinden teorinin uygulanabilirliği ortaya konulmaya çalışılmıştır. Bireysel güvenlik ve ağ güvenliği gibi önemli başvuru nesnelerinin yanı sıra devlet, toplum, ulus ve ekonomi gibi başvuru nesnelerinin de siber uzayın güvenlikleştirilmesinde önemli başvuru nesneleri olabileceğine vurgu yapılmıştır. (Hansen ve Nissenbaum, 2009)

[9] Burada bahsedilen söylemler ve demeçler, bu tezin "AB'nin Siber Güvenlik Politikası" bölümünde detaylı olarak incelenmiştir.

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 (everyday security practises) ve teknikleştirme (technification). Hansen ve Nissenbaum hiper güvenlikleştirmeyi büyük ölçekli, ani basamaklı afet senaryolarının güvenlikleştirilmesi olarak tanımlamaktadır. (Hansen ve Nissenbaum, 2009: 1164) Günlük güvenlik uygulamaları, kişilerin gündelik yaşamda karşılaştıkları siber güvenlik olaylarının güvenlikleştirilmesini ifade etmektedir. (Hansen ve Nissenbaum, 2009: 1165) Teknikleştirme ise güvenlikleştirme 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: 1166)

Siber güvenlik, Hansen ve Nissenbaum'un ifade ettiği gibi ayrı bir sektör olarak sınıflandırılabilecek olsa bile, tüm güvenlik sektörleri ile iç içe geçmişliği referans göstermesi sebebiyle, bu çalışma başlı başına bir sektör olmaktan çok tüm sektörlerle bağlantılı bir güvenlik olgusu olarak değerlendirilmiştir.[10] Bu çalışmanın genelinde ana referans noktası siber güvenliğin tüm sektörleri kapsayan bir güvenlik olgusu olduğu yönündedir.

1.5. Sonuç

Siber güvenlik, bu bölümde Kopenhag Ekolünün temsilciliğini yaptığı güvenlikleştirme kuramı ile ilişkilendirilerek kuramsal zemine oturtulmuştur. Siber güvenliğin politika yapım sürecinde bir olgu olarak ortaya çıkış süreci ve tehdit olarak değerlendirilmesi bu kuram kapsamında sunulmuştur. Her olayı, her kavramı bir teori ile tam olarak bağdaştırmak mümkün olmamaktadır. Bu bölümde, uluslararası ilişkiler disiplininde sıkça referans gösterilen teoriler[11] içinde konuyu en iyi açıklayan kuramın güvenlikleştirme kuramı olduğu öne sürülmüştür. Bu bağlamda AB'nin politika yapım

[10] Siber güvenliğin bir güvenlik sektörü olarak tanımlanması bu tezin amaçlarını ve sınırlarını aşmaktadır. Bu sebeple çok daha derin bir teorik tartışma gerektiren bu konu burada sadece tezin argümanının gerektiği ölçüde ele alınmıştır.

[11] Burada "uluslararası ilişkiler disiplininde sıkça referans gösterilen teoriler" olarak bahsedilen, uluslararası ilişkiler disiplinindeki geleneksel teoriler (realizm, liberalizm, sosyal inşacılık) ve post-pozitivist teorilerdir (Marksizm, eleştirel teori, feminizm, yeşil teori, post-yapısalcılık, post-modernizm). Bu teoriler ile ilgili detaylı bilgi için bkz. (Arı, 2013a; Arı, 2013b; Arı, 2014; Gözen, 2014; Sönmezoğlu, 2010; Balta, 2014).

süreci ve siber güvenliği bir güvenlik meselesi haline getirmesinin analizindeki kuramsal altyapı sağlanmıştır.

Kuramsal temellendirmesi yapılmış olan siber güvenliğin ortaya çıkmasındaki tehditlerin açıklanması gerekliliği bulunmaktadır. Ayrıca bu tehditlere karşı devletlerin ve uluslararası aktörlerin politikalarından örnekler vermek faydalı olacaktır. Bu bağlamda sonraki bölümde siber tehditlerin temelini oluşturan siber saldırı teknikleri, muhtemel riskler ile birtakım devletler ve uluslararası örgütlerin bu tehditlere yönelik geliştirmiş olduğu politikalara yer verilmiştir.

Günlük yaşamda önemli değişikliklere sebep olabilecek siber olayların varlığı ve bunların ne şekilde gerçekleştiğinin bilinmesi AB'nin siber güvenlik politika yapım sürecinin daha anlaşılabilir olması açısından önem arz etmektedir. Bu bağlamda, ikinci bölümde günümüz dünyasında sıklıkla karşılaşılan siber saldırı teknikleri ve siber güvenlik uygulamaları irdelenmektedir.

2. BÖLÜM

SİBER SALDIRI TEKNİKLERİ VE ÖRNEKLERİ

Bu bölümde günlük hayatta sıklıkla karşılaşılan siber saldırı teknikleri örneklerle açıklanmıştır. AB'de siber olayları bir güvenlik sorunu olarak görme ve güvenlikleştirme sürecinin temelini oluşturan örneklerin ve dünya genelinde sıkça karşılaşılan siber saldırı tekniklerinin bilinmesinde fayda olacaktır.

Siber saldırı tekniklerinden dünya genelinde sıkça karşılaşılan ve yaygın olarak kullanılan yöntemler olarak oltalama (phishing), kötücül yazılım (malware), botnet, hizmeti engelleme (DoS/DDoS) saldırıları ve sosyal mühendislik saldırıları çalışma kapsamına dâhil edilmiştir. Ayrıca Kötücül yazılımlardan Truva atı (trojan), virüs, solucan, reklam içerikli ve casus yazılımlar detaylandırılmıştır. Bu bölümde ayrıca devletler ve kuruluşlar için önemli bir tehdit olan ancak siber saldırı tekniği olarak değerlendirilemeyecek olan APT (Advanced Persistent Threat) saldırılarına da değinilmiştir. Diğer yandan, AB'yi doğrudan etkileyen siber olaylar olarak Estonya, Alman Parlamentosuna yapılan siber saldırılar ve TV5 Monde örneklerine bu bölümün ikinci kısmında yer verilmiştir.

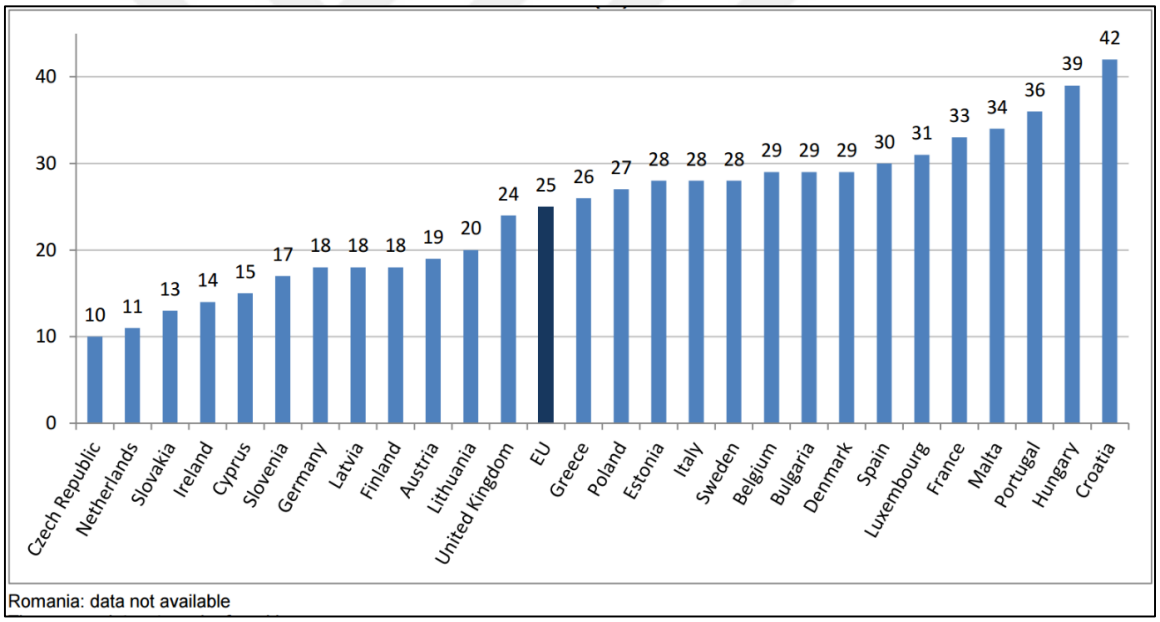
Bu siber saldırılar, güvenlikleştirme sürecinde etkili ve etkin bir siber güvenlik politikası oluşturmak için AB yetkilileri tarafından referans gösterilen olaylar olarak karşımıza çıkmaktadır. Avrupa Komisyonu üyeleri tarafından verilen basın demeçlerinde ve yasal düzenleme önerilerinde AB'nin siber saldırılara karşı alması gereken önlemlere yönelik olarak siber saldırılara ve örneklerine sıklıkla başvurulduğu gözlemlenmektedir. AB'nin siber güvenlik stratejisi ve politikalarının anlatıldığı 3. bölümdeki analiz için bu örneklere bakmak özellikle önemlidir.

2.1. Örneklerle Siber Saldırı Teknikleri

Bu bölümde siber saldırı teknikleri, siber suçlar kapsamında ele alınmıştır. İlk olarak siber suç tanımlanmış, devamında ise siber suçların işleniş biçimleri aktarılmıştır. Siber suçları kısaca teknolojik devrin ayrılmaz parçası olan bilgisayarlar ve iletişim ağlarının suç işlenmesinde araç, amaç ya da ortam olarak kullanıldığı suçlar olarak tanımlayabiliriz (Uluslararası Telekomünikasyon Birliği, 2008: 27). Siber suç, genel

olarak bilişim sistemine yönelik veya bilişim sistemlerinin kullanıldığı suçlar olarak da tanımlanabilmektedir (Karagülmez, 2011: 44). "Bilgisayar suçu" terimi bazen "siber suç" teriminin yerine kullanılsa da, "siber suç" denildiğinde bilgisayarı da kapsayan ancak sadece bilgisayarlarla kısıtlı olmayıp siber uzaydaki bütün cihaz, araç ve sistemlere karşı ya da bunlar aracılığı ile işlenen suçlar kastedilmektedir. Siber güvenliğin sağlanabilmesi için önemli unsurlardan birisi de siber suçların önlenmesidir. Nitekim siber güvenliğin sağlanması bu suçların önlenmesine bağlıdır (Gercke, 2009: 10,17).

Siber suçları geleneksel suçlardan[12] ayıran önemli özelliklerinden birisi de işleniş biçimindeki çok çeşitliliktir. Nitekim aynı suçlar farklı şekillerde defalarca işlenebilmektedir. İnternet dünyasında milyonlarca virüs çeşidi ve zararlı yazılımlar bulunmaktadır. Bunlara her gün bir yenisi eklenebilmektedir. Çalışmamızın da ana konusunu oluşturan AB'de de durum dünya geneli ile paralel gitmektedir.



Şekil 2 AB'de Güvenlik Sorunları ile Karşılaşan İnternet Kullanıcısı Yüzdesi (2015)

Kaynak: (Eurostat, 2016: 1)

Şekil 2'de AB üyesi ülkeleri kapsayan Eurostat çalışması verilerine dayanarak farklı cinsiyet, farklı yaş ve farklı eğitim gruplarındaki internet kullanıcılarının durumları

[12]Örneğin geleneksel bir dolandırıcılık suçu, sadece belirli yollarla işlenebilirken, siber suç olarak değerlendirildiğinde bunun işleniş biçimi açısından birçok türüne rastlamak mümkündür. Bu bölümde siber tehdit çeşitleri altında da örneklerine yer verilmiştir.

incelenmiştir. Araştırma sonuçlarına göre AB düzeyinde her dört internet kullanıcısından birinin internette güvenlik sorunu yaşadığı gözlenmektedir. Şekil 2'de de görüleceği gibi, AB'de en fazla güvenlik sorunu yaşayan üç ülke Hırvatistan (%42), Macaristan (%39) ve Portekiz (%36)'dir. En az güvenlik sorunu ile karşılaşan internet kullanıcısına sahip AB üyesi ülkeler ise Çek Cumhuriyeti (%10), Hollanda (%11) ve Slovakya (%13)'dır. Bu verilerden de yola çıkarak AB'nin siber güvenliğe verdiği büyük önemin yerinde ve gerekli olduğunu söylemek mümkündür.

Siber güvenliğin sağlanması ve siber suçların önlenebilmesinde siber tehditlerin tanımlanması ve tespiti önem arz etmektedir. Çalışmanın bu kısmında analiz edilen siber saldırı yöntemleri bugüne kadar yaygın şekilde kullanılmış olan yöntemlerden oluşmaktadır. Öte yandan, her yeni olay yeni bir işleniş şeklini ortaya çıkarmakta ve bunların hepsinin tanımlamasının yapılıp, tespit edilmesini sağlamak mümkün olmamaktadır. Bu açıdan verilen örnekler sınırlayıcı değil, örnekleyici bir tanımlamayı ifade etmektedir.

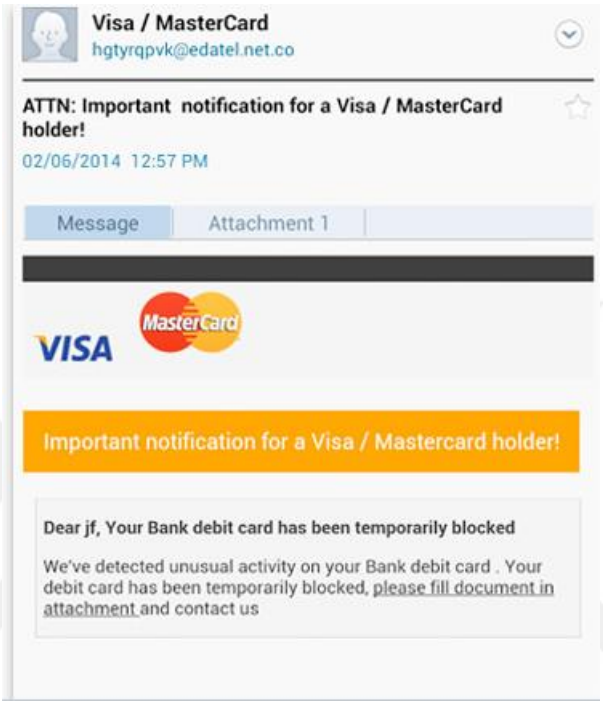
2.1.1. Oltalama (phishing[13])

Oltalama, kimlik hırsızlığı gibi kişisel verileri kopyalamak için kullanılan yöntemlerin başında gelmektedir. İnternet kullanıcılarının kandırılması ve ikna edilmesi yöntemi ile gerçek ya da tüzel kişilerin kendine özel verilerinin, kredi kartı gibi bilgilerinin ele geçirilmesini sağlayan bir internet dolandırıcılığı yöntemidir. (Canbek ve Sağıroğlu, 2007: 126) Oltalama, genellikle e-posta aracılığı ile yapılan bir yöntemdir. Kişilerin kullanmakta oldukları sosyal medya hesapları ve mail hesapları aracılığı ile kişinin müşterisi olduğu bir bankadan ya da üyesi olduğu bir kuruluştan mail geliyormuş gibi bir mail atılır. Mail içerisine yerleştirilen yönlendirme linkinin tıklanması ile bilgileri elde etmek isteyen kişinin belirlemiş olduğu yere, link aracılığı ile girilen bilgiler kaydedilir ve bu bilgiler yetkisiz kişilerin eline geçmiş olur.

Oltalama yönteminin en sık kullanıldığı alan olarak ise karşımıza finans sektörü ve resmi kuruluşlar çıkmaktadır. (APWG, 2015) Nitekim bu kuruluşlar aracılığı ile

[13] "phishing", "balık tutma" anlamına gelen ve İngilizce karşılığı "fishing" olan kelimenin ilk iki harfinin "ph" ile değiştirilmesi ile oluşan bir terimdir. Bu özgün isimlendirme yapılırken bilgisayar korsanlarının yaptığı eylemlerin gerçek hayattaki sıradan bir balık tutma eyleminin yanına farklı bir zekâ becerisinin gerekliliğini de belirtmek maksadıyla böyle bir tanımlama yapılmıştır. (Hekim ve Başıbüyük, 2013: 139) Türkçeye oltalama ve yemleme şeklinde çevrilmiştir. Bu çalışmada oltalama tercih edilmiştir.

gönderilen e-postaların kopyası yapılarak farkın anlaşılması çok zor bir hale sokulmaktadır. Bu yönteme maruz kalan kişilerin, kişisel bilgilerine ulaşan kişiler, bu bilgiler aracılığı ile kişilerin hesaplarına yetkisiz erişim ve yetkisiz işlem yapma yetisine sahip olabilmektedirler. Kötü niyetli üçüncü kişilerin bu yöntemlerle haksız kazanç elde etme olasılığı da artmaktadır (Canbek ve Sağıroğlu, 2007: 123-131).



Şekil 3 Oltalama E-postası Örneği

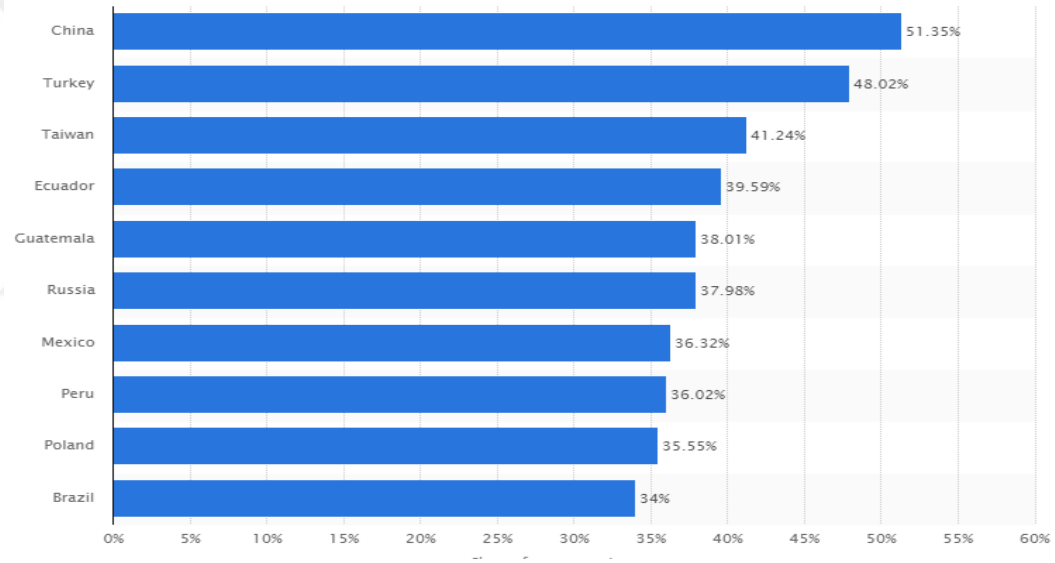
Kaynak: (Fox, 2014)

Şekil 3'te de görüldüğü gibi, resmi bir kurumdan gönderilen e-posta ile hemen hemen aynı içeriğe sahip bir e-posta oluşturularak gönderilen mailde, mail içindeki linkin tıklanıp, ilgili yerlerin doldurulması sonucu, buraya girilen bilgiler kötü niyetli üçüncü kişilerin eline geçmiş olmaktadır.

Oltalama yapan kişiler, genellikle sunucusu farklı ülkelerde bulunan web siteleri tasarlayarak bu sitelere yönlendirilen linkler aracılığı ile bilgileri elde ederek, amacına ulaştıktan sonra bu sitelerin ya sunucularını değiştirerek ya da kapatarak ulaşılabilir olmaktan çıkarlar. Özellikle bilişim hukukunda gelişmemiş ülkelerde bu sitelerde bağlantı kurulan yerlerin ve kullanan kişilerin tespit edilmesi çok zordur (Easttom ve Taylor, 2011: 7).

2.1.2. Kötücül Yazılım (malware[14])

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. Şekil 4'te de görüleceği gibi Çin başta olmak üzere Türkiye ve Tayvan'da bilgisayarlara bulaşan kötücül yazılım oranlarının daha yüksek olduğunu söylemek mümkündür (Statista, 2016).



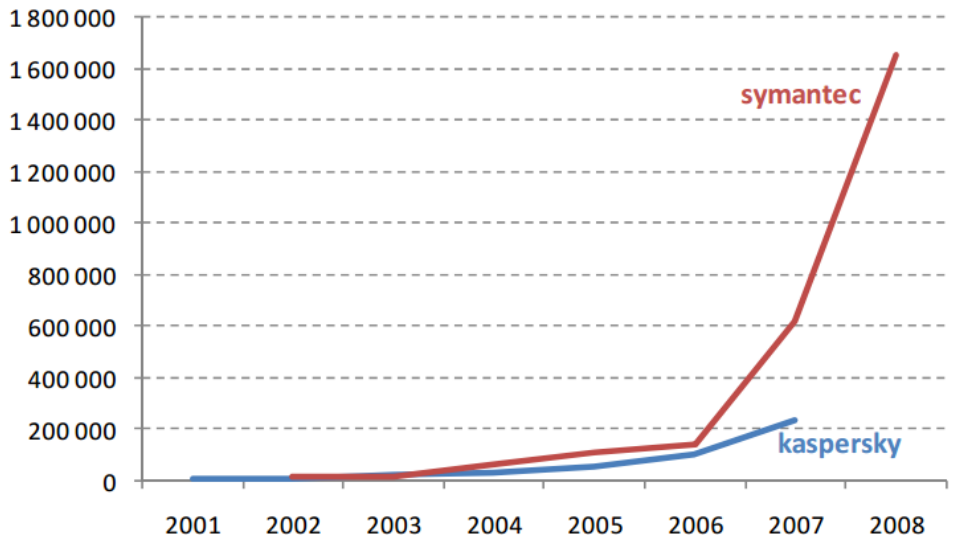
Şekil 4 Kötücül Yazılım Bulaşan Bilgisayar Oranları (2016)

Kaynak: (Statista, 2016)

Kötücül yazılımın 2008'deki mevcut çeşitliliğine Şekil 5'te yer verilmiştir. Hem çeşitliliğinin hem de miktarının her geçen gün artması, tespit edilemeyenlerin de mevcut olduğunu düşünecek olursak, kötücül yazılımın oluşturduğu tehdidin boyutunu göstermektedir. Nitekim bu tür yazılımlar aracılığı ile kötücül yazılım üretilmesi ve yayılması sonucu ülke ekonomilerinde gelir kayıpları yaşanmaktadır. ABD'nin 2007

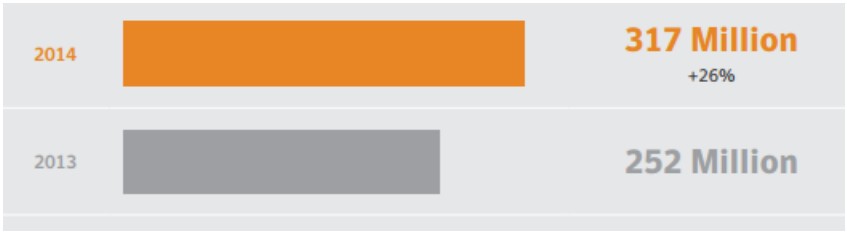
[14] Malware, İngilizce "malicious software" in kısaltmasıdır. (Christensson, 2016) Türkçe karşılığını, kötü amaçlı yazılım ve kötücül yazılım olarak kullanmak mümkündür. Bu çalışmada kötücül yazılım teriminin kullanılması tercih edilmiştir.

yılında kötücül yazılımlar sebebiyle 67,2 milyon dolar değerinde zarara uğradığı belirtilmiştir. Kötücül yazılımların suç aracı olarak kullanılması ve bunların önlenmesine yönelik alınacak tedbirleri de hesaba kattığımızda karşılaşılan zararın açıklanandan daha fazla olacağını öngörmek mümkündür. (OECD, 2009: 69)



Şekil 5 Kötücül Yazılım Miktarındaki Değişim (2001-2008)

Kaynak: (Reimsbach-Kounatze, 2012: 38)

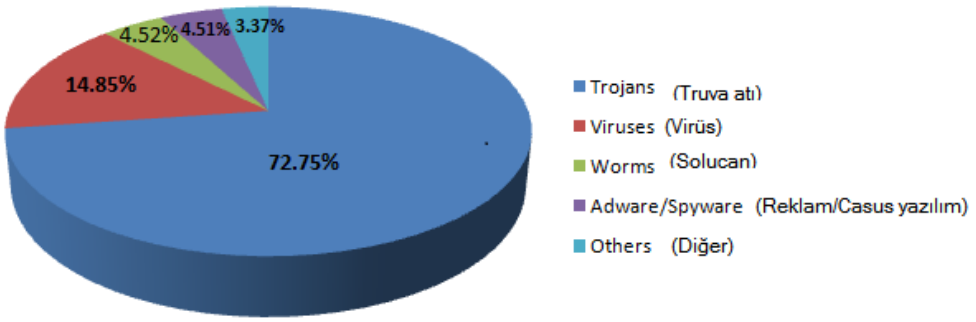


Şekil 6 Kötücül Yazılım Miktarındaki Değişim (2013-2014)

Kaynak: (Symantec, 2015: 90)

Yukarıdaki iki şekil farklı dönemleri kapsadığı için birlikte değerlendirilebilir. Şekil 5'e bakıldığında 2001 ve 2008 yılları arasındaki artış gözlemlenmektedir. Ayrıca Şekil 6'da da görüleceği üzere 2013 ve 2014 yılları arasında yaklaşık olarak %26'lık bir miktar artışı söz konusudur. Miktarı artarken çeşitliliği de artan kötücül yazılımların hem tespiti zorlaşmakta, hem de bu tür yazılımları önlemeye yönelik yeni yatırım alanları

ortaya çıkarmaktadır. Bu bağlamda sıkça rastlanılan kötücül yazılımların bilinmesinde fayda olacaktır.



Şekil 7 Kötücül Yazılım Çeşitleri (2015 1. Çeyrek)

Kaynak: (Optimo, 2015)

Optimo Antivirüs'ün yapmış olduğu çalışmaya göre en yaygın kötücül yazılım çeşitlerine değinecek olursak, Şekil 7'de de görüleceği üzere 2015 yılının birinci çeyrek verilerine göre truva atının (trojans) %72.75 ile en yaygın kötücül yazılım olduğunu söylemek mümkündür. %14.85 ile virüsler bu sıralamayı takip etmektedir. %4.52 ile solucanlar (worms) en yaygın kötücül yazılım olarak üçüncü sırada karşımıza çıkmaktadır. Reklam içerikli ve casus yazılımlar %4.51 ile en yaygın dördüncü kötücül yazılım çeşidi olarak karşımıza çıkmaktadır. (Optimo, 2015) Bu bağlamda çalışma kapsamında Truva atı, virüs, solucan ve reklam içerikli ve casus yazılımlar kısaca irdelenecektir.

2.1.2.1. Truva Atı[15]

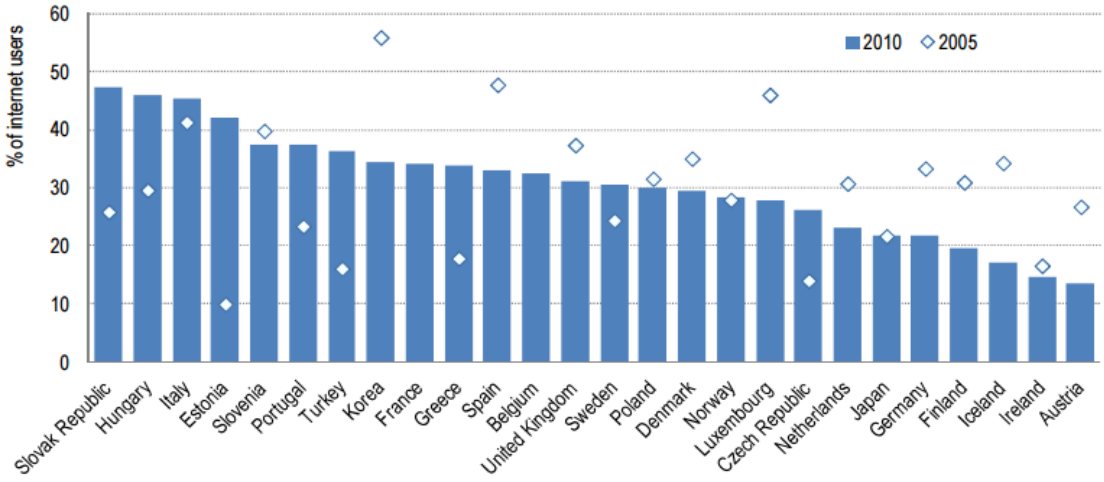
Truva atı, internet kullanıcıları için faydalı gibi görünen ancak içinde barındırdığı zararlı kodlar sebebiyle bilişim güvenliğine zarar veren bir program türüdür (OECD, 2009: 229). Truva atları, bilgisayarları kullanıcılarının isteğinin dışında yönetmek ve bilgisayarlara erişim sağlamak için kapı açan programlardır. Özellikle lisanslı ve ücretli

[15] Bu kötücül yazılıma Truva atı isminin verilmesinin sebebi Yunan mitolojisindeki bir armağan gibi görülen, Truva kentinin ele geçirilmesi için Yunanlı askerleri taşıyan tahta bir ata verilen isimden kaynaklanmaktadır. Kötücül yazılım olarak Truva atı, diğer zararlı yazılımlarda olduğu gibi kendi kendine çalışmaz ve kullanıcının bunu çalıştırması gerekir. Tıpkı tahta bir ata Yunanlıların içeri alınmadan bir faydasının olmayacağı gibi kullanıcı da Truva atını çalıştırmazsa kopyalanıp dağıtılmış olmasına rağmen zarar vermez. (Dülger, 2004)

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[16]) aracılığı ile kullanıcının bağlı olduğu sistemlere erişim sağlayarak kullanıcın bilgilerini kullandığı şifreleri ele geçirebilir (Canbek ve Sağıroğlu, 2007: 124).

2.1.2.2. 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).



Şekil 8 Virüse Maruz Kalan Kullanıcı Yüzdesi (2005-2010)

[16] İngilizce karşılığı "back door" olan "arka kapı" bilgisayarlar üzerindeki normal kimlik tanımlama süreçlerini ve kullanıcı bilgilerini atlatarak yetkisiz erişim için oluşturulan ve kullanıcının bilgisi dışında uzaktan erişimi kapsayan yöntemler olarak tanımlanabilir. Truva atları ile sisteme erişim noktasında benzer olmalarına rağmen Truva atı iyi gibi görünen ve zararlı bir yazılımdır, arka kapılar ise sadece sisteme erişimi sağlayan gizli yapılardır. Sistemi oluşturan kişilerin sistemi test etmek için bıraktıkları açıkların sonradan kapatılmasının unutulması suretiyle ya da sisteme sızarak daha sonradan erişim sağlamak amacıyla bilgisayar korsanları tarafından açık bırakılan portlar aracılığı ile kullanılan bir yöntem olarak karşımıza çıkmaktadır. (Canbek ve Sağıroğlu, 2007)

Kaynak: (Reimsbach-Kounatze, 2012: 23)

Şekil 8'de 2005 ve 2010 yıllarına ait olan internet kullanıcılarının ne kadar virüse maruz kaldığı verilmiştir. Estonya en fazla artış oranı gösteren ülke olarak karşımıza çıkmaktadır. 2005 yılında en fazla virüse maruz kalan ülke Kore iken 2010 yılında ise Slovak Cumhuriyeti olmuştur.

Virüslerin maddi zarar veren boyutlarına en güzel örnek 3 Mayıs 2000'de Filipinli bir genç tarafından yazılan ve bir gecede milyonlarca bilgisayara bulaşan "i love you" virüsü verilebilir. Tüm dünyada yayılan ve e-posta eki olarak gelen "i love you" isimli dosyanın çalıştırılmasıyla bilgisayarlara bulaşan virüs kısa sürede yaklaşık olarak 55 milyon bilgisayara ulaşarak bunların 3 milyon kadarına bulaşmıştır. Bulaştığı bilgisayarlardan kullanıcıların şifrelerine ve kişisel bilgilerine erişim sağlayan virüsün, uğrattığı maddi zarar ise yaklaşık olarak 8 milyar dolar olarak açıklanmıştır (Ward, 2010).

2.1.2.3. 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 adetine 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 bu süre içinde 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).

2.1.2.4. Reklam İçerikli 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. Reklam içerikli yazılımlar, web[17] tarayıcıları aracılığı ile bilgisayara yerleşerek sürekli kullanıcının isteği dışında, sayfaların açılmasına ve reklamı yapılan sayfalara yönlendirmelere sebep olmaktadır. 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[18]) da dâhil 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

[17] İngilizce karşılığı web olarak kullanılan kelimenin Türkçe karşılığı "ağ" olarak kullanılmakla birlikte kelimenin anlamını tam olarak karşılamadığı düşünüldüğü ve "network" kelimesi ile karıştırılabileceği için çalışmada orijinal dilindeki hali ile kullanılmıştır.

[18] "Spam" bir Amerikan firmanın baharatlı domuz eti için kullandığı "spiced pork and ham" kelimesinin baş harflerinden oluşan Amerikan kökenli bir kelimedir. İngilizce karşılığı spam olan, istenmeyen e-postalar genellikle pazarlama ve reklam amaçlı kendi tanıtımını yapmak isteyen firmaların/kişilerin kendi tanıtımlarını karşı tarafın isteği olmadan cep telefonu, e-posta gibi yöntemlerle kullanıcılara ulaştırmasıdır (Memiş, 2001, s. 431).

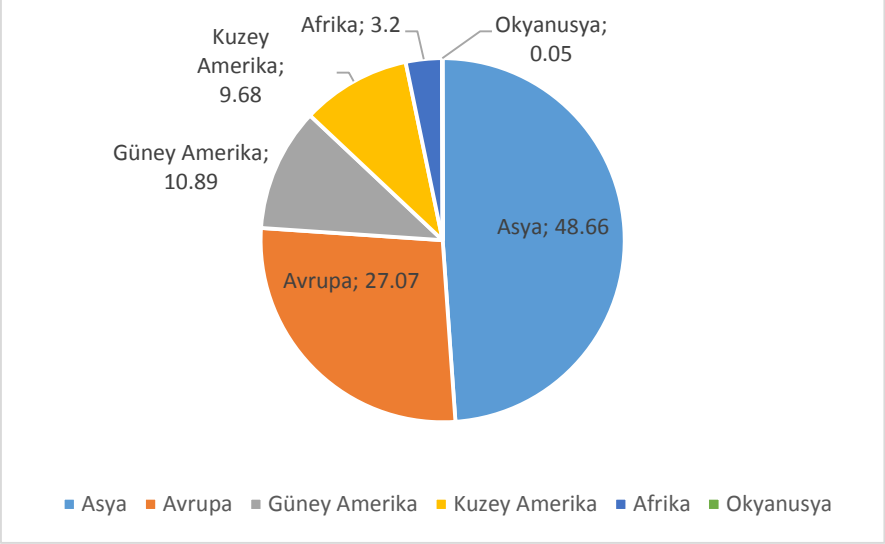
bilgisayarlara da bu içerikler gönderilerek bu tür cihazların da kötücül yazılımlara malzeme olması sağlanmaktadır (OECD, 2006).

Ülke	Yüzde(%)	Ülke	Yüzde(%)
1.Hindistan	% 12.19	7.Rusya	% 3.34
2.ABD	% 7.06	8.Fransa	% 3.04
3.İtalya	% 6.95	9.Pakistan	% 2.95
4.Kore	% 5.37	10.Polonya	% 2.77
5.Brezilya	% 4.17	11.Endonezya	% 2.73
6.Vietnam	% 4.16	12.Çin	% 2.73

Şekil 9 En Fazla İstenmeyen E-posta Üreten 12 Ülke (2013)

Kaynak: (Sophos, 2013: 27)

Şekil 9'da Sophos'un araştırma verilerine göre en fazla istenmeyen e-posta üreten ülkeler verilmiştir. Toplam istenmeyen e-posta miktarı dikkate alındığında 2013 yılı itibariyle en çok istenmeyen e-posta üreten ülke %12.19 ile Hindistan, ikinci ise %7.06 ile ABD'dir. Bu veriler göze alındığında AB üyesi ülkelerin de dünyada en fazla istenmeyen e-posta üreten ülkelerden olduğu görülmektedir.



Şekil 10 Kıtaya Göre İstenmeyen E-posta (2013)

Kaynak: (Sophos, 2013: 27)

Şekil 10'da da kıtalara göre istenmeyen e-posta üretim oranları yüzdesel olarak gösterilmiştir. Kıtalara göre değerlendirme yapmak gerekirse Şekil 10'da da görüleceği gibi toplam istenmeyen e-posta miktarının %48.66'lık bir oranı Asya ülkelerinden çıkmaktadır. %27.07'lik oranla bunu Avrupa izlemektedir. Bu da AB'nin siber saldırılara karşı önlem almak istemesinde önemli bir veri olarak karşımıza çıkmaktadır.

Kötücül yazılımlara bir başka örnek ise, 2008 yılında ABD'deki Başkanlık seçimleri öncesi "Obama Başkanlığı reddedecek" içerikli bir e-postadır. Bu e-posta yoluyla dünyada başlayan dalgada, kötücül yazılımlar kullanıcıların bilgisayarlarına bulaşarak büyük miktarda zarara yol açılmıştır (SophosLabs, 2008).

Casus yazılımlar, hedef sisteme bulaştıktan sonra kendilerini çoğaltma ve daha fazla yaymaya ihtiyaç duymazlar. Bu özellikleri ile virüslerden ve solucanlardan farklı olarak değerlendirilebilirler. Kurban olarak seçilen bilgisayarlara yerleştikten sonra gizli kalarak istenilen bilgileri toplayarak amacına ulaşmış olurlar (OECD, 2009). Reklam içerikli yazılımlar ise sisteme bulaştıktan sonra kullanıcıya gösterilecek reklamların çalıştırılmasını sağlar, casus yazılımlardaki gibi kullanıcıların kişisel bilgilerinin toplanıp üçüncü kişilere ulaştırılmasını kapsamamaktadır. Temel amacı reklamları kullanıcıya göstermektir (Canbek ve Sağıroğlu, 2007). Bu kısımda değerlendirilen bir diğer yöntem olan istenmeyen e-postalarda ise casus ve reklam içerikli yazılımlardan daha farklı olarak ticari kaygı motivasyonu biraz daha yüksektir. Nitekim genellikle pazarlama aracı olarak kullanılabilen bir unsur olarak karşımıza çıkmaktadır.

2.1.3. Botnet[19]

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

[19] İngilizce "robot" kelimesinin son üç harfi ve "network" kelimelerinin ilk üç harfinin birleşmesiyle oluşmuştur.

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).

Botnetler, farklı amaçlarla kullanılabilmektedir. Bunlardan bir kaçını şu şekilde sıralayabiliriz: virüsleri yaymak, reklam ve casus içerikli e-posta iletileri (spam) göndermek, bilgisayar ve sunuculara saldırmak ve diğer türlerdeki suçları işlemek. (Microsoft, 2016) Botnetlerin asıl hedefinin ev kullanıcıları olduğu bilinmektedir. Nitekim Google tarafından evlerde kullanılan bilgisayarların yaklaşık %10'unun botnet ağlarının birer parçası olduğu ve yaklaşık yüz milyon civarı bilgisayarın botnet ağlarında olduğu belirtilmiştir (Milliyet, 2011).

Şekil 11 Botnetlerin İşleyişi

Kaynak: (Karabağlı, 2015)

Şekil 11'de görüldüğü gibi bilgisayar korsanı tarafından zombiler üzerinde kurulan kötücül yazılımlar belirli bir kaynaktan gelecek DDoS[20] komutları uygulayarak hedef sisteme saldırıları gerçekleştirmektedir. Bu şekilde kullanıcıların isteği dışında kişisel bilgisayarları farklı emellere hizmet etmesi amacıyla kullanılmış olmaktadır.

[20] Bu kavram için detaylı inceleme bir sonraki başlıkta yapılmıştır.

2007 yılındaki Birleşmiş Milletlerin (BM) resmi sitesine yapılan siber saldırıyı botnet saldırısına örnek olarak verebiliriz. BM'nin resmi sitesine Türk bilgisayar korsanları tarafından yapılan siber saldırıda ABD ve İsrail'in Ortadoğu politikalarına protesto olarak da "Hey İsrail ve ABD, çocukları ve diğer insanları öldürmeyin. Barış evrenseldir. Savaşa hayır," notu bıraktıkları görülmüştür (BBC, 2007a). Öte yandan, AB ülkelerini etkileyen önemli botnet saldırıları şunlardır; 2007 ve 2008 yıllarında Estonya[21] ve Litvanya devlet kurumlarına yapılan siber saldırılar, 2008 yılından itibaren yayılmaya başlayan "Conficker"[22] isimli botnet. (Malmström, 2010). Bu saldırıların temel amaçları ise banka hesaplarından para aktarmak ve bankaların gizli finansal bilgilerini deşifre etmek, kullanıcıları belli tutarlar ödeyerek virüsten kurtarmaya yönelik gasp faaliyetleri, devletlerin kritik güvenlik altyapı faaliyetlerine zarar vermek için gerçekleştirilen sabotaj faliyetleri, bir devlet ya da örgüte yasadışı baskı olarak sıralanabilir. (Malmström, 2010).

2.1.4. Hizmeti Engelleme (DoS/DDoS[23]) 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).

[21] Estonya hükümetine yönelik gerçekleştirilen siber saldırıların uğrattığı zararın 19-28 milyon Euro aralığında olduğu tahmin edilmektedir. (Malmström, 2010)

[22] Conficker isimli botnetin 12 milyon civarında bilgisayara bulaştığı ve günde 10 milyar civarında spam e-posta ürettiği bilinmektedir. Fransa, İngiltere ve Almanya bu botnet saldırılarından en çok etkilenen ülkelerden olmuştur. 2009 Ocak ve Şubat aylarında Birleşik Krallık Savunma Bakanlığı personellerinin e-posta hesaplarını bu botnetlerin verdiği zararlar dolayısı ile kullanılamadığı bilgisi verilmiştir. (Malmström, 2010)

[23] DoS (Denial of Service)/DDoS (Distributed Denial of Service) İngilizce'deki kullanımı ile hizmeti engelleme/dağıtılmış hizmeti engelleme saldırıları anlamına gelmektedir. DoS ve DDoS arasındaki fark katılımcı sayıları ile ilgilidir. DDoS, botnetler aracılığı ile birden çok bilgisayarın aynı hedefe yönlendirilerek gerçekleştirildiği saldırılar için kullanılan isimdir.

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).

Hizmeti engelleme saldırılarına örnek olarak; 2014 yılında İngiltere istihbarat biriminin bir parçası olan Hükümet İletişim Karargâhı (GCHQ-Government Communications Headquarters), Anonymous ve LulzSec gibi bilgisayar korsanlığı yapan grupların iletişim kurmakta kullandığı sohbet odalarına DDoS saldırı düzenlemiştir. (Collins, 2014) 2008 - 2014 yılları arasında Esad yönetimine bağlı çalışan istihbarat birimlerinde Irak istihbarat servisi (Genel Güvenlik Departmanı, GSD -General Security Department) ve Suriye istihbarat servisi (Hava Kuvvetleri İstihbarat İdaresi, AFID- The Air Force Intelligence Directorate) ele geçiremediği elektronik servislere sayısız DoS saldırısı düzenlemiştir. (Haberler.com, 2015) 2012 yılında Orta Doğu ülkelerini hedef alan flame virüsünün[24] altyapı sistemlerini servis dışı bırakmayı amaçlayan Ulusal Güvenlik Ajansı (NSA-National Security Agency) ve GCHQ yapımı bir kötücül yazılım olduğu iddia edilmiştir (Nakashima, Miller ve Tate, 2012; McElroy ve Williams, 2012). 2010 yılında ortaya çıkan Stuxnet'in[25] de, İran nükleer santrallerindeki Siemens -Gözetici Kontrol ve Veri Edinme – (SCADA-Supervisory Control and Data Acquisition) sistemlerine saldırıp, sistemlerin düzenli çalışmasını aksatmayı başaran ve SCADA sistemlerini servis dışı bırakan NSA ve MOSSAD (İsrail İstihbarat Servisi) ortak yapımı bir kötücül yazılım olduğu iddia edilmiştir (Bölükbaş, 2014). Örneklerden de anlaşılacağı gibi, hizmeti engelleme saldırıları sadece bireyler tarafından kullanılan ve bireyleri

[24] "Flame (alev) virüsü, casusluk faaliyetlerini sürdürebilmek amacıyla, klavye, USB bağlantılar, işlemci, mikrofon, depolama aygıtları, kablosuz ağlar, monitör, Bluetooth gibi birçok donanımı kullanabilecek kapasiteye sahiptir. Sızdığı bilgisayarlarda kendini belli etmemek için beş farklı şifreleme algoritması ile kendini kriptolayarak gizleyebilen virüs, casusluk işlemlerini arka planda yapabilmektedir." (Karspersky, 2015) "Yapılan incelemelerde virüs başta İran, İsrail, Sudan, Suriye, Lübnan, Suudi Arabistan ve Mısır olmak üzere 600 den fazla kuruluş, akademik kurum ve devlet sisteminin hedef alındığı tespit edilmiştir. Virüs, 2010 Mart ayında Karspersky tarafından tespit edilmiştir." (Lee, 2012; Greenfield, 2012)

[25] Stuxnet Microsoft'un güvenlik uyarısıyla gündeme gelmiştir. Hedefi veya hedefleri hakkında özel bilgilere sahip olması gereken, çoklu sistem eksikliklerinden yararlanabilen, illegal yollarla ele geçirilmiş güvenlik sertifikaları sayesinde sistemlere erişerek bu sistemleri kilitleyip işlerliğini ortadan kaldıran özel ve çok gelişmiş bir virüs olarak tanımlanabilmektedir (Bıçakçı, 2013: 42).

etkileyen bir saldırı türü değildir. Devletler için de güvenlik tehdidi olarak kendini göstermektedir. Hatta devletler tarafından da kullanılmaktadır.

2.1.5. 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).

Sosyal mühendislik saldırı örnekleri genellikle finans sektörü ile ilgili olarak dolandırıcılıklarda karşımıza çıkmaktadır. Nitekim kişilerin zaaflarından faydalanılarak ele geçirilen bankacılık işlemlerinde kullanılan şifreler aracılığı ile hesapların boşaltılması örnekleri oldukça fazladır. 2007 yılında bir banka müşterisinin yaklaşık 20.000,- TL sinin sosyal mühendislik sonucu elde edilen kişisel bilgiler üzerinden dolandırıldığı görülmüştür (İnternethaber, 2008).

Tarih: 10 Kasım 2010, Çarşamba, 11:41
Gönderen: ahmetzen@golfgrup.com
Alıcı: sensin@postaci.com
Konu: yakın akraba

Sevgili Arkadaşım,
Ben Ali Gücen, Singapurda ve deneyimli bir muhasebe uzmanı olarak Bahraid Bankasında çalışmaktayım. Bu fırsatı size haber vermek ve sunmaktan büyük bir mutluluk duyuyorum; sizinle aynı soyadı taşıyan eski bir müşterimi geçtiğimiz pazar günü (07.11.2010) kalp krizi nedeniyle kaybettik. 26 Aralık 2004'te Sumatra yakınlarında gerçekleşen tsunami nedeniyle müşterim bütün yakınlarını, yani bütün varislerini kaybetmişti. Müşterimin hesabında bulunan 3.7 milyon dolar para için herhangi bir yakın akraba bulunamadı.

Müşterimin yaşayan hiçbir yakın akrabasının kalmadığından emin olduktan sonra, tek soyadı tutan kişi olarak, yakın akrabalık konusunda sizinle temasa geçmemin uygun olduğunda karar verdim. Ölen müşterimin tek varisi olarak kalan kaynağın size aktarılmasını planlayabilirim. Bu konuda herhangi bir çekinceniz olmaması için gerekli yasal bilgi ve belgelerin sizin adınıza düzenleneceğinizi belirtirim.

Mirasın sizin adınıza devriyle ilgili son tarihi kaçırmamak için ivedi olarak sizden bu konuda işbirliği ve anlayış konusundaki cevabınızı bekliyorum. Bu konuyla ilgileniyorsanız ve benimle işbirliği yapmayı kabul ediyorsanız, benimle hemen irtibata geçiniz. Size konuyla ilgili bilgi ve belgelerle birlikte, sizden ödeme için istenen dokümanlar konusunda en kısa zamanda iletişime geçeceğim. Bu süreçte hukuki işlemler için gerekli olan harcamaların %35'i sizin tarafınızdan, %65'i benim tarafımdan karşılanacaktır.

Saygılarımla,
Ahmet Akın,
mhyakin@safim.com

Şekil 12 E-posta Aracılığı İle Yapılan Sosyal Mühendislik Saldırısı Örneği

Kaynak: (BİLGEM, 2015)

Şekil 12'de görüldüğü gibi bir e-posta da sosyal mühendislik saldırılarında araç olarak kullanılabilmektedir. Şekildeki örnekte, hedefin sosyal mühendislik saldırısı sürecine bir şekilde dâhil olmasını sağlayan sahte bir senaryo uydurularak, kurbanı para kazanacağına inandırmak amacı ile bir e-posta gönderilmektedir. Kendisi hakkında güven kazanmak amacıyla çeşitli sahte kimlikler hazırlanarak, e-posta, kısa mesaj ve telefon açma yöntemlerinin üçünü bir arada kullanmak suretiyle gerçekleştirilen bir sosyal mühendislik saldırı örneği bu şekilde gerçekleşmektedir.

Bu noktada belirtmek gerekir ki, buraya kadar verilen siber saldırı tekniklerinden farklı olarak kullanılan birçok başka siber saldırı türü bulunmaktadır. Dünyada en yaygın kullanılan yöntemler bunlar olduğu için çalışma kapsamında bunların değerlendirilmesi yeterli görülmüştür. Yukarıda belirtilen siber saldırı tekniklerine ek olarak; kriptografik saldırılar[26], zamanlama saldırıları (timing alalysis)[27], IP aldatmacası (IP spoofing)[28], oturum çalma (session hijacking)[29] gibi siber saldırı teknikleri de bulunmaktadır (Çifci, 2013). Nitekim gelişen teknoloji ile bu çeşitlilik sürekli artış göstermektedir. Bütün bunlara ek olarak devletler ve uluslararası örgütler için önemli bir siber tehdit çeşidi olarak APT saldırılarının değerlendirilmesinde de fayda olacaktır.

2.2. 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)

[26] Kriptografik saldırılar, şifrelenmiş bilgilerin şifresini kırmak ya da çözmek için gerçekleştirilen saldırıları ifade etmektedir. (Canbek ve Sağıroğlu, 2007)
[27] Zamanlama saldırıları, sabit veri işleme zamanına sahip olmayan algoritmaların sızdırdığı zamanlama yan-kanal bilgisinden faydalanılarak gerçekleşen saldırıları ifade etmektedir. (Kocher, 1996: 106)
[28] IP aldatmacası, sahte kaynak IP adresi ile internet protokolü oluşturulmasını ifade etmektedir. Yapılan işlemler oluşturulan sahte IP adresi üzerinden gerçekleştiriliyormuş gibi görülür. (Velasco, 2000)
[29] Oturum çalma, farklı bir kullanıcının oturumuna sahip olmaya olanak sağlayan siber saldırı türlerini ifade etmektedir.

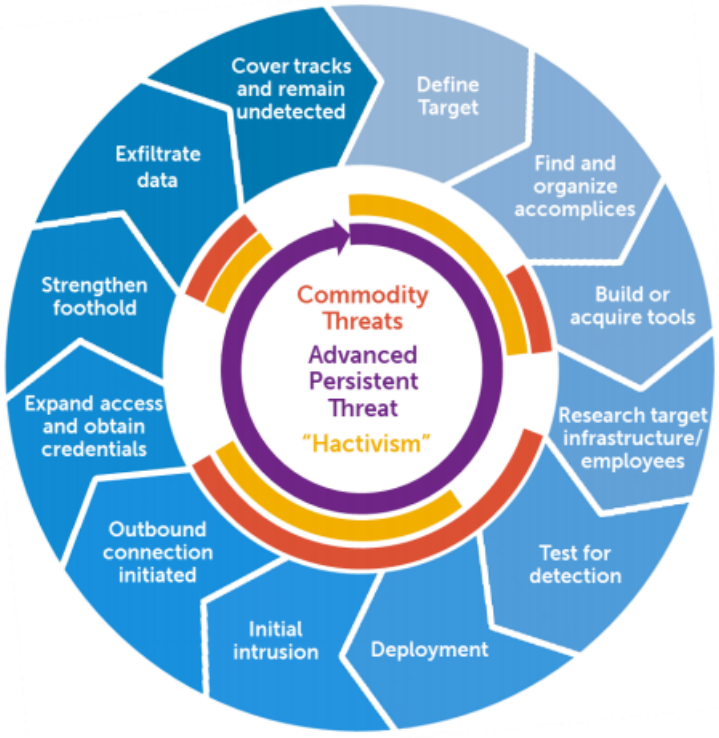
APT saldırılarında aşağıdaki üç hususun birlikte sağlanması gereklidir (NIST, 2011):

i) Uzun bir zaman süresi boyunca sürekli olarak amaçlarının sağlanması için ağa yerleşmek,

ii) Bulunduğu ağdaki savunuculara (antivirüs programları ve güvenlik duvarları) karşı adaptasyon sağlamak,

iii) Sonuca ulaşmak amacıyla gerekli etkileşim düzeyini korumak için kararlı olmak.

Yukarıda belirtilen koşullardan yola çıkılarak APT saldırılarının anatomisinin Şekil 13'teki gibi olduğunu söylemek mümkündür.



Şekil 13APT Saldırılarının Anatomisi

Kaynak: (ENISA, 2014: 3)

Şekil 13'te de görüleceği üzere APT saldırıları hedefin tanımlanması (define target) ile başlar. Hedef belirlendikten sonra sırasıyla şu aşamalardan geçilerek sonuca ulaşılmaya çalışılır: Suç ortakları bulmak ve organize etmek, gerekli araçları kurmak veya elde etmek, hedef altyapı ve çalışanlarla ilgili araştırma yapmak, tespit için test yapmak,

konuşlanmak, güvenliği kırmak ve ilk saldırıyı yapmak, giden bağlantıyı başlatmak, erişimi genişletmek ve kimlik edinmek, dayanağı güçlendirmek, verileri çekmek, fark edilmeden kalmak ve izleri örtmek. Başarılı bir APT saldırısı için bu aşamalarının tamamının sağlanması gerekmektedir. APT saldırıları, yukarıda sayılmış olan siber saldırı tekniklerinin bir ya da bir kaçının birlikte kullanılması ile gerçekleştirilebilir. Oltalama, sosyal mühendislik gibi saldırı teknikleri ile arka kapılar oluşturularak hedef ağlara yerleşilerek saldırılar gerçekleştirilir. (Rouse, 2010)

APT saldırılarının en bilinen örneği Sofacy grubu olarak da bilinen APT 28 grubunun gerçekleştirmiş olduğu saldırılardır. (BBC, 2016) Saldırılarını Gürcistan, Doğu Avrupa ve NATO üyesi ülkelerdeki kişiler üzerinde yoğunlaştıran APT 28 grubunun Rus kaynaklı bir siber casus grup olduğu öne sürülmektedir. Nitekim yapılan saldırılardaki yazılım dilinin Rusça olması, hedef alınan sektörlerin ve ülkelerin Rusya'nın çıkarlarına uygun olması ve saldırı saatlerinin Rusya'daki mesai saatleri ile uyumlu olması gibi sebeplerden dolayı Rus devleti kaynaklı bir siber saldırı grubu olduğu düşünülmektedir. 2007 yılından beri gerçekleştirdiği ve tespit edilen saldırılar sonucunda Gürcistan başta olmak üzere birçok devlet kurumunun bilişim sistemleri altyapılarına önemli ölçüde zarar verdiği bilinmektedir. 2013'te tespit edilen bir saldırısında ise Gürcistan'da ehliyet sahibi olan kişilerin bulunduğu excel dosyasına yerleştirilen zararlı yazılım aracılığı ile Gürcistan İç İşleri Bakanlığında bulunan bilgisayarlara zarar verdiği tespit edilmiştir. (Fire Eye, 2014)

APT 28 siber casusluk grubunun; Norveç Ordusu, Meksika hükümeti, Pakistan Deniz Kuvvetleri, Avrupa Birliği Komisyonu, Dünya Bankası, OPEC, Hizb ut-Tahir, Macaristan Hükümeti, Özbekistan Dışişleri Bakanlığı, Türkiye'deki Askeri Ataşelikler gibi kurumları hedef olarak belirlediği düşünülmektedir. (Fire Eye, 2014) Alman parlamentosuna yönelik seri halinde devam eden siber saldırıların da bu grup tarafından yapıldığı öne sürülmektedir. Rusya'nın bu suçlamalara karşılık cevap vermemesi de bu ihtimali güçlendiren bir durum olarak karşımıza çıkmaktadır. (BBC, 2016)

APT 28 siber saldırı grubunun stratejik kurumlara yönelik saldırılarında genel olarak şu adımları izlediği gözlemlenmiştir: Oltalama saldırısı ile hedef kaynağa erişimin sağlanması, zararlı yazılımın kurulması, diğer saldırı bileşenlerinin yüklenmesi, yerleşilen ağ ve sistem üzerinde yatay hareketin sağlanması, hedefin bulunması ve verinin

sızdırılması. (Fire Eye, 2014) Bu aşamalardan geçen bir APT 28 grubu saldırısının başarı ile sonuçlandığını söylemek mümkündür.

APT saldırılarının kurum ve kuruluşların bilgi sistemleri altyapılarına sızarak ve yerleşerek bu ağlara ve sistemlere kalıcı zararlar verdiği düşünülmektedir. Buradan hareketle her hangi bir zaman ve mekân sınırı olmayan bu tür saldırıların hedefinde AB kurumları ve AB üye devletlerinin de olabileceğini söylemek mümkündür. APT saldırıları, AB'nin ve üye ülkelerinin güvenlik değerlendirmelerinde ve siber güvenlik politikalarının oluşturulmasında – yani siber uzayın güvenlikleştirilmesinde – referansta bulunulan önemli bir tehdit olarak karşımıza çıkmaktadır. Ayrıca, özellikle askeri hedeflerin seçilmesi sebebi ile askeri güvenlik sektörü ile siber güvenliğin bağlantısını net olarak ortaya koyan bir örnek olduğu da söylenebilir.

2.3. AB'de Siber Saldırı Örnekleri

AB'nin siber güvenlik politikası oluşturma sürecinde yukarıda belirtilen siber tehditlerin varlığı büyük önem taşımaktadır. Bununla birlikte dünya genelindeki siber saldırı örnekleri ve siber uzayın bir sınırının bulunmaması bir diğer sebep olarak karşımıza çıkmaktadır. Ayrıca her an bir siber tehdit ile karşı karşıya kalınabilecek olması büyük önem arz etmektedir. Bu bölümde de AB üyesi ülkelere gerçekleştirilen siber saldırılara örnekler verilmiştir. Ayrıca siber olayların güvenlikleştirilmesi sürecinde AB yetkililerinin söylemleri ile önerileri de analiz edilen konulardandır.

2.3.1. Estonya Örneği

2007 yılında Estonya hükümeti tarafından, Rusların Estonyalıları Nazi işgalinden kurtarmasını simgeleyen Kızıl Ordu Anıtının kaldırılması üzerine yaklaşık bir ay süresince Estonya internet altyapısı ve kamuya ait web sayfaları ve bankacılık hizmetleri siber saldırıya uğramıştır. Rusya'daki bazı internet sitelerinde siber saldırıların nasıl yapılacağına ilişkin yöntemler verilerek, siber saldırıların amatör bilgisayar kullanıcıları tarafından da kolaylıkla yapılabileceği gözler önüne serilmiştir (BBC, 2007b).

Resmi kurum ve kuruluşlarında internet altyapısını en yoğun kullanan ülkelerden olan AB üyesi Estonya'ya düzenlenen bu saldırı neticesinde birçok resmi web sayfası kilitlenmiş ve hizmet veremez hale gelmiştir. DDoS siber saldırı yöntemine maruz kalan

Estonya'ya yapılan siber saldırı on binlerce zombi bilgisayar tarafından gerçekleştirilmiştir (Richards, 2009).

30 Nisan-18 Mayıs 2007 tarihleri arasında ise siber saldırılar etkisini artırarak daha organize şekilde düzenlenmeye başlanmıştır. Estonya'nın ulusal bilgi iletişim ağları, internet hizmet sağlayıcıları büyük zararlar görmüştür. Ülkenin en büyük bankası olan Hansabank'a yapılan saldırılar sonucu bankanın sistemleri çökmüş ve hizmet veremez hale gelmiştir. Estonya'nın saldırılardan Rusya'yı sorumlu tutup konuyu NATO (Kuzey Atlantik Antlaşması Teşkilatı - NATO) gündemine taşımasıyla, NATO tarafından Estonya'ya siber-terörizm uzmanları gönderilmiştir. İletişimin ve ticaretin sürekliliğini durma noktasına getiren saldırıların, birçok farklı ülkeden yapılmış olmasına rağmen ana kaynağının Rusya'da bulunan ve Kiril alfabesiyle yazılan bir programdan kaynaklandığı tespit edilmiştir. Ancak Rusya'dan, bu saldırıların Rus hükümeti tarafından gerçekleştirilmediği yanıtı verilmiştir. Yine de suçlamaları reddeden Rus hükümeti suçluların bulunması konusunda ise Estonya'ya gerekli bilgileri vermeyeceğini açıklamıştır. (Traynor, 2007)

Gelişmiş bilişim sistemlerine sahip olan Estonya örneğinde de olduğu gibi, bu sistemlere bağımlı olmak, aynı zamanda siber saldırılar için son derece savunmasız olmak anlamına da gelebilmektedir. Nitekim bankaların, finans kurumlarının, devlet dairelerinin ve borsanın faaliyetlerinin durma noktasına gelmesi Estonya'da günlük yaşamı sürdürülemez hale getirmiştir. Klasik savaş yöntemleri ile kıyaslayınca, bilişim sistemlerine yapılan saldırılar yoluyla bir devletin ya da örgütün daha düşük maliyetlerle, daha kısa sürelerde büyük çapta zarara uğratılabildiği görülmüştür.

AB'nin etkili bir siber güvenlik politikasının oluşturulabilmesi için verilen demeçlerde sıkça referans gösterilen bir olay olarak Estonya örneği önemli bir yere sahiptir. Nitekim dönemin AB İçişlerinden sorumlu Avrupa Komisyonu üyesi Anna Cecilia Malmström 30 Eylül 2010'da verdiği basın demecinde, Estonya örneğine de referans göstererek siber saldırılara karşı AB'nin önlem alması ve bu önlemlerin birlik genelinde uygulanabilecek düzenlemeler ile kalıcı hale getirilmesi gerektiğine vurgu yapmıştır (Malmström, 2010). Daha detaylı vermek gerekirse; basın demecinde Malmström: "Siber suçlular bugün tahribat yaratmaktan ziyade maddi kazanç arzusu ile motive olmaktadırlar. Elektronik vandalizmin bir türü olarak zararlı yazılım yaymak yerine, önemsiz e-posta göndermek, banka hesaplarından para aktarmak, kredi kartı

numaraları çalmak, reklamların görüntülenmesi veya içine bir arka kapı sağlamak gibi amaçlarını gerçekleştirmek için zararlı kodlar oluşturarak cihazlara bulaştırmaktadırlar." şeklindeki ifadeleri ile güvenlikleştirme sürecinin unsurlarından olan tehditi siber suç işleyenler ve zararlı yazılımlar olarak tanımlamaktadır. Devamında "Kişisel bilgisayarlarınız banka güvenlik sistemlerinin çökertilmesi ve hesabınızdan para aktarmak için ya da kredi kartı numarası gibi hassas bilgileri çalmak için diğer binlerce bilgisayarla birlikte kullanılabilir." diyerek bireyleri tehdite maruza kalacaklar olarak – yani başvuru nesnesi olarak– işaret etmektedir. Malmström, mevcut yasal boşlukların bulunduğunu ve tehditin ortadan kaldırılması gerekliliğini ise "Mevcut yasal çerçevenin iki önemli zayıflığı bulunmaktadır: Bilgi sistemlerine karşı gerçekleşen geniş çaplı saldırılara yeterli cevap verilememektedir. Bilgi sistemlerine karşı saldırılar için kullanılan botnet ve benzeri yöntemlere ilişkin yasal hükümlerin olmamasından ve büyük ölçekli saldırılar ile ilgili caydırıcı cezalar olmamasından kaynaklanmaktadır." sözleriyle dile getirmektedir. Ayrıca demecinin sonlarında yer verdiği "Bu tür saldırılara karşı sınır ötesi işbirliği konusunun hızlı bir şekilde ele alınması gerekmektedir. Devam eden saldırılara karşı operasyonel işbirliği yapmaya yönelik mekanizmalar Üye Devletlerin, özellikle diğer kolluk kuvvetleri tarafından yardım taleplerini karşılama ve yanıt verme açısından olması gerektiği gibi etkili değildir." ifadeleri ile de durumun acil önlem alınması gereken bir tehdit unsurunu içerdiğine vurgu yapmaktadır. Çalışmanın kuramsal temellendirmesini oluşturan güvenlikleştirme sürecinde söz ediminin örneği olarak bu basın demecini ve tehdidin oluşturulup alımlayıcı kitleye kabul ettirilme gayretini etkili bir örnek olarak verebiliriz. Basın demecinde kullanılan her kelimenin bu bağlamda özenle seçilmiş olduğunu söylemek yerinde olacaktır. Ek olarak dönemin Dijital Ajandadan sorumlu Avrupa Komisyonu üyesi Neelie Kroes ile birlikte verdikleri yasal düzenleme önerileri de güvenlikleştirme sürecinin önemli belgeleri olarak karşımıza çıkmaktadır (Avrupa Komisyonu, 2010a).

2.3.2. Alman Parlamentosuna Yapılan Siber Saldırılar

7 Ocak 2015 tarihinde Rus hacker grubu CyberBerkut tarafından Alman Parlamentosu Bundestag ve Şansölye Angela Merkel'in web sayfalarına yönelik gerçekleştirilen siber saldırılar saat 10.00'da başlayıp akşam saatlerine kadar kullanımdaki sayfalara erişimin engellenmesine sebep olmuştur. (BBC, 2015a) Devamında ise siber saldırıların sadece bununla sınırlı olmadığı ve zararlı yazılımlar

aracılığı ile Alman Parlamentosuna yönelik olarak gerçekleştirilen saldırılar sonucu Parlakom ağı üzerinde bulunan ve sayısı yaklaşık 20.000'i bulan politikacılara, destek personellerine ve memurlara ait bilgisayarlara erişim ve bu bilgisayarlardan veri akışı sağlanmıştır. Kötücül yazılımlar aracılığı ile gerçekleştirildiği belirtilen saldırıların 2015'in Haziran ayında yapılan raporlamasında virüs bulaşan bilgisayarlardan veri akışının devam ettiği bilgisi verilmiştir. (BBC, 2015b)

Alman Parlamentosuna yönelik gerçekleştirilen siber saldırıların kaynağı kesin olarak bilinememekle birlikte Rus İstihbarat Servisinin sorumlu olduğu öne sürülmektedir. Ukrayna başbakanı Arseny Yatsenyuk, Merkel ile yaptığı görüşmede Rus istihbarat servisinin sorumlu olduğunu dile getirmiştir. (BBC, 2015a) Almanya'nın iç istihbarat kurumu, Alman devlet bilgisayar sistemleri üzerindeki siber saldırıların Arkasında Rusya'nın olduğunu belirtmiştir. Federal Anayasayı Koruma Dairesi (BfV) Alman Parlamentosuna yönelik gerçekleştirilen siber saldırılardan sorumlu kişilerin Rus kökenli olduğunu belirtmiştir. Rusya bu suçlamalara bir cevap vermemiştir. (BBC, 2016)

BfV başkanı Hans-Georg Maassen Alman devlet kurum ve kuruluşlarına yönelik siber saldırıların Rus kökenli siber casus grubu olan APT28, Pawn Storm, Fancy Bear ve Sednit gibi isimlerle anılan Sofacy tarafından istihbarat verileri toplamak için yapıldığını öne sürmüştür. (BBC, 2016) Bu saldırıların diğer siber saldırılar gibi kritik altyapı ile ilgili veri toplama dâhil olmak üzere santraller ve diğer hizmetleri hedef aldığını vurgulamıştır. Ayrıca Maassen, "Siber uzay bir melez savaş yeridir. Bu alanda casusluk ve sabotaj için yeni işletim alanları açılır." ifadeleri ile siber güvenliğin sağlanmasının önemine dikkat çekmiştir. (BBC, 2016) 2004 yılında Avrupa Parlamentosu'na seçilen, AP'de Yeşiller Grubu/Hür Avrupa İttifakı üyesi olan ve halen parlamentonun Dış İlişkiler Komisyonu üyeliğini yürüten Cem Özdemir, Alman Parlamentosuna yönelik gerçekleştirilen saldırılar için "Rusya'nın AB'yi istikrarsızlaştırmak için açık bir çıkarı var." demiştir (Bölinger, 2016). Özdemir'in bu sözleri ile Avrupa Birliği için açık bir söz edimi kullanımının olduğunu görebiliriz. Burada başvuru nesnesi AB'dir. Tehdit ise Rusya olarak işaret edilmektedir.

2.3.3. TV5 Monde Örneği

7 Ocak 2015'te Paris'te Fransız mizah dergisi Charlie Hebdo'nun merkez binasına gerçekleştirilen silahlı saldırı sonucu 12 kişi yaşamını yitirmiştir. Radikal İslamcı kişiler

tarafından gerçekleştirildiği öne sürülen saldırı sonrası, Avrupa ülkelerinde Anti-İslamcı yaklaşımlar sergilenmiştir (BBC, 2015c; AlJazeera, 2015). Bunun üzerine kendini radikal İslamcı bir grup olarak tanıtan CyberCaliphate TV5 Monde'ye yönelik siber saldırılar gerçekleştirmiştir.

8 Nisan 2015'te Fransız televizyon kanalı TV5 Monde kanalının tüm kanallarına ve web sayfalarına yapılan siber saldırı sonucu, kanal hizmet veremeyecek duruma gelmiştir. Bilgisayar korsanları, TV5 Monde kanallarının kontrollerini ele almalarının yanı sıra, televizyon kanalının web sayfalarını ve sosyal medya hesaplarını da ele geçirmişlerdir. Kanala düzenlenen siber saldırı sivil ve askeri sektörlerin yanı sıra Batı dünyasında medya sektörünü de içine alarak güvenlik zafiyetlerini gün yüzüne çıkarmıştır. Fransız güvenlik ajanslarınca, 7 Ocak 2015'te Paris'te gerçekleşen Charlie Hebdo saldırısından sonra Fransa'da yaklaşık 1500 yerel yönetim kuruluşunun ve küçük işletmenin siber saldırıya uğradığı rapor edilmiştir. (Maurice, 2015)

Siber saldırılar, TV5 Monde örneğinde olduğu gibi fiili olaylara tepki olarak karşımıza çıkabilmektedir. Devlet-dışı aktörlerin de iyi organize olarak konvansiyonel ve dijital saldırılar gerçekleştirebilmesi AB'yi sınırlı yetkileriyle yüzleştirmiştir. Ayrıca bu konuda Hollanda Dışişleri bakanı Bert Gerard Koenders ve AB Dış İlişkiler ve Güvenlik Politikasından sorumlu Yüksek Temsilci Federica Mogherini'nin birlikte kaleme aldıkları yazıda TV5 Monde'ye gerçekleştirilen saldırılar ve önceki yıllarda medyaya yönelik gerçekleşen siber saldırılara vurgu yapılmıştır. Bu saldırıları referans göstererek "Siber saldırılar, devletlere ve devlet dışı aktörlere siyasi bir baskı için araç olarak kullanılmaktadır." şeklinde demeç vermişlerdir. (Koenders ve Mogherini, 2015). AB'nin siber olayları güvenlikleştirmesinde Koenders ve Mogherini'nin bu demeci, çalışmanın teorik çerçevesini oluşturan güvenlikleştirme sürecinin bir unsuru olan söz ediminin açık bir örneği olarak karşımıza çıkmaktadır. Burada başvuru nesnesi devletler ve devlet dışı aktörler iken, tehdit olarak siber saldırılar gösterilmiştir. Alımlayıcı kitleye kabul ettirilecek tehdit günlük yaşamda karşılaşılan bir örnek üzerinden verilmiştir.

2.4. Sonuç

AB'nin siber güvenlik politikasının ve strateji belgesinin oluşmasında önemli yere sahip olan gündelik yaşamda karşılaşılan örnekler, güvenlikleştirme söyleminin oluşmasında da büyük öneme sahiptir. AB'nin strateji belgesi, güvenlikleştirme sürecinin

temel taşı olarak karşımıza çıkmaktadır. Bu belgenin oluşturulmasında AB yetkililerinin söylemleri, dünya genelinde yaşanan siber olaylar ve AB'yi doğrudan etkileyen siber saldırılar önemli yer tutmaktadır. Estonya saldırıları, Alman Parlamentosuna yapılan siber saldırılar ve TV5 Monde örneği her zaman AB için önemli referans kaynakları olmuştur. Alımlayıcı kitle olarak AB vatandaşlarına yönelik AB yetkilileri tarafından verilen demeçlerde güvenlikleştirme sürecindeki tehdidin tanımlanması ve alımlayıcı kitleye kabul ettirilmesi aşamasında günlük yaşamdaki örneklere vurgu yapıldığını söylemek yerinde olacaktır.

AB'nin siber güvenlik strateji belgesi ve politikaları AB'nin en önemli dokümanı olarak karşımıza çıkmaktadır ve önümüzdeki bölümde irdelenecektir. Nitekim siber olayların tehdit olarak tanımlayıp, bu konuda alınması gereken önlemleri sıralaması bakımından bu strateji belgesi güvenlikleştirmenin en önemli ayağını oluşturmaktadır. Bundan sonraki bölümde güvenlikleştirme sürecinin temel taşı olan strateji belgesi ve AB'nin politikaları detaylı bir şekilde incelenerek çalışma neticelendirilmektedir.

3. BÖLÜM

AB'NİN SİBER GÜVENLİK STRATEJİSİ VE POLİTİKALARI

Bu bölümde, AB'nin siber güvenlik politikasını oluşturan temel doküman olan "Cybersecurity Strategy for the European Union"[30] (Avrupa Komisyonu, 2013b) (Avrupa Birliği için Siber Güvenlik Stratejisi) belgesi detaylı olarak incelenmiştir. Üye devletlerin siber güvenlik politikalarından yola çıkarak ortak bir siber güvenlik politikasının nasıl oluşturulduğu, politikaların ve kurumların bu bağlamda nasıl işlediği ve nasıl işleyeceğinin öngörüldüğü ile ilgili değerlendirmeler yapılmıştır. Bu tezin ikinci bölümünde incelenen siber saldırı yöntemlerinden yola çıkılarak; gerek dünya genelindeki örneklerden ders almak, gerekse AB'yi doğrudan etkileyen örneklerle tekrar karşılaşmamak için siber güvenliğin sağlanması konusunda AB tarafından oluşturulan politikalar bu bölümün ana konusunu oluşturmaktadır.

Bu bölümde ilk olarak AB'nin ortak siber güvenlik politikası için oluşturduğu strateji belgesi öncesinde siber güvenliğin sağlanması için gerçekleştirilen eylemler değerlendirilmiştir. Devamında ise strateji belgesi üzerinden bağlam açıklanıp, strateji belgesinin detayları incelenmektedir. AB'nin siber güvenlik stratejisinde öncelikli olarak üye devletlerin ulusal siber güvenlik politikalarını oluşturmaları teşvik edilmiştir. AB'nin müşterek siber güvenlik politikasının oluşturulmasını da bu temel üzerinde kurduğunu söylemek mümkündür.

3.1. Strateji Belgesi Öncesinde AB'deki Gelişmeler

AB'nin ortak siber güvenlik politikası için oluşturduğu strateji belgesi öncesinde siber güvenliğin sağlanması için gerçekleştirilen eylemlerin ve politikaların bilinmesi faydalı olacaktır. AB'nin kritik altyapı ve siber güvenlik bağlantı vurgusu açıklanıp, AB'deki kurumsallaşmanın en temel ayağını oluşturan ENISA değerlendirilmiştir. Sonrasında AB'de siber güvenlik ile ilgili önemli yasal düzenlemelere ve AB'de ağ ve bilgi güvenliği siyasetinin oluşmasına yer verilmiştir. Bu bölümde strateji belgesine giden süreçte AB'de gerçekleşen gelişmeler kronolojik olarak ve dört başlık altında

[30] Bu stratejinin orijinal dilindeki tam metni Ek'te sunulmuştur.

gruplandırılarak verilmiştir. Devamında ise strateji belgesi üzerinden bağlam açıklanıp, strateji belgesinin detayları incelenmektedir.

3.1.1. AB'nin Kritik Altyapı ve Siber Güvenlik Bağlantısı Vurgusu

AB, siber güvenliğin sağlanması hususunda uluslararası ortamda önemli bir aktör olarak karşımıza çıkmaktadır. AB'de siber güvenliğin sağlanması ve kritik bilgi altyapısının korunması önemli konular olarak değerlendirilmekte ve bu doğrultuda politikalar geliştirilmektedir.

Kritik altyapı, zarar görmesi veya tahrip olması durumunda kendisine bağlı sistemlerin veya yapıların da önemli düzeyde zarar görmesine ve kesintiye uğramasına neden olan yapıları ifade etmektedir (Westby, 2005). Kritik altyapılar gelecek zararların yaygın etki yaptığı, buna yönelik saldırıların toplumları korkutarak, devlet yapılarını acizleştirdiği yapılardır. "Kritik altyapılar devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasından bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir. Kritik altyapıların korunması, gelişmiş ülkelerin önemli gündem maddelerinden birisi olarak karşımıza çıkmaktadır." (Karabacak, 2011) Örneğin, deprem, sel ve fırtına gibi olağandışı durumlar bir şehirde ulaşım, taşımacılık gibi hizmetlerin aksamasına sebep olmaktadır. Ancak bir nehirdeki köprülerin yıkılması, telekom altyapısının devre dışı bırakılması gibi olaylar insanların şehri tahliye etmesi ve acil yardım hizmetlerinin aksaması sonucunu doğurmaktadır.

Kritik bilgi altyapısı, kesilmesi veya tahrip olması durumunda vatandaşların sağlığı, güvenliği ve ekonomik refahı veya hükümetin ve ekonominin işleyişi üzerinde önemli etki doğuracak bir biriyle bağlantılı bilgi sistemleri ve ağları olarak tanımlanabilir. (OECD, 2008: 1-3) Kritik bilgi altyapısı ülkelerin siber saldırılara karşı korunmasında, yapılan siber saldırılara karşı anında önlem alınması hususunda büyük öneme sahiptir.

AB tarafından kritik olarak kabul edilen sektörler 10 Ekim 2001 tarihli 574/2001 sayılı bildirisinde belirtilmiştir. Avrupa Komisyonu kritik altyapıların belirlenmesinde kapsamın, büyüklüğün ve zaman etkisinin önemine vurgu yapmıştır. (Avrupa

Komisyonu, 2001a) Buna göre, *kapsam*, kritik bir altyapının kaybı durumunda etkilenilecek olan coğrafi büyüklüğü ifade etmektedir. Yani, kritik altyapının zarar görmesi durumunda ya da kaybı söz konusu olduğunda etkilenen coğrafi alanın yerel mi, ulusal mı, uluslararası mı olduğu ile ilgilidir. (Avrupa Komisyonu, 2001a) *Büyüklük* ise kaybın ya da zarar durumunun hiç, minimum, orta veya büyük olarak derecelendirilmesini ifade etmektedir. Bir olayın büyüklüğünün değerlendirilmesinde siyasi, ekonomik ve çevresel faktörlerin de etkili olacağı belirtilmektedir. Siyasi faktörler olarak kritik altyapılara yapılan saldırılar sonrasında hükümetlere olan güven üzerindeki etkisinden bahsedilebilir. Ekonomik faktörler olarak ise gayrisafi milli hasılaya olan etki ve ekonomik kayıpların oluşup oluşmaması örnek olarak verilebilir. Çevresel faktörlere ise etkilenen kişi sayısı, hayat kaybının olup olmaması gibi kamu etkisi ve çevre etkisi örnek olarak verilebilir. Ayrıca diğer kritik altyapılar ile ilgili olan bağlantısı da önemli bir değerlendirme kriteri olarak karşımıza çıkmaktadır. (Avrupa Komisyonu, 2001a) *Zaman etkisi* ise olası bir kritik altyapı saldırısından etkilenildiği durumda bunun ne kadarlık bir zaman diliminde kayıplara yol açacağını ifade etmektedir. Hemen, 24 saat içerisinde, bir hafta içerisinde gibi zaman dilimleri belirlenmesi örnek olarak verilebilir. (Avrupa Komisyonu, 2001a)

20 Ekim 2004 tarihinde terörle mücadelede kritik altyapıların korunması Avrupa Toplulukları İletişim Komisyonu tarafından kritik altyapı yeniden tanımlanmıştır. Ayrıca bu çalıştay kapsamında kritik sektörler tekrar değerlendirilmiş ve bunların kriterlerinin neler olabileceği tartışılmıştır. Bu komisyondan çıkan tanıma göre kritik altyapılar "zarara verilmesi ya da yok edilmesi durumunda vatandaşların sağlığı, güvenliği, huzuru ve ekonomik refahı üzerinde veya üye ülkelerin hükümetlerinin işleyişi üzerinde önemli etkilere yol açma ihtimali yüksek olan fiziksel ve bilgi teknolojileri ağları, hizmetleri, olanakları ve varlıkları" olarak ifade edilmiştir. (Avrupa Komisyonu, 2004) Bu tanımdan yola çıkarak AB'nin kritik altyapılara olan yaklaşımının ve kritik sektörlerin ekonominin birçok sektöründen temel devlet hizmetlerine kadar uzanan geniş bir yelpazeden oluştuğunu söylemek mümkündür. Güvenlikleştirme kapsamında değerlendirildiğinde de bu tanımın kapsayıcı olduğu ve pek çok güvenlik sektörü altında değerlendirilebileceğini söylenebilir. Nitekim güvenlikleştirmenin etkisi ve güç başvuru nesnesinin önem derecesine göre şekillenmektedir. Burada başvuru nesnesi olarak doğrudan vatandaşın ve devletin bekasının olması, güvenlikleştirme sürecinde kritik altyapı güvenliğine kayda değer bir önem atfedilmesine sebep olmaktadır. Güvenlikleştirme de pekiştirilmektedir.

24 Kasım 2005 tarihinde Avrupa Komisyonu tarafından yayınlanan Avrupa Kritik Altyapılarının Korunması Programı (EPCIP) hakkındaki Yeşil Kitapta (Avrupa Komisyonu, 2005) kritik altyapıların korunması amacıyla alınacak önlemler, hazırlıklar ve sorumluluklar genel olarak belirlenmiştir. Yerellik, tamamlayıcılık, gizlilik, paydaş iş birliği ve ölçülülük EPCIP'in temel değerleri olarak verilmiştir. Yerellik ile kritik bilgi altyapı güvenliğinin kurulmasında yerel düzeyde önlemlerin alınması gerektiği vurgulanmıştır. Tamamlayıcılık ilkesi yerel düzeyde ve AB düzeyindeki politikaların tamamlayıcılığına dikkat çekilmiştir. Gizlilik kritik bilgi altyapı güvenliği ile ilgili AB ve devletler arasında yapılacak olan bilgi paylaşımının güvenli bir şekilde yapılması gerekliliğini ifade etmektedir. Paydaş işbirliği ile Komisyon, sanayi/iş dernekleri, standardizasyon organları ve sahipleri, operatörler ve kullanıcılar (iş ve hizmet sağlama amaçlı kritik bilgi altyapısını kullanan organizasyonlar olarak tanımlanmaktadır) arasındaki iş birliğine dikkat çekilmiştir. Ayrıca EPCIP uygulanmasına katkıda bulunması gerekliliği belirtilmiştir. Ölçülülük ilkesi ise alınacak önlemler ile risk düzeyi ile orantılı olacağını ifade etmektedir. Uygun risk yönetimi tekniklerini uygulayarak, bağıl kritiklik, fayda-maliyet oranı, koruyucu güvenlik seviyesi ve mevcut azaltma stratejilerinin etkinliği dikkate alınarak, en fazla risk alanları üzerinde durulmasının sağlanacağı ifade edilmiştir. Ulusal ve uluslararası düzeydeki sorumluluklar da bu kapsamda değerlendirilmiştir. Yeşil Kitapta ayrıca Kritik Altyapı Uyarı Bilgi Ağı (CIWIN)[31] hakkında da bilgi verilmiştir.

3.1.2. Siber Güvenlik Politikasında Kurumsallaşma: ENISA

Yukarıdaki gelişmelere paralel olarak yürütülen kurumsallaşma çalışmaları sonucunda 5 Haziran 2003 tarihinde Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nın (European Union Agency for Network and Information Security ENISA) bir tüzel kişilik olarak kurulması kararının alınmasını takiben 14 Mart 2004 tarihinde fiilen kuruluşunu tamamlamıştır. ENISA, AB'nin siber güvenliğinin sağlanması konusunda koordinasyonu sağlamak ve Avrupa genelinde üst düzeyde ağ ve bilgi güvenliğinin sağlanmasını amaçlamaktadır. (ENISA, 2016a)

[31] Kritik Altyapı Uyarı Bilgi Ağı (CIWIN) Avrupa komisyonu tarafından kritik altyapılara ve güvenlik açıklarına ilişkin verilerin üye devletler ile kolay akışının sağlanması için oluşturulmuştur. Üye devletlere, AB kurumlarına, kritik altyapı sahiplerine ve işletmecilere ait ortak tehditler, güvenlik açıkları, güvenlik ihlallerine karşı alınmadı gereken tedbirler ve izlenecek stratejiler hakkında destek vermek suretiyle risklerin azaltılmasını ve yardımı amaçlamaktadır. (Avrupa Komisyonu, 2016c)

ENISA kurulduğu tarihten günümüze dek sürekli gelişme göstermiştir ve kurulduğunda bir bilgi akışı merkezi olmasına rağmen günümüzde birçok alanda etkin bir şekilde faaliyetlerini sürdürmektedir. Kritik bilgi altyapı güvenliği konusunda sertifikasyon hizmetleri de sunmaktadır. Siber güvenlik uzmanları için eğitimler düzenlemekte, üye devletlere ağ ve bilgi güvenliğinin sağlanması konusunda danışma merkezi işlevini yürütmektedir. Ayrıca yayınları ile de rehber niteliğinde uygulamalara öncülük etmektedir. (ENISA, 2016b) AB'nin siber güvenliğinin sağlanması konusunda aktif rol alan bir kurum olarak ENISA'nın varlığı siber güvenliğin güvenlikleştirme sürecinde söylemlerin kurumsallaştırılması ile daha somut hale getirilmesine örnek olarak verilebilir. ENISA, üye devletleri, özellikle, ulaşım ve enerji altyapısı gibi endüstriyel kontrol sistemleri konusunda ulusal siber direnç kapasiteleri geliştirmeye teşvik etmek amacıyla 2013 yılında AB için Endüstriyel Kontrol Sistemleri - Bilgisayar Güvenliği Olaylarına Müdahale Ekibi (ICS-CSIRTs)[32] ni oluşturmuştur. Üye devletleri ve AB kurumlarını Pan Avrupalı siber olaylara karşı desteklemeye devam ederek siber güvenliğin sağlanmasında aktif rol almıştır. Bu kapsamda, ENISA kamu özel ortaklığı geliştirip, uzmanlara fikir üretme toplantıları (fikir üretme) düzenlemektedir.[33]

Avrupa Birliği, strateji belgesi öncesinde çıkarmış olduğu yasal düzenlemeler ile de konuya verdiği öneme dikkat çekmiştir. Nitekim bu bağlamda önemli dönüm noktaları olarak aşağıdaki düzenlemeleri örnek olarak verebiliriz:

i) 23 Kasım 1995 tarihli Verilerin Korunması Direktifi (Avrupa Birliği, 1995)
ii) 31 Temmuz 2002 tarihli Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi (Avrupa Birliği, 2002)
iii) 24 Şubat 2005 tarihli Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı (Avrupa Birliği, 2005)
iv) 15 Mart 2006 tarihli Verilerin Saklanması Direktifi (Avrupa Birliği, 2006)

[32] Computer Security Incident Response Team(s) for Industrial Control Systems (Endüstriyel Kontrol Sistemleri - Bilgisayar Güvenliği Olaylarına Müdahale Ekibi)
[33] Ekim 2012'de, ENISA, bazı üye devletler ile pilot olarak "Avrupa Siber Güvenlik Ayı" organize etmiştir. (ENISA, 2015b) Siber güvenlik ve Siber suçlarla ilgili AB-ABD Çalışma Grubu da farkındalığı sağlamak ve bilinci artırmak için Güvenli İnternet Programı (çevrimiçi çocukların güvenliğine odaklanmış) oluşturmuştur (Avrupa Komisyonu, 2012). Kasım 2010'da AB-ABD Zirvesi'nde kurulan bu Çalışma Grubu, siber güvenlik ve siber suç konularında geniş bir yelpazede işbirliği içinde yaklaşımlar geliştirilmesi ile görevlendirilmiştir (Avrupa Komisyonu, 2010c).

3.1.3. AB'de Siber Güvenlik İle İlgili Önemli Yasal Düzenlemeler

23 Kasım 1995 tarihli Verilerin Korunması Direktifi ile kişisel verilerin işlenmesi sırasında kişi hak ve özgürlüklerinin korunması ve mahremiyetin sağlanması amaçlanmıştır. Ayrıca işlenen kişisel verilerin AB üyesi ülkelerin ulusal sınırları içerisinde güvenli ve serbest bir şekilde dolaşımının sağlanması için gerekli çerçeve kuralları belirlenmiştir. Sadece gerçek kişilere ilişkin verilerin işlenmesine yönelik uygulamaların yer aldığı direktifte tüzel kişilere ilişkin esaslar üye devletlerin inisiyatifinde bırakılmıştır. (Avrupa Birliği, 1995)

Direktifte verilerin işlenmesi ile ilgili olan kişisel veri, anonim veri, kişisel verilerin işlenmesi, veri koruma görevlisi gibi kavramların tanımlaması yapılmıştır. İşlenen verilere ilişkin olarak da verilerin kaliteli olması, hukuka uygun olarak işlenmesi, ilgili kişinin açık rıza beyanı ile gerçekleştirilmesi ilkelerine yer verilmiştir. Ayrıca veri işleyen kişinin bilgi verme sorumluluğu, ilgili kişinin işlenen verileri isteme hakkı ve haklı sebepler olması durumunda veri işlenmesi işlemine itiraz etme hakkı gibi ilkeler de ayrıca düzenlenmiştir. Direktifin 25. ve 26. maddelerinde ise işlenen verilerin AB üyesi olmayan devletlerle paylaşımının nasıl olacağı hakkında detaylı düzenlemeler yapılmıştır. Bu kapsamda Komisyon tarafından veri transfer edilecek ülke içinde gerekli veri güvenliğinin sağlandığına kanaat beyan edilirse bilgi paylaşımının gerçekleştirilebileceği ve AB üyesi ülkeler ile eşit sayılacağı, ancak bu koşulları sağlamıyorsa veri paylaşımının olmayacağı belirtilmiştir. (Avrupa Birliği, 1995)

31 Temmuz 2002 tarihli Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi ise 1995'teki direktifi tamamlayıcı niteliktedir. 1995 tarihli direktifte sadece gerçek kişilerin verilerine ilişkin düzenlemeler yer alırken bu direktifte tüzel kişiler de kapsama alınmıştır. Direktifle birlikte elektronik haberleşme alanında temel hak ve özgürlüklere saygı gösterilmesi, özel yaşamın gizliliği ve kişisel verilerin korunmasının sağlanması amaçlanmıştır. Teknolojik gelişmeler karşısında kişisel verilerin korunmasına ilişkin düzenlemeler de direktifte yer bulmuştur. Ayrıca ticari elektronik iletilere ve istenmeyen e-postalara yönelik düzenlemeler de direktifte değerlendirilmiştir. Kişilere önceden rızası alınmaksızın istenmeyen e-posta gönderilmesi yasaklanmıştır. Doğrudan reklam içerikli elektronik iletilerde reklam göndericisinin isminin saklanmaması ve geçerli bir adresinin bulunması zorunluluğu da bu direktifle düzenlenmiştir. Bu direktifte

olmayan ancak 1995 yılındaki direktifte bulunan konular için mevcut düzenlemenin geçerli olduğu vurgulanmıştır. (Avrupa Birliği, 2002)

24 Şubat 2005 tarihli Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı ile AB çapında bilgi sistemlerine yönelik gerçekleştirilen siber saldırılara ilişkin ceza yargılamasının güçlendirilmesi amacıyla üye devletlerle iş birliği hedeflenmiştir. Çerçeve kararın 11. Maddesi gereğince üye devletlerin iş birliğini sağlayabilmesi için 7 gün 24 saat çalışan operasyonel iletişim noktaları belirlemek zorunda olduğu belirtilmiştir. Çerçeve karar kapsamında bilgi sistemlerine yetkisiz erişimler ve sistemlerin engellenmesi cezalandırılabilecek bilişim suçları olarak değerlendirilmiştir. Ayrıca üye devletler bunlar için caydırıcı, etkili ve orantılı bir şekilde para cezası içeren yasal düzenlemeler oluşturmak ile yükümlü kılınmışlardır. (Avrupa Birliği, 2005)

15 Mart 2006 tarihli Verilerin Saklanması Direktifi ile de 2002 tarihli direktifte değişiklikler yapılmıştır. Üye ülkelerin kendi yasal mevzuatlarında tanımlanmış olan telefon ve e-posta verilerinin, suçların soruşturulması, tespiti ve kovuşturulması amacıyla saklanması konularında üye ülkelerin yasal mevzuatlarının uyumunu sağlamayı amaçlamıştır. Direktif gerek gerçek kişilerin gerekse tüzel kişilerin abone veya kayıtlı kullanıcıyı tanımlamak için gerekli yer ve trafik verileri hakkında uygulanmaktadır. Bu direktif ile birlikte üye devletlere internet servis sağlayıcılarının iletişim bilgilerinin iletişim tarihinden itibaren 6 aydan az 2 yıldan fazla olmamak üzere saklama yükümlülüğü de getirilmiştir. (Avrupa Birliği, 2006)

Güvenlikleştirme sürecinin temel taşı olarak değerlendirebileceğimiz strateji belgesinin oluşturulmasına giden süreçte yukarıda verilen yasal düzenlemelerin büyük önemi olmuştur. Bir önceki belgenin açıkta kalan yerlerinin tamamlanarak ilerlediği görülmektedir. Bu süreçte güvenlikleştirme sürecinin önemli safhalarından olan alımlayıcı kitleye tehdidin tanımlanması ve kabul ettirilmesi bu süreçte gerçekleşiştir. Tehdit, çıkartılan yasal düzenlemeler ile pekiştirilmiş ve alımlayıcı kitleye kabul ettirilebilir hale gelmiş ve önlem alınması gereken bir durum olarak kabul ettirilmiştir.

3.1.4. AB'de Ağ ve Bilgi Güvenliği Siyasetinin Oluşması

Avrupa'nın gelişmiş bir kaynak ve önleme kapasitesine sahip olmadığı sürece siber güvenlik olaylarına karşı korunmasız kalacağı ifade edilmektedir. (Avrupa

Komisyonu, 2013b: 5). Bu ifadeyi Kopenhag Ekolünün güvenlikleştirme yaklaşımı üzerinden okursak, strateji belgesinin burada tehdidin yaşamsallığı ve ona karşı yeterli önlemlerin geliştirilmemesi durumunda geç olacağı (korunmasız kalınacağı) söylemini kullandığı, böylelikle meseleye hem aciliyet hem de öncelik atfettiği söylenebilir. Bu yüzden Komisyon Ağ ve Bilgi Güvenliği (NIS[34]) siyasetini geliştirmiştir. Bunu sağlamak için de 2004 yılında Avrupa Birliği Ağ ve Bilgi Güvenliği Kurumu (ENISA) kurulmuştur ve Avrupa Parlamentosu ve Avrupa Konseyi tarafından güncellenerek şimdiki halini almıştır. Buna ek olarak, elektronik iletişim araçları ile ilgili çerçeve yönergeler ağlarla ilgili riskleri yönetmeyi sağlamaktadır. Ayrıca AB veri koruma kanunu ile verilerin kontrolü sağlanmaktadır. (Avrupa Komisyonu, 2010b) AB bünyesinde gerçekleştirilen bu ilerlemelerin yeterli olmadığı ve ulus devletlerin politikalarını da kapsayacak yasal düzenlemelerin gerekliliği duyulmuştur. Bu bağlamda AB tarafından aşağıdaki düzenlemeler yapılmıştır. Ulusal otoriteleri de kapsayacak şekilde ortak paydada buluşulmuş bir NIS politikası için 2012'de AB'nin kurumlarıyla uyumlu çalışan merkezi Brüksel'de olan CERT (Bilgisayar Acil Müdahale Ekibi) kurulmuştur. AB kurumlarındaki problemlerle ilgilenen kısmı ise CERT-EU olarak belirtilmiştir. Bu ekibin temel görevi AB ve üye devletlerde çıkabilecek olan olası kriz durumlarında acil müdahale edip, gerekli önlemleri alarak etkili bir NIS politikasını yürütmektir. (CERT, 2015)

AB, NIS politikası kapsamında üye devletlerinin yetkili makamları arasında bilgi paylaşımını ve karşılıklı yardımı sağlayarak, koordineli önleme, tespit etme, azaltma ve müdahale mekanizmaları kurmak istemektedir. "Üye Devletler için Avrupa Forumu (EFMS)" kapsamında kaydedilen ilerleme üzerine NIS kamu politikası üzerinde verilen tartışmalar ve değişimler gerçekleştirilmiştir (Avrupa Komisyonu, 2013b: 5). Katılımcıları üye devletlerin kamu otoriteleri olan bu forum kapsamında etkili bir NIS

[34] İngilizce karşılığı NIS (Network and Information Security/Ağ ve Bilgi Güvenliği) olan kavram, bütün AB metinlerinde NIS olarak geçtiği için kavram kargaşası oluşturmaması için bu çalışmada da İngilizce karşılığı olan NIS ile kullanılmıştır. NIS ilk defa 2001 yılında AB Komisyonunun "Network and Information Security: Proposal for A European Policy Approach" (Avrupa Komisyonu, 2001b) belgesi ile gündeme gelmiştir. 2006 yılında "Strategy for a Secure Information Society" (Avrupa Komisyonu, 2006), 2009 yılında "Action Plan and a Communication on Critical Information Infrastructure Protection (CIIP)" (Avrupa Komisyonu, 2009b) ve 2011 yılında "Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'" (Avrupa Komisyonu, 2011a) belgelerinde de yer bulmuştur.

politikası için sorunların detaylı olarak tartışılması mümkün olmaktadır ve politika yapım sürecinde farklı bakış açılarına da yer verilebilmektedir (Avrupa Komisyonu, 2009c).

Yukarıda verilenlere ek olarak AB, üye devletler ile işbirliğini geliştirmeyi amaçlamaktadır. Üye devletlerin katıldığı ilk platform Siber Avrupa (Cyber Europe)'dır (ENISA, 2010). 2010 yılında gerçekleşen ilk adımdan sonra 2012'de gerçekleşen ikinci adımda ise özel sektörler de yerini almıştır (Trimintzios, Gavrila ve Klejnstrup, 2012). 2014 yılında gerçekleşen son Siber Avrupa buluşmalarında katılımcı sayısı daha da genişletilerek sivil toplum kuruluşları, üye devlet temsilcileri, AB temsilcileri olmak üzere geniş yelpazede görüşmeler gerçekleşmiştir (Gavrila, Ogée, Trimintzios ve Zacharis, 2014). 2011 yılında ayrıca AB ve ABD Siber Atlantik 2011 de bir araya gelmiştir ve gelecek yıllar için de birçok uluslararası aktörün yer alacağı uygulamalar düşünülmektedir (ENISA, 2015a). Bundan sonraki bölümde strateji belgesi detaylı olarak incelenecektir. Strateji belgesi öncesi AB'deki gelişmelere gerek duyuldukça sonraki bölümde de satır aralarında yer verilmiştir.

3.2. Avrupa Birliği için Siber Güvenlik Stratejisi

Bu bölümde, AB siber güvenlik stratejisi incelenmektedir. Bu çalışmada, üye devletlerin politikalarına tek tek değinilmemiştir ama bu politikaların bir kısmının AB'nin strateji belgesini (bundan sonra kısaca "strateji belgesi") yayınlamasından sonra AB desteğiyle oluşturulduğu söylenebilir. [35]

Bölümün içeriği ve alt başlıkların sıralaması analitik bir çerçeve ve anlamlı bir perspektif sunabilmek için AB'nin siber güvenlik strateji belgesine göre yapılmıştır.[36]

[35] ENISA (European Union Agency for Network and Information Security/ Avrupa Ağ ve Bilgi Güvenliği Ajansı) tarafından yapılan çalışmaya göre üye devletlerin ulusal siber güvenlik politikalarının oluşturulma yılları şu şekildedir: Avusturya (Avusturya Cumhuriyeti Federal Başbakanlık, 2013), Belçika (CMR, 2012), Hırvatistan (Milanović, 2015),Çek Cumhuriyeti (Çek Cumhuriyeti Milli Güvenlik Kurumu, 20115), Güney Kıbrıs (Kıbrıs Elektronik Haberleşme ve Posta Yönetmeliği Komiserliği ,2012), Danimarka (2015) (Danimarka Siber Güvenlik Merkezi, 2015), Estonya (Ekonomik İşler ve İletişim Bakanlığı, 2014), Finlandiya (Güvenlik ve Savunma Komitesi Sekreterliği, 2013), Fransa (Başbakanlık, 2015), İrlanda (Cumarsaide, 2015), İtalya (İtalya Bakanlar Kurulu, 2013), Almanya (Federal İçişleri Bakanlığı, 2011), Macaristan (Ulusal Siber Güvenlik Koordinasyon Kurulu, 2013), Litvanya (Litvanya Cumhuriyeti Devlet Güvenlik Bakanlığı, 2011), Lüksemburg (Lüksemburg Hükümet Büyük Dükalığı, 2011), Hollanda (Güvenlik ve Terörle Mücadele için Ulusal Koordinatörlüğü, 2011), Polonya (İdare ve Dijitalleştirilme Bakanlığı, 2013), Romanya (Romanya Hükümeti, 2013), Slovak Cumhuriyeti (Slovak Cumhuriyeti Hükümeti, 2008), İspanya (Başbakanlık, 2013), İngiltere (İskoçya- (İskoçya Hükümeti, 2015)) (Kabine Ofisi, 2011). Bunlara ek olarak, Yunanistan, İsveç ve Slovenya'nın ulusal siber güvenlik politikaları için dokümanlarının hazırlanma aşamasında olduğu belirtilmiştir. (ENISA, 2016c)

[36] Bu bölümdeki alt başlıklar kapsamlı ve analitik bir çerçeve sunabilmesi açısından AB'nin siber güvenlik strateji belgesindeki başlıklarla aynı olacak şekilde düzenlenmiştir. AB'nin geliştirdiği

İnceleme kapsamında strateji belgesinde belirtilen hususlar kapsamlı bir şekilde verilmiştir. Ek olarak, Birliğin diğer dokümanlarında ilgili kısımlara yapılabilecek referanslar ve kişisel yorumlar ile çalışma zenginleştirilmiştir. Strateji belgesi ve ilgili AB politikaları, güvenlikleştirme kapsamında irdelenerek okuyucuya sunulmuştur.

3.2.1. Bağlam

Strateji belgesinde bağlam olarak öncelikle son yıllarda, internetin ve daha geniş tanımlarsak siber uzayın toplumun tüm kesimlerinde muazzam bir etkiye sahip olduğu; günlük yaşamımızın, temel haklarımızın, sosyal etkileşimlerimizin ve ekonomik bağımlılığımızın bilgi ve iletişim teknolojilerine bağlılığı vurgulanmıştır. Açık ve özgür bir sanal âlemin, dünya çapında bir siyasi ve sosyal kaynaşmayı teşvik ederek; ülkeler, topluluklar ve vatandaşlar arasındaki engelleri küresel çapta bir bilgi paylaşımı ve etkileşime izin vererek çığır açtığına dikkat çekilmiştir. Bunun aynı zamanda düşünce ve ifade özgürlüğü alanlarını genişlettiği, özellikle Arap Baharı boyunca daha adil ve demokratik toplumların ortaya çıkmasına zemin hazırladığı belirtilmiştir. (Avrupa Komisyonu, 2013b: 2) Bunun yanında, dijital dünyanın, sağladığı inanılmaz faydalar ile birlikte aynı zamanda savunmasız bir alan olduğu vurgusu yapılmıştır. Bununla birlikte siber güvenlik olaylarının bağımlı olduğumuz su, bakım, elektrik ve mobil servisler gibi kritik altyapı hizmetlerini tehdit ettiğine ve tehditlerin; suç içeren, siyasi amaçlı, terörist veya devlet destekli tehditler olmak üzere farklı kaynaklara sahip olabileceğine dikkat çekilmiştir (Avrupa Komisyonu, 2013b: 2). Bu sebeple belgenin ilgili bölümünün öncelikle bağlamı tasvir ettikten sonra, tehdit tanımlamasını yaptığı görülmektedir. Bu da güvenlik söz ediminin kullanıldığı yerdir.

AB, siber uzayın açık (open) ve özgür (free) olmasını onamıştır. Strateji belgesinde temel haklar, demokrasi ve hukukun üstünlüğü siber uzayda korunması gereken temel ilkeler olarak belirtilmiştir. Stratejide, özgürlüğün ve refah seviyesinin artan bir biçimde sağlam ve yenilikçi internete bağlı olduğu ifade edilmiştir (Avrupa Komisyonu, 2013b). Özgürlüğün aynı zamanda güvenliği de gerektirdiğinin ve siber uzayın, kötü niyetli faaliyetler ve yanlış kullanımlara karşı korunması gerektiğinin altı çizilmiştir. Bu alanda hükümetlere düşen rollere büyük önem atfedilmiştir. Hükümetlerin, erişim ve açıklığı korumak, temel haklara saygı, internetin güvenilirliğini

politikalar da strateji belgesi ile harmanlanarak bu kapsamda tek bölüm halinde sunulmuştur. Strateji belgesinden ve diğer AB dokümanlarından Türkçeye yapılan çeviriler yazar tarafından yapılmıştır.

ve birlikte işlerliğini (interoperability) korumak gibi çeşitli görevleri olduğunu belirtmiştir. Aynı zamanda, sektörde öncü rolü üstlenmek ve başarılı olmak istenilmesi durumunda özel sektörlere de önemli roller düştüğüne dikkat çekilmiştir (Avrupa Komisyonu, 2013b:2). Strateji belgesine göre, bilgi ve iletişim teknolojileri ekonomik büyümenin belkemiği haline gelmiştir ve tüm ekonomik sektörlerde kritik bir rol oynamaktadır. Günümüzde, finans, ekonomi, sağlık, enerji ve ulaşım gibi birçok iş modeli varlığını internet ve bilgi sistemlerinin düzgün işleyişi üzerine inşa etmektedirler. (Avrupa Komisyonu, 2013b: 2)

AB tarafından, Avrupa Dijital Tek Pazarının[37] sağlanarak, GDP (Gross Domestic Product/Gayrisafi Yurtiçi Hâsıla) oranını yılda yaklaşık 500 milyar Euro (ortalama olarak kişi başına 1000 Euro) artırmanın mümkün olduğu belirtilmektedir. (EPC, 2010) Dijitalleşme kapsamında bilgi iletişim araçları arasındaki bağlantı için kişilerin bu sistemlere güvenmesi gerektiği belirtilmiştir. Ancak, Avrobarometre'nin AB üyesi ülke vatandaşları arasında yaptığı araştırmalarına göre, yaklaşık 3 Avrupalıdan birinin birbirlerinin internet kullanma yeteneklerine güvenmedikleri belirtilmiştir (Eurobarometer, 2012). Büyük bir çoğunluğun da açık olarak güvenlik problemleri nedeni ile bilgi iletişim ağları ile yakın ilişkiler kurmaktan çekindiği belirtilmiştir. Çalışma kapsamında her on kişiden en az birinin internet korsanlığı saldırısının kurbanı olduğu vurgulanmıştır (Eurobarometer, 2012). Bu da bize siber güvenlik ile ilgili olarak alımlayıcı kitlede bu konuda geliştirilecek politikaları kabul etme potansiyelinin varlığını göstermektedir.

Strateji Belgesinde tehdit tanımlaması çerçevesinde AB ekonomisinin çeşitli yönlerden siber suçlardan etkilendiği, siber suçluların daha karmaşık metotlar kullanarak, bilgi sistemlerinin içine sızmakta, önemli bilgileri çalmakta oldukları ifade edilmiştir (Avrupa Komisyonu, 2013b: 3). Ekonomik casusluğun ve devlet odaklı aktivitelerin artmasının AB üyesi devletlerin hükümetlerinde ve şirketlerde yeni bir güvenlik alanı

[37] Avrupa Dijital Tek Pazarı(DTP), insanlar ve iş için dijital fırsatlar açmak ve dijital ekonomide bir dünya lideri olarak Avrupa'nın pozisyonunu geliştirmeyi amaçlamaktadır. Avrupa Komisyonunun 10 siyasi önceliğinden biri olan Dijital Tek Pazar ile kişilerin, hizmetlerin ve sermayenin serbest dolaşımının sağlanması, sorunsuz adil rekabet koşulları altında, işletmelerin, tüketicilerin ve kişisel verilerin sağlandığı yüksek güvenlikli çevrim içi faaliyetlerinin gerçekleştirilmesi beklenmektedir. 6 Mayıs 2015 tarihinde kabul edilen Dijital Tek Pazar stratejisi, 2016 yılı sonuna kadar 16 girişimcinin de dâhil olmasıyla tamamlanması planlanmaktadır. "Erişim", "çevre", ve "ekonomi ve toplum" olmak üzere üç sütun üzerinde inşa edilen DTP ile dijital teknolojilerin gelişmiş kullanımı ile yeni olanaklar sunarak yeni istihdam alanları oluşturmak amaçlanmaktadır. (Avrupa Komisyonu, 2016a)

oluşturduğu belirtilmiştir. Öte yandan, AB dışındaki ülkelerin, siber uzayı devamlılığı sağlayabilmek ve kendi vatandaşlarını kontrol etmek amacıyla kullanabildiği, ancak, AB'nin bu konuda tamamen temel hakların korunmasına dayalı bir tutum izlediği ifade edilmiştir. (Avrupa Komisyonu, 2013b: 3) Burada yapılan vurgu, güvenlik ile özgürlük dengesinin gözetildiği ve devletlerin bekası söylemiyle siber uzayın kişi hak ve hürriyetlerini kısıtlayıcı şekilde kullanılmaması gerektiğidir.

Yukarıda sayılan faktörler dünyadaki hükümetlerin neden kendi siber güvenlik stratejisini geliştirdiğini ve bu konuyu neden en önemli uluslararası sorunlardan biri olarak gördüğünü açıklamaktadır. AB, strateji belgesi ile siber güvenliğin sağlanmasında önemli bir adım atmaktadır. Bu açıdan strateji belgesinde bağlam kısmında incelenen hususların tehdidin tanımlanmasında ve kamuoyu oluşturabilecek altyapının hazırlanmasına bir giriş olduğu söylenebilir. Belgenin başlı başına yaşamsal (existential) olan tehdidin tanımlanmasından, alımlayıcı kitleye kabul ettirilip, buna yönelik acil önlemlerin alınmasını ihtiva ettiğini söylemek mümkündür. Stratejide, bundan sonraki bölümlerde, AB politikaları ve AB kurumları ile üye devletlere yüklenen sorumluluklar ön plana çıkmamaktadır. Tezin izleyen bölümünde bunlara değinilmektedir.

3.2.2. AB için Siber Güvenliğin İlkeleri

Strateji belgesinde sınırsız ve çok katmanlı internetin, hükümetlerin düzenlemeleri olmaksızın küresel ilerlemenin en önemli aracı haline geldiği ifade edilmektedir. (Avrupa Komisyonu, 2013b: 3). Özel sektörler internetin yapımında ve yönetiminde öncü rol oynarken; şeffaflığın, hesaplanabilirliğin ve güvenilir olmanın önemi gün geçtikçe artmaktadır. Bu strateji belgesi aynı zamanda AB'nin siber güvenlik politikasının da temellerini çizmektedir. Bu bağlamda AB, strateji belgesinde ilk olarak siber güvenlik politikalarında geçerli olmak üzere siber güvenliğin ilkelerini belirlemiştir (Avrupa Komisyonu, 2013b: 3). AB, siber güvenliğin ilkelerini "AB'nin temel değerleri", "temel hakların, düşünce özgürlüğünün, kişisel bilgilerin ve gizliliğin korunması", "herkes için erişim", "demokratik ve etkili çok paydaşlı yönetişim" ve "güvenliği sağlamak için paylaşılmış sorumluluk" olarak beş ilke şeklinde belirtmektedir (Avrupa Komisyonu, 2013b: 3). Strateji belgesinde belirtilen bu ilkeler ile güvenlikleştirme sürecindeki başvuru nesnesine referans gösterilecek bir temel oluşturulduğu söylenebilir. Burada tehditle başa çıkılırken güvenlik ve özgürlük arasındaki ilişkinin bu ilkeler üzerinden sağlanmaya çalışıldığı söylenebilir. Bu da, alınacak önlemlerin güvenliğin

negatif değer olduğu vurgusunu yapan Kopenhag Ekolünün öngörüsüne benzer şekilde temel hak ve özgürlükleri kısıtlamaması gerektiği şeklinde yorumlanabilir.

Bu bağlamda, AB'nin temel değerlerinin sadece fiziksel dünyada değil dijital dünyada da geçerli olduğu belirtilmiştir. Günlük hayatta geçerli olan yasaların, teamüllerin ve normların siber uzayda da aynı şekilde geçerli olduğu belirtilmiştir (Avrupa Komisyonu, 2013b: 4). Diğer yandan, Siber güvenliğin ancak AB'nin temel değerleri ve anayasal hakları tehdit etmediği sürece etkili olabileceği vurgulanmıştır. Karşılıklı olarak bireysel hakların da güvenilir bir ağ ve bilgi sistemleri olmadan korunamayacağı dile getirilmiştir. Siber güvenlik için kişisel bilgiler ağlarda tutulurken AB veri koruma yasasına[38] uygun davranılması gerektiği belirtilerek, kişisel verilerin gizliliğine önem atfedilmiştir (Avrupa Komisyonu, 2013b: 4).

Sınırlı internetin vatandaşlar için dezavantaj oluşturduğu vurgulanmakla birlikte herkesin internete erişebilmesi ve bilgi akışında bulunabilmesi için gerekli düzenlemelerin yapılması gerekliliği belirtilmiştir. İnternetin güvenliği ve emniyetinin herkes için sağlanması gerekliliği belirtilmiştir. Dijital dünya tek bir yapı tarafından kontrol edilememektedir. Yönetişimi etkileyen birçok aktör bulunmaktadır. İnternetin gelişimi ile birlikte sivil toplum kuruluşları, ticari faaliyet gösteren firmalar bu yapılarda yer alabilmektedir. (Avrupa Komisyonu, 2009a) AB'nin, bu çok paydaşlı yönetişim yaklaşımını ve tüm paydaşların internete girebildiği oluşumları desteklediği vurgulanmıştır. Bu politika ile bunun zemini oluşturulmuş ve desteklenmiştir. Her alanda bilgi ve iletişim teknolojilerindeki artan bağımlılık insan hayatı gibi doğru tanımlanması gereken konularda açıklara yol açmıştır. Tüm ilgili aktörlerin, ister kamu yetkilileri, ister özel şirketler ya da vatandaşlar siber güvenliği güçlendirmek için birlikte hareket etmesi ve koordineli bir şekilde çalışması gerekliliğine vurguda bulunulmuştur. Nitekim güvenlikleştirme kuramı ile bağdaştırmak gerekirse alımlayıcı kitlenin hacimsel büyüklüğünün yanı sıra, tüm aktörlerin koordineli çalışmasının başarılı bir güvenlikleştirme için önemli olduğu söylenebilir. Çünkü güvenlikleştirme sadece söz edimi ve bunun alımlayıcı kitle tarafından kabulünden oluşmaz.

[38] AB veri koruma yasası, 11 Haziran 2015'te Avrupa Konseyine (Council of the European Union) gönderilen düzenlemeyi ifade etmektedir. Verilerin korunmasına ilişkin olarak detaylı yasal düzenleme kişisel verilerin korunması ve işlenmesi ile ilgili politikaları ve düzenlemeleri içermektedir. (Avrupa Birliği Konseyi, 2015)

3.2.3. Stratejik Öncelikler ve Eylemler

Strateji belgesinin "Stratejik Öncelikler ve Eylemler" bölümünde AB'nin herkese özgürlük sağlayabilecek ve herkesin yararlanabileceği çevrimiçi bir çevre oluşturabilmesinin üzerinde durulmuştur. Bu bölümün güvenlikleştirme kapsamında alınacak önlemleri içerdiği söylenebilir. Strateji belgesi, siber güvenlik alanında AB üyesi ülkelerin öncelikli rolü olduğunu belirtmekle birlikte, bu strateji ile aynı zamanda AB'nin daha etkin bir politika oluşturulabileceği üzerinde durmuştur. AB kurumları, üye devletler ya da şirketler gibi birçok aktör içeren kısa ya da uzun vadeli eylemlerin oluşturulması gerektiği vurgulanmıştır. (Avrupa Komisyonu, 2013b: 4)

AB, stratejisini bu bağlamda beş önemli nokta çerçevesinde belirlemiştir: Siber direnci başarabilmek, şiddetli bir biçimde siber suçları azaltabilmek, siber savunma stratejisi ve Ortak Güvenlik ve Savunma Politikası ile ilgili kabiliyetler geliştirmek, siber güvenlik için endüstriyel ve teknolojik kaynaklar geliştirmek, AB için tutarlı bir uluslararası siber güvenlik politikası oluşturmak ve AB'nin temel değerlerini ilerletmek. Bu beş noktayı detaylı şekilde değerlendirmek faydalı olacaktır.

3.2.3.1. Siber Direnci Başarabilmek

Strateji belgesinde siber direncin sağlanabilmesinin, hem devletlerin hem de özel sektörlerin etkili bir biçimde iş birliği içinde olması ile mümkün olduğu vurgulanmıştır (Avrupa Komisyonu, 2013b: 5). Siber risklere karşı uzlaşılmış bir işbirliği eylemlere karşı ulusal sınırları aşan bir yaklaşım sergilenmesi ve acil durumlarda tüm ülkeler tarafından uyumlu bir cevap verilmesi sağlanabilecektir. (Avrupa Komisyonu, 2013b: 5) Bunun da iç pazarların iyi işlemesini ve AB içinde iç güvenliğin artmasını sağlayan bir durum olarak karşımıza çıkacağı belirtilmektedir (Avrupa Komisyonu, 2013b: 5).

Bu bağlamda strateji belgesi özellikle NIS'in önemine değinmiş ve üye devletler arasında işbirliği, bilgi paylaşımı ve koordinasyonun gerekliliğine vurgu yapmıştır. Belgede ayrıca ağ ve bilgi sistemlerinin büyük çoğunluğu özel sektörde de kullanıldığı için siber güvenliğin sağlanabilmesi için özel sektörle iş birliğinin önemi vurgulanmıştır. Özel sektörün, sektörler arasındaki en iyi uygulamaları paylaşarak kendi siber esneklik kapasitelerini geliştirmeleri gerektiği belirtilmiştir. Ayrıca endüstri tarafından geliştirilen araçlarla sebep ve sonuçları ortaya koyan mekanizmaların kamu sektörü için de yararlı

olacağı vurgulanmıştır. Ancak, yine güvenlik söylemiyle, bu düzenlemelere rağmen özel sektörlerin hala NIS olaylarına karşı güvenilir bilgi sağlamaktan yoksun olup, kriz yönetimini tam olarak sağlayamadıkları ve güvenilir çözümler bulmakta zorlanmakta oldukları belirtilmiştir. Yine bu bağlamda alınacak önlemler şu şekilde sıralanmıştır: En önemi alanlarda (enerji, ulaşım, bankacılık, borsa, internet servis sağlayıcıları) karşılaşılacak riskleri değerlendirip, kriz yönetimi için güvenilir ve dirençli bilgi sistemleri ve ağlar sağlamak. (Avrupa Komisyonu, 2013b: 6) Siber güvenlik kültürünü algılamanın, özel sektörlerde iş fırsatları ve rekabeti artırmak anlamına geldiği ve bu kuruluşların ulusal NIS sağlayıcılara bilgi vermekte ve bilginin güvenilirliğinin devamını sağlamaya çalışmakta oldukları vurgulanmıştır. Ulusal NIS otoritelerinin diğer düzenleyici organlarla (özellikle kişisel veri koruma yetkilileriyle) uyumlu bir işbirliği içerisinde olması gerektiği ve NIS sağlayıcıların ayrıca oluşabilecek risklere karşı da kanun uygulayıcılarına rapor vermesi gerektiği vurgulanmıştır. (Avrupa Komisyonu, 2013b: 6)

Strateji belgesinde ayrıca Avrupa Kamu-Özel Ortaklığı'nın (EP3R), AB düzeyinde geçerli ve uygun bir platform olduğu ve bunun daha da daha geliştirileceği belirtilmiştir. EP3R kapsamında, kamu sektörü ve özel sektör arasındaki iş birliği geliştirilerek politikaların etkinliği artırılmaya çalışılmaktadır. (Avrupa Komisyonu, 2009b) Ayrıca bu strateji ile birlikte AB çapında üye devletlerin NIS yeteneklerini koordine ederek işbirliğini kolaylaştırıp telekomünikasyon gibi önemli altyapılar için mali destek sağlayacak Bağlantılı Avrupa Kuruluşu (The Connecting Europe Facility/CEF) düzenlenmiştir. (Avrupa Komisyonu, 2015a) AB içinde gerçekleşen siber olaylarda üye devletlerin ve özel sektörün uyum içinde olması da önemlidir.

Strateji Belgesinde Avrupa Komisyonun yapacağı görevler ise şu şekilde belirtilmiştir: Komisyon'un ortak araştırma merkezi tarafından yürütülen aktivitelerine üye devletlerle, kritik altyapı sahipleriyle ve operatörleriyle yakın işbirliği içinde devam etmesi ve dirençli sistemler geliştirmek için teşviklerde bulunmak, 2013'ten önce AB destekli yeni projelere imza atarak kötücül yazılımlarla mücadele etmek gibi faaliyetlerdir(Avrupa Komisyonu, 2013b: 7). Bu eylem planı kapsamında 7,7 Milyon

Euro tutarında AB fonu ile 15 Milyon Euro genel bir bütçeye sahip olan CIP[39]-ICT PSP[40]-2012-6 oluşturulmuştur (Avrupa Komisyonu, 2016b). Siber direnci başarabilmek için ayrıca ENISA'dan beklenen düzenlemeler ise şu şekilde belirtilmiştir: Üye devletleri, özellikle, ulaşım ve enerji altyapısı gibi endüstriyel kontrol sistemleri konusunda ulusal siber direnç kapasiteleri geliştirmeye teşvik etmek; 2013 yılında AB için Endüstriyel Kontrol Sistemleri - Bilgisayar Güvenliği Olaylarına Müdahale Ekibi (ICS-CSIRTs)[41] nin fizibilitesini incelemek; üye devletleri ve AB kurumlarını Pan Avrupalı siber olaylara karşı desteklemeye devam etmek. Ayrıca, bu strateji ile Komisyon Endüstriden ise, kamu sektörü ile işbirliği içerisinde güçlü bir koruma sistemi için öncülük yapmasını istemiştir. (Avrupa Komisyonu, 2013b: 7)

Farkındalığı artırmak için siber güvenliği sağlamanın AB için ortak bir sorumluluk olduğu ve son kullanıcıların ağ ve bilgi güvenliğinin sağlanmasında önemli bir rol oynadığına stratejide özel vurgu yapılmıştır. Onların çevrimiçi iken karşılaşabilecekleri sorunlara karşı farkında olmaları gerektiği ve siber saldırıları basit adımlarla önleyebileceği ile birlikte son zamanlarda geliştirilen girişimlere devam edilmesi gerekliliği vurgulanmaktadır. Bu ifade de yine hedef kitlenin harekete geçirilmesi (mobilization) açısından yine güvenlikleştirme teorisi ile kolaylıkla açıklanabilir. Stratejide ayrıca, Europol, Eurojust ve ulusal veri koruyucuların da farkındalığı artırma konusunda aktif olarak rol oynamalarının sağlanması konusunda çalışmalar yapılacağı belirtilmiştir. (Avrupa Komisyonu, 2013b: 9)

3.2.3.2. Siber Suçları Büyük Ölçüde Azaltmak

Dijital dünyada yaşamaya devam ettikçe, siber suçluların sömürmek için fırsatları artmaya devam edecektir. Siber suçlar en hızlı büyüyen suç şeklidir, her gün bir milyondan fazla insan siber suça maruz kalmaktadır (Avrupa Komisyonu, 2013b: 9). Bu suç şebekeleri her gün daha yanıltıcı ve karışık işlemeye devam etmekte ve bunlarla mücadele için daha güvenilir sağlam araçlara ihtiyaç duyulmaktadır. Siber suçlular az riskle ve büyük parayla çalışmaktadırlar. Bu da bu alanı klasik suçlardan daha çok tercih

[39] Competitiveness and Innovation framework Programme (Rekabet Edebilirlik ve Yenilik Çerçeve Programı)
[40] Information and Communication Technologies Policy Support Programme (Bilgi ve İletişim Teknolojileri Politika Destek Programı)
[41] Computer Security Incident Response Team(s) for Industrial Control Systems (Endüstriyel Kontrol Sistemleri - Bilgisayar Güvenliği Olaylarına Müdahale Ekibi)

edilen bir yöntem olarak kullanılmaya teşvik etmektedir (Avrupa Komisyonu, 2013b: 9). AB'nin siber suçları azaltmak için kullandığı yöntemlerin, güvenlikleştirme sürecindeki tehdidin inşasından sonra acil ve olağanüstü eylemler ile önlem alınması gerekliliği ile açıklanması mümkündür. Bu bağlamda siber suçları azaltmak için güçlü ve etkili bir yasamanın varlığı büyük önem arz etmektedir.

3.2.3.2.1. Güçlü ve Etkili Yasama

AB'nin ve üye devletlerin siber suçlarla mücadele edebilmek için etkili yasalar yapmak zorunda olduğu strateji belgesinde vurgulanan konulardan olmuştur. 2001 yılında oluşturulup, 2004 yılında imzaya açılan ve Budapeşte Sözleşmesi[42] olarak bilinen Avrupa Konseyi'nin (Council of Europe) siber suçlar üzerine kabul ettiği ve AB'nin de taraf olduğu anlaşma, uluslararası düzeyde kapsamlı bir çerçevenin kabul edildiğinin göstergesi olarak karşımıza çıkmaktadır. Ayrıca, AB, siber güvenlikle ilgili cinsel istismar ve çocuk pornografisi konusunda bir direktifi kabul etmiştir. (Avrupa Birliği, 2011) AB özellikle botnet kullanımı yoluyla, bilgi sistemlerine karşı saldırılar üzerine bir Direktif üzerinde de anlaşmaya varmıştır. (Avrupa Komisyonu, 2014) Avrupa Komisyonunun güçlü ve etkili yasama için gerekli olan şu düzenlemeleri yapması planlanmıştır: Siber suç ile ilgili direktiflerin hızlı aktarılması ve uygulanmasını sağlamak; Siber Suçlarla ilgili Avrupa Konseyi Budapeşte Sözleşmesini onaylamayan üye devletlerin mümkün olduğu kadar erken onaylamasını sağlamak (Avrupa Komisyonu, 2013b: 9). Bu noktada bu tedbirlerin güvenlikleştirme çerçevesinde olağandışı önlemler olarak değerlendirilemeyeceğini ama AB'nin bu alanda yoğunlukla yasama yoluyla tehditle başa çıkılmasını tercih ettiğini söylemek mümkündür. Diğer taraftan, bu uygulamaların hangilerinin temek hak ve özgürlükler açısından sorunlara yol açtığının görülmesinin biraz zaman alacağı da söylenebilir.

3.2.3.2.2. Siber Suç ile Mücadele için Operasyonel Yeteneği Geliştirmek

Strateji belgesinde Siber suç tekniklerinin hızla gelişmesi kanun uygulayıcı kurumların güncel olmayan operasyonel araçlarla siber suçlarla mücadelesi olanaksız hale geldiği belirtilmiştir. Yine belgeye göre, Bugün, tüm AB üyeleri siber suçlara etkili

[42] Siber suçlar sözleşmesi olarak bilinen ve Avrupa Konseyi (Council of Europe) tarafından 2001 yılında Strazburg'da oluşturulup, 2004 yılında imzaya açılan bilgisayar suçları ile internet suçlarını ilk defa gözeten uluslararası bir anlaşmadır. 2015 yılı Kasım ayı itibariyle sözleşmeyi 47 ülke imzalamış ancak 7 ülke henüz ulusal yasama sürecini tamamlamamıştır. (Avrupa Konseyi, 2001)

olarak karşılık verecek mekanizmalara sahip değildir. Dolayısıyla, üye ülkelerin etkili ulusal siber suç birimlerine olan ihtiyaçları stratejide vurgulanan bir diğer husus olarak karşımıza çıkmaktadır (Avrupa Komisyonu, 2013b: 9). Stratejide alınan önlemler konusundaki yetersizliğe dikkat çekilmesi de güvenlikleştirme çerçevesinde okunabilir. Burada aciliyet de görmek mümkündür.

Siber suçlarla mücadelede operasyonel yeteneklerin geliştirilmesi için Avrupa Komisyonu tarafından yapılması gerekenler stratejide şu şekilde belirtilmiştir: Fonlama programları aracılığıyla, üye devletlerin boşlukları tespit etmesi ve siber suçları araştırması konusunda desteklemelidir. (Avrupa Komisyonu, 2014) Stratejiye göre Avrupa Komisyonu ayrıca akademi, üye devletlerin hükümetleri ve özel sektör arasındaki bağlantıyı kurmalıdır; üye devletlerle birlikte siber suçlarla mücadele için en iyi önlemi (tehdit analizi gibi) almalıdır; Avrupa siber suç merkezi[43] ile yakın bir çalışma içerisinde olmalıdır. Ayrıca Komisyon, ortak politikalar geliştirmek için Eurojust ve Europol ile uyum içinde olmalıdır (Avrupa Komisyonu, 2013b: 10). Siber suçlarla mücadelede operasyonel yeteneklerin geliştirilmesine yönelik gerçekleşecek eylemleri de güvenlik sektörleri ile ilişkilendirmek mümkündür. Siber güvenliğin tüm diğer güvenlik sektörleri ile geçişken bir yapısı olduğu iddiası bu örnekle de kanıtlanmaktadır.

3.2.3.2.3. AB Düzeyinde Koordinasyonu Geliştirme

Siber güvenlik strateji belgesinde koordinasyonun önemi vurgulanırken, AB'de kolluk kuvvetlerinin ve adli makamların, AB ve ötesinde kamu ve özel paydaşları bir araya getirerek koordineli ve işbirlikçi bir yaklaşımla üye devletlerin işini tamamlayabileceği belirtilmektedir. Bu kapsamda Komisyon, Europol ve Eurojust'a büyük görevler düştüğü ifade edilmiştir. Komisyonun, Avrupa Siber Suçlar Merkezi (EC3) çalışmalarını siber suçlarla mücadelenin odak noktası olarak kabul edip desteklemesi beklenmektedir. Ayrıca analiz ve istihbaratı desteklemesi, araştırmalar yapması, işbirliğini kolaylaştırması, üye devletler, özel sektör ve diğer yetkili paydaşlar ile bilgi paylaşımı için kanallar oluşturması gibi konularda aktif rol alacağı vurgulanmaktadır. Komisyonun bu alandaki rolü strateji belgesi sonrasında da tekrar değerlendirilmiş ve Birlik Hukuku ve veri koruma kanunu ile uyumlu bir çalışma yürütülmesini sağlamak da görevlerinin arasına eklenmiştir. (Avrupa Birliği Konseyi,

[43] Avrupa Siber Suçlar Merkezi (The European Cybercrime Centre) (EC3), AB ve Europol iş birliği ile 2013 yılında kurulan ve AB üyesi ülkelerdeki bilgisayar suçları ile ilgilenen birimdir (Europol, 2016a).

2015a) Bunun dışında Komisyon, Çocukların sanal ortamlar üzerinden cinsel istismarı ile ilgili yeni mevzuat üzerinde AB çabalarını artırmaya çalışmaktadır. (Avrupa Birliği, 2011) Komisyon çocuklar için daha iyi bir internet için Avrupa stratejisini kabul etmiş ve diğer ülkelerle küresel bir ortaklık da başlatmıştır (Avrupa Komisyonu, 2012).

Ayrıca Komisyon, Europol'den üye devletlerin siber suç soruşturmaları için Avrupa Polis Koleji (CEPOL[44]) iş birliği ile operasyonel ve analitik destek sağlamasını, çocuk cinsel istismarı, dolandırıcılık, botnet ve saldırı alanlarında siber suç örgütlerinin lağvedilmesini sağlaması için talepte bulunmuştur. Düzenli olarak stratejik ve operasyonel raporlar üretme ve eylem tanımlama misyonunu da Europol'e aktarmıştır (Avrupa Komisyonu, 2013b: 10). Komisyon Eurojust'tan ise siber suç araştırmalarına adli işbirliği için ana engellerin belirlenmesi ve üye devletler ve üçüncü ülkeler arasında koordinasyon sağlanarak operasyonel ve stratejik düzeyde eğitimler verilmesi talebinde bulunmuştur (Avrupa Komisyonu, 2013b: 10). Komisyonun bu girişimleri kurumsal bazda alınan önlemlere örnek gösterilebilir. Genel olarak Komisyonun Eurojust ve Europol'den bu taleplerinin siber mücadelede etkinliği artırmak için görev ve yetki paylaşımı yaparak, bilgi alışverişi yoluyla işbirliği içinde olmak olarak değerlendirilebilir.

3.2.3.3. Ortak Güvenlik ve Savunma Politikası (OGSP) Çerçevesinde Siber Savunma Politikası Geliştirmek

Strateji belgesinde, siber güvenlik için siber savunma çabasının gerekliliği de vurgulanmıştır (Avrupa Komisyonu, 2013b: 11). Bu vurgu bu tez için askeri güvenlik ile siber güvenlik bağlantısını göstermesi açısından önemlidir. Strateji belgesinde ayrıca üye devletlerin iletişim ve bilgi sistemlerinin dayanıklılığını artırmak için savunma politikalarını ve ulusal çıkarlarını da destekleyen bir siber savunma politikası geliştirilmesi gerektiği belirtilmiştir (Avrupa Komisyonu, 2013b: 11). Tehditlerin çok yönlü olduğu varsayılarak, kritik siber varlıkların korunmasında sivil ve askeri yaklaşımlar arasındaki sinerjinin geliştirilmesi gerektiği vurgulanmıştır. Araştırma ve geliştirmeyi de içeren bu çabaların üye devletlerin hükümetleri, akademi ve özel sektörler arasındaki yakın iş birliği ile desteklenmesi gerektiği belirtilmiştir. Ayrıca AB ve

[44] European Police College (CEPOL) (Avrupa Polis Koleji), 2000 yılında tasarlanan ve 2014 yılından itibaren aktif olarak AB'ye kolluk kuvveti yetiştirmek için gerekli eğitimleri ve personeli sağlayan Budapeşte'de kurulmuş bir okuldur. AB bütçesi tarafından finanse edilen CEPOL'e siber suçların önlenmesi için kalifiye personel yetiştirilmesi görevi de verilmiştir. (CEPOL, 2016)

NATO'dan her iki örgütün de üyeleri olan devletlerin dayandığı kritik hükümet, savunma ve diğer bilgi altyapılarının direncini artırmak için nasıl önlem aldıklarını araştırarak mükerrerliği (duplication) önlemeyi hedeflenmiştir (Avrupa Komisyonu, 2013b: 11).

Siber güvenliğin askeri güvenlik boyutunu ortaya koyan bir şekilde, Yüksek Temsilcinin aşağıdaki temel faaliyetlere ağırlık vermesi gerektiği strateji belgesinde belirtilen bir diğer önemli husus olarak karşımıza çıkmaktadır (Avrupa Komisyonu, 2013b: 11-12).

- Operasyonel AB siber savunma gerekliklerini ve teknolojilerini tüm yönleriyle değerlendirmek ve geliştirmek, doktrin, liderlik, organizasyon personel, teknoloji, altyapı, birlikte çalışabilirliği sağlamak,
- OGSP misyonları çerçevesinde bir siber savunma stratejisi benimsemek, dinamik risk yönetimini sağlayabilmek ve gelişmiş tehdit analizi yapabilmek,
- AB'nin sivil ve askeri kanadı arasında diyalog ve koordinasyon sağlamak (bilgi akışı, erken uyan, risk değerlendirmesi, farkındalığı artırma)
- Uluslararası ortaklarla (NATO ve diğer uluslararası organizasyonlar ve benzerleridir) ilgili diyalog sağlamak.

Yüksek Temsilciye yüklenen bu sorumluluklar ile güvenlikleştirme sürecindeki söz ediminin kullanımı ve önlemler alınması açısından, süreçteki aktörlerden birinin AB'nin kendi güvenlik stratejisini hazırlayacak olan/hazırlayan –yani bu konuda yetkili– bir figür olması dikkat çekicidir. Dolayısı ile burada Yüksek Temsilci gibi AB'de önemli ve stratejik görevlere sahip birinin bu misyonu yüklenmesi güvenlikleştirme sürecine hizmet eden bir unsur olarak karşımıza çıkmaktadır.

3.2.3.4. Siber Güvenlik için Endüstriyel ve Teknolojik Kaynakları Geliştirmek

Strateji belgesinde Avrupa'nın mükemmel araştırma ve geliştirme kapasitelerine sahip olduğu fakat yenilikçi endüstriyel ve teknolojik ürün sunan birçok küresel liderin AB dışında bulunduğuna dikkat çekilmektedir. Avrupa'nın bu dışa bağımlığının yeni riskleri de ortaya çıkartabileceği vurgulanmaktadır. Dolayısıyla AB sınırları dışında üretilen teknoloji için çözümlerde menşeinin bulunduğu yerlerde üretilmekte ve bu da bağımlılık seviyesini artıran bir durum olarak karşımıza çıkmaktadır. Bu bağımlılığı azaltıp AB içinde gerekli çözümlerin bulunabilmesi için düzenlemelere duyulan ihtiyaç

vurgulanmaktadır (Avrupa Komisyonu, 2013b: 12). Bu kapsamda siber güvenlik ürünleri için Tek Pazarı, AR-GE yatırımlarını ve yenilikçiliği teşvik etme özel başlıklar altında değerlendirilmiştir. Bu eylemlerin, güvenlik sektörlerinden ekonomik güvenlik sektörü kapsamında detaylı olarak değerlendirilmiş bir alan olduğu söylenebilir. AB'nin söylemini pekiştirmek ve politikanın etkinliğini sağlayabilmek için kullandığı yöntemlerin güvenlikleştirme süreçlerini pekiştirdiğini söylemek yerinde olacaktır.

3.2.3.4.1. Siber Güvenlik Ürünleri İçin Tek Pazarı Teşvik Etme

Strateji belgesinde, yüksek seviyede güvenliği sağlamanın sadece güvenliği öncelik haline getirerek çözümlenebileceği vurgulanmıştır. Yani burada açıkça aciliyet ve öncelik vurgusu vardır.

Buna rağmen bazı aktörlerin hala güvenliğe birçok gelir getiren konudan daha az önem verdiği gözlemlendiği ve Avrupa'da kullanılan Bilgi ve İletişim Teknolojileri (Information and Communication Technology–ICT) ürünleri için siber güvenlik performans gereksinimlerinin olması gerekliliği vurgulanmıştır. Bu bağlamda özel sektörü rekabete sürükleyecek teşviklerin gerekliliğine dikkat çekilmiştir (Avrupa Komisyonu, 2013b: 12). Yeterli siber performans gösteren şirketleri, iyi bir siber güvenlik performansı ile ödüllendirip bu şirketleri satış noktası yapmak gibi bir örnek ile bunun sağlanabileceği düşünülmektedir. Son derece güvenli ürünler için Avrupa çapında bir piyasa talebi yaratılması gerekliliği vurgulanmaktadır. İlk olarak bu stratejinin, Bilgi ve iletişim teknolojileri ürünlerinde güvenlik konusunda işbirliği ve şeffaflığı artırmayı hedeflediği belirtilmiştir. Bu değer zinciri boyunca, iyi bir siber güvenlik uygulaması belirlemek ve oluşturmak için ilgili Avrupa kamu ve özel paydaşlarını bir araya getirerek bir platform kurulması çağrısı yapılması, güvenli bilişim çözümleri geliştirilmesi ve benimsenmesi vurgulanmaktadır. Risk yönetimi gibi konularda AB çapında sertifika programları düzenlenmesi gerekliliği de stratejide belirtilmiştir. Komisyonun konumsal farklılıkların yarattığı dezavantajları önlemek için üye devletler arasında tutarlı yaklaşımların benimsenmesini teşvik etmeyi hedeflediği de vurgulanmıştır. (Avrupa Komisyonu, 2013b: 12)

İkinci olarak, Komisyonun güvenlik standartlarının gelişimini destekleyerek ve veri güvenliğini sağlamak için sertifika programlarıyla bu iş birliği düzenlemelerine yardımcı olmayı planlandığı belirtilmiştir. Çalışmanın endüstriyel kontrol sistemleri,

enerji ve ulaşım altyapısı gibi kritik ekonomik sektörlerde, özellikle tedarik zincirinin güvenliğine odaklanması beklendiği vurgulanmıştır (Avrupa Komisyonu, 2013b: 13). Böyle bir çalışma üzerine inşa edilen ve devam eden Siber Güvenlik Koordinasyon Grubu (CSCG) ve Avrupa Standardizasyon Kuruluşları[45] (CEN, CENELEC ve ETSI) standardizasyon çalışmalarının yanı sıra ENISA, Komisyon ve diğer birlik kurumlarının uzmanlık alanlarının genişletilmesi hedeflenmiştir. (Avrupa Komisyonu, 2011b) Komisyonun bu kapsamda yapacağı ilk işin 2013 yılından itibaren birlik içindeki BİT ürünleri genelinde uygulanmak üzere kamu özel platformu kurarak kurumsal zeminin hazırlanmasını sağlamak olduğu belirtilmiştir. Ayrıca önemli derecede ortaya çıkan güvenlik açıklarının ulusal otoritelerle paylaşılması kararlaştırılmıştır (Avrupa Komisyonu, 2013b: 13). Komisyonun bu süreçte ENISA'dan ilgili ulusal yetkili makamlar, geliştirilmiş paydaşlar, Uluslararası Avrupa Standardizasyon Kuruluşları ve Avrupa Komisyonu Ortak Araştırma Merkezi ile işbirliği içerisinde teknik kurallar ve tavsiyeler geliştirmesini beklediği ifade edilmiştir. Komisyonun ayrıca, sanayi liderliğindeki güvenlik standartlarının geliştirilmesi ve benimsenmesi, siber güvenlik ile ilgili şirketlerin standartlarını geliştirmek, güvenlik etiketleri oluşturmak için kamu ve özel sektörü teşvik edeceği belirtilmiştir. (Avrupa Politika Merkezi, 2010) Stratejinin bu bölümünde ekonomik güvenlik ile siber güvenlik ilişkisinin net bir şekilde kurulduğu söylenebilir.

3.2.3.4.2. Araştırma Geliştirme (Ar-Ge) Yatırımları ve Yenilikçiliği Teşvik Etme

Ekonomik güvenlik ile ilgili olarak, AB'nin Ar-Ge yatırımlarını ve yenilikçiliği teşvik ederek güçlü bir endüstriyel politikayı desteklediği vurgulanmıştır. Yabancı teknolojilere Avrupa bağımlılığını azaltmak için iç pazarın geliştirilmesi gerekliliğinin altı çizilmiştir. Ayrıca AB'nin kriptografi gelişimini desteklemeye devam edeceği bildirilmiştir. Bu çerçevede geliştirilecek politikaların gerekli teşviklerin sağlanması ve Ar-Ge sonuçlarının gereklerinin yerine getirilmesi için ticari çözümler üreterek neticelendirmek zorunda olduğu ifade edilmiştir (Avrupa Komisyonu, 2013b: 13).

[45] Standardizasyon kuruluşları ile AB çapında minimum gereksinimler belirlenerek hizmet kalitesinin arttırılması ve standartlaşma sağlanmaya çalışılmaktadır. 1984 yılından itibaren varlıklarını devam ettiren ve 2003 yılında tekrar revize edilen ve uzmanlık alanına göre farklılık gösteren kuruluşlar AB direktifleri ile ulusal mevzuatlara da yerleşmiştir (Avrupa Birliği, 2012).

AB, Ar-Ge çalışmaları kapsamında yaklaşık 80 milyar Euro bütçeye sahip Horizon 2020[46] çerçeve programını oluşturmuştur. Komisyonun önerisi ile bu program siber suç ile mücadelede güvenilir bilgi ve iletişim teknolojileri için özel hedefleri de içermektedir. (Amos, 2014) Bu program kapsamında AB'nin bilişim teknolojileri ile ilgili güvenlik araştırmalarını desteklemesi, uçtan uca güvenli iletişim teknolojileri hizmetleri ve uygulamaları için çözümler sağlaması, mevcut çözümler için ağ ve bilgi sistemleri kurması hedeflenmektedir (Rabesandratana, 2013; Avrupa Komisyonu, 2015). Komisyonun bu kapsamda Ar-Ge yatırımları ve yenilikçiliği teşvik etmek için Horizon 2020'yi aktif bir şekilde kullanacağı ifade edilmiştir. Bu program, ayrıca siber suç ve terör faaliyetleriyle mücadele edecek araç ve gereçler geliştirmek için de bir çözüm yolu olarak düşünülmektedir. AB kurumları ve üye devletlerin kurumları arasında daha iyi koordinasyon sağlamak için araştırma gündemleri oluşturmak da Komisyona yüklenen bir misyon olarak karşımıza çıkmaktadır. (Avrupa Komisyonu, 2013b: 14) Yine benzer amaclarla 2013 yılı sonuna kadar, kamu idarelerinin satın alma gücünü geliştirmek için pratikler belirlemek ve uyumlaştırıcı çözümler bulması konusunda, endüstriyi ve akademiyi desteklemek için Komisyon ile üye devletlerin arasında görüşmeler de yapılmıştır (Eurostat, 2015).

Komisyonun Ar-Ge çalışmaları kapsamında ayrıca; ortaya çıkan eğilimleri ve ihtiyaçları karşılayacak yeterli dijital araçlar geliştirmesi için Europol ve ENISA'nın da katkılarını beklediğini dile getirmiştir (Europol, 2015). Son olarak, Komisyon kamu ve özel paydaşlardan, sigorta sektörü ile işbirliği içinde, risk primleri hesaplamak için uyumlaştırılmış ölçümlerini, buna binaen düşük risk primlerinden faydalanmak için güvenlik yatırımlarını yapmış şirketler sağlayarak siber güvenlik sektörüne yapılan yatırımların genişletilmesini istemiştir (Avrupa Komisyonu, 2013b: 14). Bu bağlamda gerçekleştirilmesi düşünülen eylemlerin, güvenlik sektörlerinden ekonomik güvenlik ile yakından ilgili olduğunu söylemek mümkündür.

[46] Horizon 2020, Avrupa Komisyonunun Avrupa Çalışma Alanı içerisinde 1984'ten bu yana sürdürdüğü çerçeve programlarından sekizincisi olarak bilinmektedir. 2014-2020 yılları arasını kapsayan süreçte gerçekleştirilecek olan araştırma ve teknolojik geliştirme çerçeve programı olarak bilinmektedir. Çerçeve programlar içinde en büyük bütçeye ve kapsama sahip olan program Horizon 2020'dir. Ayrıca siber güvenliğin sağlanması için de program kapsamında önemli ölçüde destek sağlanmaktadır. (Amos, 2014; Grove, 2011)

3.2.3.5. AB için Tutarlı Bir Uluslararası Siber Güvenlik Politikasının Oluşturulması ve AB Temel Değerlerini Teşvik Etmek

Stratejide, AB'nin uluslararası siber güvenlik politikasının oluşturulmasını sağlamak için AB'ye özgü davranış normları geliştirerek, siber güvenlikle ilgili mevcut uluslararası yasaları uygulayarak; açık, özgür ve güvenli internet kullanımını teşvik için ulusal otoritelerle işbirliği içinde çalışacağı ifade edilmiştir. AB'nin ayrıca, siyasal aktif siber kapasite oluşturmak ve uluslararası düzeyde sayısal uçurumun kapatılması için de elinden geleni yapacağı vurgulanmıştır. (Kroes, 2013) AB'nin uluslararası siber konularla bağlantısının uluslararası angajman kuralları çerçevesinde, insan onuru, özgürlük, demokrasi, eşitlik, hukukun üstünlüğü, temel haklara saygı gibi AB'nin ilkeleri temelinde ilerleyeceği belirtilmiştir (Avrupa Komisyonu, 2013b: 14; Avrupa Birliği Konseyi, 2015c). Bu yolla güvenlik ile özgürlük arasındaki dengenin kurulmaya çalışıldığı söylenebilir.

3.2.3.5.1. Siber Güvenliği AB Dış İlişkilerine Entegre Etme ve Ortak Dış ve Güvenlik Politikası

Stratejide, Komisyon tarafından sadece Yüksek Temsilci ve üye devletler aracılığı ile sınırlı olacak bir siber güvenlik politikasının yetersiz olduğunu vurgulamıştır. Bunlara ek olarak uluslararası düzeyde de işbirliği geliştirilecek uluslar arası ortaklar ve organizasyonlar ile de güçlü ilişkiler kurmayı içeren bir siber güvenlik politikasının benimsediklerini dile getirmektedir. AB'nin siber uzay konusunda uluslararası ortakları ile görüşmelerinin AB üyeleri ve üçüncü ülkeler ile olan ikili diyaloglara değer katmak uzere dizayn ve koordine edilmesi gerekliliği vurgulanmaktadır. (Avrupa Komisyonu, 2013b: 15)

Strateji belgesinde siber güvenliğin saglanmasında alınacak önlemler arasında AB'nin üçüncü ülkeler ile olan diyalogunda AB değerlerini paylaşmak konusunda hemfikir olanlara özel bir odaklanma olacağının vurgusu yapılmaktadır. Verilerin korunması konusunda yüksek seviyelere ulaşmayı teşvik ederek, siber uzay konusundaki küresel değişikliklerin üzerine eğilmek için bu alanda aktif olan Avrupa Konseyi, OECD, BM, AGİT, NATO gibi organizasyonlarla yakın işbirlikleri geliştirmeyi planladığı vurgulanmaktadır. (IBP, 2014: 127) İkili düzeyde, ABD ile işbirliğine özel bir önem atfedilmektedir. Bilhassa siber suç ve siber güvenlik konularında AB-ABD Çalışma

Grubu kapsamında daha ileri seviyelerde geliştirileceğinin sinyalleri verilmektedir. (Avrupa Komisyonu, 2011c; Avrupa Birliği Dış İlişkiler, 2014; Avrupa Komisyonu, 2010d)

Stratejide, AB'nin uluslararası siber güvenlik politikasının ana unsurlarından birinin de siber uzayı özgürlük ve temel haklar alanı olarak geliştirmek olacağı belirtilmiştir. Genişleyen internet ağının, demokratik reformları ve onun dünya çapında yükselmesini ilerletmesi için gerekli adımların atılacağı vurgulanmıştır. Artan küresel bağlantıya sansür ve kitlelerin gözetiminin eşlik etmemesi gerektiği vurgulanmıştır (Avrupa Komisyonu, 2013b: 15). Avrupa Komisyonunun 2011'de ongordugu sekilde, stratejide AB'nin kurumsal sosyal sorumluluğu teşvik edeceğinin ve bu alandaki küresel koordinasyonu geliştirmek için uluslararası girişimler başlatacağının altı çizilmiştir. (Avrupa Komisyonu, 2011d)

Stratejide öngörülen politikalarla uyumlu bir şekilde, Avrupa Parlamentosu, daha güvenli bir siber uzay için sorumluluğun vatandaştan devlete küresel bilgi toplumunun bütün oyuncularının elinde olduğunu vurgulamıştır. AB'nin bütün paydaşların bağlı olacağı siber uzayda davranış normlarını tanımlama çabalarını destekleyeceği belirtilmiştir (Pawlak, 2015). Strateji belgesinde AB'nin uluslararası güvenlik konusunda, şeffaflık ve devlet davranışında yanlış anlaşılmaların azaltılması kapsamında güven inşa edici ölçütlerin geliştirilmesinin desteklendiği vurgulanmıştır. Ayrıca, strateji belgesinde AB'nin siber konularda yeni uluslararası yasal enstrümanlar oluşturulmasından yana olmadığı belirtilmiştir. Nitekim, siber suçları tanımlamak için Budapeşte Sözleşmesinin (Avrupa Konseyi, 2001) üçüncü ülkelerin adaptasyonuna açık bir enstrüman olduğu belirtilerek, bu konvansiyonun bu alanda uluslararası işbirliği için temel bir doküman olduğu ve ulusal siber suç yasamasının şekillenmesi için bir model oluşturduğu vurgulanmıştır (Avrupa Komisyonu, 2013b: 16).

3.2.3.5.2. Üçüncü Ülkelerle Siber Güvenlik ve Kritik Bilgi Altyapı Alanlarında İşbirliği Geliştirme

Strateji belgesinde açık ve güvenilir bir erişim söz konusu olmadığı için dünyadaki herkesin internetin pozitif etkilerinden aynı ölçüde yararlanamadığı belirtilmektedir (Avrupa Komisyonu, 2013b: 16). Avrupa Birliği'nin bu nedenle erişimi geliştirmek, bütünlüğü ve güvenliği sağlamak için etkili bir siber mücadele kapsamında

üçüncü ülkelerin çabalarını desteklemeye devam edeceği belirtilmiştir (Lonardo, 2015). Stratejide, Üçüncü ülkelerle siber güvenlik ve kritik bilgi altyapısı alanlarında işbirliğinin geliştirilmesi hususunda üye devletlerle uyum içerisinde, Komisyon ve Yüksek Temsilcinin yapacakları şu şekilde ifade edilmiştir (Avrupa Komisyonu, 2013b: 16)

- Küresel siber konularda koordinasyonu ve işbirliğini geliştirmek,
- Siber güvenlik önlemleri konusunda güven arttırıcı normların gelişimini desteklemek ve Budapeşte Sözleşmesini teşvik etmek,
- Erişim de dahil olmak üzere temel hakların geliştirilmesi ve korunmasını sağlamak,
- Bilgi ve ifade özgürlüğüne odaklanmak,
    - Çevrimiçi ve çevrimdışı ifade özgürlüğü geliştirmek,
    - Kitle için kullanılacak ürün ve hizmetlerin ihracını incelemek,
    - Açıklık ve esnekliği sağlamak,
    - Paydaşların kullanımını güçlendirici iletişim teknolojisi oluşturmak,
- Kritik bilgi altyapılarının güvenliği konusunda uluslararası partnerlerle ve kurumlarla işbirliği içinde çalışmak. (Avrupa Komisyonu, 2013c; Avrupa Parlamentosu, 2012)

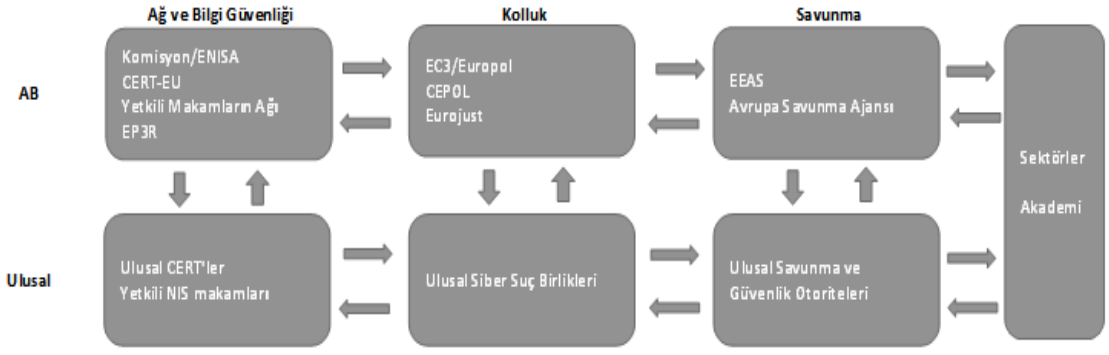
Komisyon ve Yüksek Temsilciye yüklenen bu sorumluluklar göz önüne alındığında, gerek ulusal ve uluslararası koordinasyon ve işbirliğine yönelik sorumluluklar olsun, gerekse temel hak ve özgürlüklerin korunması ile kritik bilgi altyapılarının korunmasına yönelik sorumluluklar olsun tamamının güvenlikleştirme sürecinin önemli unsurları olduğunu söylemek mümkündür. AB'nin yetenek ve araçlarını güvenlikleştirme sürecinde aktif olarak kullandığı ve bu süreçte Kopenhag Ekolünün güvenlik sektörlerini andırır şekilde çok boyutlu ele alındığını söylemek yerinde olacaktır.

3.2.4. Roller ve Sorumluluklar

Stratejinin Roller ve Sorumluluklar bölümünde AB düzeyinde ve AB üyesi ülkeler düzeyinde kimlerin hangi rolleri üstleneceğinin ve hangi kuruma hangi üye devlete hangi sorumluluğun yükleneceğinin altı çizilmiştir. Akademi ve sektörler ile sağlanacak işbirliğinin nasıl gerçekleştirileceği de bu bölümde değerlendirilmiştir. Siber

olaylar, günümüz koşullarında birbirine bağımsız dijital ekonomi ve toplumun olduğu dünyada sınırlarda durdurulamaz. Strateji belgesinde tüm aktörlerin, AB seviyesinde ve ötesinde hem ulusal hem küresel alanda birlikte çalışmak ve birlikte sorumluluk almak zorunda olduğu belirtilmektedir. AB içinde birçok farklı aktörün rollerinin ve sorumluluklarının belirlenmesi gerektiği ve bu rollerin ve sorumlulukların nasıl olacağı strateji belgesinin önemli unsurlarından biri olarak karşımıza çıkmaktadır. (Avrupa Komisyonu, 2013b: 17)

Strateji belgesine göre, konunun karmaşıklığı ve ilgili aktörlerin çeşitliliği göz önüne alındığında merkezi Avrupa denetimi söz konusu olamamaktadır. (Avrupa Komisyonu, 2013b: 17) Belgede, ulusal hükümetlerin özel sektörlerle, siber olaylara ve saldırılara karşı birlikte hareket etmek durumunda olduğu vurgulanmıştır. (Avrupa Komisyonu, 2013b: 17) Aynı zamanda, risklerin potansiyel veya gerçek sınır tanımayan doğası nedeniyle, etkili bir ulusal tepkinin de genellikle AB düzeyinde katılım ile mümkün olacağı belirtilmektedir. Kapsamlı ve etkin bir siber güvenlik politikası için ağ ve bilgi güvenliği makamları, kolluk ile savunma mekanizmasının koordinasyonu ve işbirliği büyük önem arz etmektedir. Bu üç temel ayak ve bunlar arasındaki ilişki, strateji belgesinde Şekil 13'te olduğu gibi belirtilmiştir. Nitekim iletişim ve etkileşim kadar işbirliğinin de önemi vurgulanmaktadır. (Avrupa Komisyonu, 2013b: 17) Şekil 13'ü esas alarak bu iletişim, etkileşim ve işbirliğini irdelemek faydalı olacaktır. İzleyen alt bölüm strateji belgesinde oldugu gibi, bu şemanın açıklanmasına ayrılmıştır.



Şekil 14 Yetkili NIS Makamları/CERTs, Kolluk ve Savunma Arasındaki Koordinasyon

Kaynak: (Avrupa Komisyonu, 2013b: 17)

3.2.4.1. NIS Yetkilileri, Kolluk ve Savunma Arasındaki Koordinasyon

Ağ ve bilgi güvenliği yetkilileri, kolluk ve savunma arasındaki koordinasyon strateji belgesinde ulusal, AB ve uluslararası düzey olmak üzere üç farklı bağlamda değerlendirilmiştir. Ulusal düzeyde, üye devletlerin siber olaylarla mücadele etmesi için, yeteneğini istenilen seviyeye ulaştırması gerektiği belirtilmiştir. Üye devletlerin kendi ulusal siber güvenlik stratejilerini, ulusal kuruluşların görev ve sorumluluklarını ortaya koyması gerektiğine vurgu yapılmıştır. Üye devletlerin açıkça rollerinin ve sorumluluklarının farkında olarak hareket etmesi gerektiği ve ulusal sektörler ve özel sektörler arasında da bilgi paylaşımını sağlaması gerektiği ifade edilmiştir. (Avrupa Komisyonu, 2013b: 17)

Ulusal düzeyde olduğu gibi AB düzeyinde de siber güvenlik ile ilgili birçok aktör bulunmaktadır. ENISA, Europol/EC3 ve EDA gibi üç kolluk ve savunma ajansı bulunan bir birlik olarak AB'de bu kurumlar yönetim kuruluna sahiptir ve AB düzeyinde çeşitli platformlarda temsil edilmektedirler. Bunlar arasında gerçekleşecek koordinasyon ve iş birliği ile siber güvenlik konusunda pratik çözümler üretilmesinin mümkün olacağı belirtilmektedir (Avrupa Birliği Konseyi, 2015b). Europol/EC3'ün Program Yönetim Kurulu kapsamında teknik ve politika uzmanlarından oluşan Eurojust, CEPOL, üye devletler, ENISA ve Komisyon tek çatı altında toplanarak iş birliği zemini genişletilerek uygulanmaya çalışılmaktadır (Europol, 2016b). Bu kapsamda Europol'ün üye devletlerin yetkili NIS makamları ile gerçekleştireceği işbirliği ile de koordinasyon ve etkililik çalışmalarına önem verildiği belirtilmektedir (Europol, 2016c).

Uluslararası düzeyde ise Komisyonun ve Yüksek temsilcinin üye devletlerle birlikte siber güvenlik konusunda uyumlu çalışmasına vurgu yapılmıştır. Yine güvenlik-özgürlük ilişkisini göz önünde bulundurarak, Komisyonun ve Yüksek Temsilcinin bunu yaparken AB'nin temel değerleri ile çatışan bir şey yapmaması gerektiğinin altı çizilmiştir. Ayrıca Avrupa Konseyi, OECD, OSCE, NATO, BM gibi uluslararası kuruluşlarla da işbirliği ve koordineli bir şekilde hareket etmesi gerekliliği de öne çıkan bir ayrıntı olarak karşımıza çıkmaktadır. (Avrupa Komisyonu, 2013b: 18)

3.2.4.2. Büyük Bir Siber Olay ya da Saldırı Durumunda AB Desteği

Strateji belgesi, siber saldiri durumunda yapilacak mudahalenin de ana hatlarini cizmistir. Buna göre ENISA, Siber olay ve siber saldırı durumunda aktif rol oynanayacak ve Europol ile endüstri paydaşları arasındaki bilgi ağını ve AB kurumları ile üye devletlerin kolluk kuvvetleri arasındaki işbirliğinin güçlendirilmesini sağlayacaktır (Avrupa Komisyonu, 2013b: 18). İş sürekliliğini ciddi manada etkileyecek önemli siber olaylar karşısında gerek AB çapında gerekse uyedevletler özelinde gerekli desteğin verileceği belirtilmiştir. Bu kapsamda, uygulama bazinda yeni bir duzenleme ile bir olay gerçekleşmesi durumunda olaydan etkilenen üye devletlerin kolluk kuvvetleri ile birlikte Europol/EC3'ün failleri tespit etmek ve olayları açıklığa kavuşturmak için her zaman işbirliği içinde olacağı belirtilmiştir (Europol, 2016d).

Stratejide ayrıca, siber casusluk ya da devlet destekli bir saldırı olması durumunda da birlik üyesi devletler ile dayanışma içinde olunarak, gerek kriz yönetimi gerekse sorumluların tespiti konusunda AB tarafından gereken tüm desteğin verileceği belirtilmiştir.[47] Ulusal güvenlik uygulamaları kapsamında da üye devletlere erken uyarı sistemi mekanizması için bilgilendirme yapılacağı ifade edilmiştir. (Avrupa Komisyonu, 2013b: 19) Gerçekleşen siber olay ya da saldırı kişisel verilerin gizliliğinin ihlalini içeren bir durumu içeriyorsa bu durumda da kişisel verilerin işlenmesi ve elektronik haberleşme sektöründe gizliliğin korunması ile ilgili 2002/58/EC (Gizlilik ve Elektronik Haberleşme Direktifi) sayılı direktif (Avrupa Birliği, 2002) kapsamına ulusal veri koruma otoritelerinin dahil edileceği belirtilmiştir. Strateji belgesinin paydaşlara yüklemiş olduğu bu sorumlulukların, güvenlikleştirme sürecinde tehditin tanımlanıp, alımlayıcı kitleye acil önlem alınması gerekli bir konu olduğunun kabul ettirilmesinden sonraki safhada yer alan önlemlerden olduğu söylenebilir. Nitekim gerek AB düzeyinde gerekse üye devletler nezdinde üstlenilen roller hayati öneme sahip unsurların savunmasında kullanılacak yöntemlere ve süreçlere tekabül etmektedir. Kolluk kuvvetleri düzeyinde değerlendirilen bir konu olması konunun ehemmiyetini otaya çıkarmaktadır. Bu açıdan da roller ve sorumluluklar güvenlikleştirmenin beka (survival) perspektifinden değerlendirilebilir.

[47] Buradaki desteğin Avrupa Birliği'nin İşleyişine İlişkin Antlaşma (Lizbon Anlaşması) Madde 222'de belirtilen dayanışma ilkesi kapsamında gerçekleştirileceği vurgulanmaktadır. (Avrupa Birliği, 2007)

3.3. SONUÇ

Bu bölümde, ilk olarak strateji belgesine kadar geçen süreçte AB içinde siber güvenliğin sağlanmasına yönelik atılan adımlar incelenmiş, devamında ise AB'nin siber güvenlik stratejisi ve politikaları detaylı olarak irdelenmiştir. Strateji belgesi esas alınarak verilen bilgiler çerçevesinde oluşturulacak politikalar için AB'nin belirlemiş olduğu siber güvenlik ilkeleri, stratejik öncelikleri ve eylemleri, AB kurumları ile üye devletlere yüklenen roller ve sorumluluklar detaylı olarak incelenmiştir. Güvenlikleştirmenin temel taşı olarak düşünülebilecek bir belge olması açısından, strateji belgesinin güvenlikleştirmenin tüm safhalarını kapsadığı söylenebilir. Satır aralarında dikkat çekilen hususlar ile birlikte hangi olayların hangi sektörlere dahil edilebileceği detaylandırılmıştır. Bu bağlamda AB'nin strateji belgesini güvenlikleştirmenin temel taşı olarak düşünebiliriz. Hem güvenlikleştirme sürecinin açıklanmasındaki süreçleri ihtiva eden resmi bir belge olarak, hem de farklı güvenlik sektörlerine atıf yapması sebebiyle strateji belgesi, bu tezin teorik çerçevesi içinde kolaylıkla incelenebilmiştir.

Komisyon ile Birlik Dışişleri ve Güvenlik Politikası Yüksek Temsilcisi tarafından öne sürülen ve AB düzeyinde önemli eylem planları içeren siber güvenlik stratejisi, vatandaşların haklarının korunması ve teşvik edilmesine dayanan AB'nin vizyon ve gerekli eylemleri ile AB'nin siber uzayın kendine ait olan alanın güvenli bir alan olmasını sağlamak istediğini göstermektedir. Bu vizyonun sadece, zorlukları karşılamak için sorumluluk alan bir çok aktör arasında gerçek bir ortaklık aracılığıyla gerçekleştirilebileceği vurgulanmaktadır. Komisyon ve Yüksek Temsilci bu nedenle Konseyi ve Avrupa Parlamentosunu siber güvenliğin sağlanması için çalışmalar yaparak taslak eylem planları sunma konusunda teşvik etmektedir. Güçlü destek ve bağlılığın da AB'nin güvenlik seviyesini geliştirmek ve vatandaşların haklarını korumak için gerekli olduğu belirtilmektedir.

Strateji belgesi, AB kurumlarına ve üye devletlere sorumuluklar yükleyen resmi bir doküman olması açısından mevcut politikalara uygulanabilirliğinin sağlanmasında önemli etkiye sahiptir. Ancak sadece resmi olarak bir strateji belgesinin varlığı bizi bu belgede yazan her olgunun ve durumun eksiksiz olarak uygulandığına götürmemektedir. Bu açıdan, tamamlanan uygulamalar temelinde strateji belgesi siber güvenliğin sağlanması için takdire şayan bir başlangıç olarak değerlendirilebilir. Ancak, dünya

gündemindeki değişmelere paralel olarak AB gündemi de farklı alanlara yoğunlaşabilmektedir. Örneğin, Suriye'deki iç savaş ile başlayan süreçte gün yüzüne çıkan göçmen krizi gibi küresel olaylar ile Birliğin gündemi farklı alanlarda yoğunlaşabilmektedir. Bu bağlamda önceliğin farklı alanlara verilmesi sonucunda strateji belgesinin uygulanmasına yönelik politika ve eylemlerin oluşturulmasında gecikmeler yaşanabilmektedir. Bu sebeple strateji belgesi uygulanabilirlik boyutu ile eleştiriye açık bir belge olarak karşımıza çıkmaktadır.

Strateji belgesinin uygulama süreci geliştirilmeye ve iyileştirmelere açık ve dinamik bir süreç olarak değerlendirilebilir. Bu süreçte karşılaşılabilecek yeni tehditler bu belgeye konu edilerek, ilerleyen süreçlerde bunlara yönelik olarak alınabilecek önlemler de raporlarla desteklenebilir. Özellikle üye devletlerle koordineli bir şekilde işletilen süreçlerin varlığı belgenin geçerliliğini ve uygulanabilirliğini önemli ölçüde etkileyebilmektedir. Nitekim AB üyesi her devletin sahip olduğu teknoloji kapasitesi ve gelişmişlik seviyesi farklılık gösterebilmektedir. Strateji belgesinin ve AB'nin siber güvenlik politikalarının etkililiği ve yeterliliği hakkında detaylı yorumlar son bölümde yapılmıştır.

SONUÇ

Ağ ve bilgi teknolojilerinin gelişiminin sürekli arttığı, yeni teknolojilerin üretildiği günümüzde revaçta olan bir kavram olarak siber uzay; bu alandaki hakimiyet mücadelelerini ve riskleri de beraberinde getirmektedir. Düşük maliyetlerle büyük çapta hem maddi hem manevi hasarlara yol açabilen siber saldırılar mümkün olabilmektedir. Bu çalışmada siber uzayda karşılaşılan tehditlerin AB tarafından nasıl değerlendirileceğine dair kavramsal bir çerçeve sunulmuş ve devamında AB'nin bu alandaki güvenliği sağlamak için geliştirdiği politikalar değerlendirilmiştir.

Güvenlikleştirme teorisi kapsamında kuramsal zemine oturtulan siber güvenlik olgusu; nedenleri, etkileri ve sonuçları itibariyle teorinin analiz kapsamında bize sunduğu sektörlerin bir çoğunu içinde barındıran karma bir sektör olarak karşımıza çıkmaktadır. Meydana gelen siber olaylar neticesinde ekonomik zararın ortaya çıkması ve yeni yatırım alanlarını gündeme getirmesiyle ekonomik sektörün bir çıktısı olarak değerlendirilebilecek olan siber güvenlik, ayrıca çevre ile ilgili kritik bilgi altyapı hizmetlerine yapılabilecek siber saldırılar sonucu devredışı kalacak olan hizmetler sonrasında çevreyi de olumsuz etkileyen bir unsur olarak kendine çevresel güvenlik sektöründe de yer edinebilmektedir. Kopenhag Ekolünün eleştirel kanadını oluşturan Hansen ve Nissenbaum'a göre, farklı bir sektör olarak değerlendirilen bir alan olarak siber güvenlik, söz ediminden, olağanüstü tedbirlerin alınmasına kadar tüm güvenlikleştirme süreçlerini içermektedir. Hemen hemen güvenlikleştirme kapsamında değerlendirilebilecek bütün sektörleri içeren bir alan olması sebebiyle kuramsal temellendirme için güvenlikleştirme seçilmiştir. Gerek tehdidin oluşturulması sürecinde gerekse AB'nin politika yapım sürecinde etkili olan AB aktörleri çerçevesinde en uygun kuramsal zemin olarak bu yaklaşımın seçilmesinde süreçler, roller ve sorumluluklar önemli birer etken olmuştur.

AB'nin siber güvenlik politikasının oluşturulmasında uluslararası siber saldırı örneklerinin büyük etkisi olmuştur. Nitekim sınırı olmayan bir alanda gerçekleştirilebilecek her eylem her topluluğu, her devleti etkileyebilme kapasitesine sahiptir. Oltalama, kötücül yazılım, botnet, hizmeti engelleme, sosyal mühendislik gibi siber saldırı teknikleri sonucu çeşitli siber saldırılara maruz kalabilmektedir. Bu

kapsamda etkin bir erken uyarı sistemi ve gerçekleşen siber saldırılara karşı savunma sistemi oluşturulması AB için de önemli öncelikler olarak değerlendirilmiştir.

AB'nin siber güvenlik politikasının temelini oluşturan "Avrupa Birliği için Siber Güvenlik Stratejisi" belgesi ile Birliğin ortak siber güvenlik politikası kapsamında gerçekleştireceği temel politikalar ve yol haritaları belirlenmiştir. Ayrıca gerek AB kurumlarının sorumlulukları, gerekse üye devletlerin ulusal makamlarının üstleneceği roller bu strateji belgesi ile genel bir çerçeveye oturtulmuştur. AB, bu bağlamda, akademi, kamu ve özel sektör işbirliğine büyük önem atfetmektedir. Siber güvenlik stratejisi de etkin ve kararlı bir siber güvenlik politikasının AB kurumları, üye devletlerin yetkili politika yapım mercileri ve ortak paydada buluşulmuş uluslararası ortaklıklar ile sağlanabilecek koordinasyon sayesinde sağlanabileceği vurgulanmıştır.

Buraya kadar anlatılanlardan şunu çıkarmamız yerinde olacaktır; AB siber güvenlik politikaları tüm dünyada göze çarpan ve örnek politika olabilecek kategoride unsurları içermektedir. Bu unsurlar strateji belgesi üzerinde net bir şekilde görülebilmektedir. Siber güvenliğin ilkelerinin kapsamlı bir şekilde tanımlandığı görülmektedir. Uygulamada ise bu ilkelerin sürekli olarak birlikte sağlanması mümkün görünmemektedir. Tespit edilen ve önlenen her siber olaydan sonra farklı şekillerde yeni siber olaylar meydana gelebilmektedir. Tespit edip önleme mekanizmasının yanısıra siber olayların oluşmadan önce önlenmesinin hedef edilmesi gerekmektedir. Siber olayların meydana gelmeden önleyici sistemlerle siber güvenliğin sağlanması etkili ve kalıcı siber güvenlik politikalarının ip ucunu oluşturmaktadır. Bu açıdan AB, oluşturulan müdahele ekipleri ile AB düzeyinde gerçekleşen siber olaylara müdahale edebilme yeteneğini geliştirmiştir. Bununla siber direnci bir ölçüde başarabilmiştir. Ancak halen kalıcı ve sürdürülebilir önleyici bir kontrol mekanizmasının olduğunu söylemek mümkün değildir.

Siber suçları büyük ölçüde azaltmak için AB'nin strateji belgesinde öne çıkardığı güçlü ve etkili yasamanın uygulamada da çok mümkün olmadığı görülmektedir. Bunun en önemli örneği şudur: Komisyonun 2013 yılında hazırladığı ve siber güvenlik politikalarının temel dokümanlarından olan ağ ve bilgi güvenliğine ilişkin taslak metin (Avrupa Komisyonu, 2013a) ancak 2016 (Avrupa Komisyonu, 2016d) yılında direktif haline gelebilmiştir. Yasamanın bu kadar geç işlemesindeki önemli sorunlar; üye devletlerin iç hukuk sistemlerine uyumun zaman alması, Birlik gündeminin siber güvenlik dışındaki olaylarda yoğunlaşması, üye devletlerin tutumları olarak sıralanabilir.

Siber suç ile mücadelede operasyonel yeteneği geliştirmek için AB düzeyinde atılan adımlar da yeterli olamamaktadır. Bu amaçla kurulan Avrupa Siber Suç Merkezi etkili olamamaktadır. Gerek üye devletlerin bilgi paylaşımındaki yetersizliği ve konuya gereken hassasiyeti göstermemesi, üye devletlerin teknoloji kapasitelerinin farklılık göstermesi bu merkezin sağlıklı olarak veri akışını sağlayan bir kurum olmaktan uzaklaştırmaktadır.

AB düzeyinde koordinasyonun geliştirilmesini de siber suçları büyük ölçüde azaltmak için önemli bir görev olarak gören AB, bu koordinasyonda üye devletler, Akademi ve AB kurumlarına sorumluluklar yüklemektedir. Ancak bunun için kurumsal bir zeminin olmayışı bu alandaki yetersizliği de beraberinde getirmektedir.

Ortak Güvenlik ve Savunma Politikası kapsamında politikalardaki mükerrerliğin önlenmesi amacıyla hem AB hem de NATO üyesi ülkelerdeki üyelerin politikaları uyumlaştırılmaya çalışılmıştır. Bu kapsamda da Yüksek Temsilciye NATO ile diyalogun geliştirilmesi görevi verilmiştir. Ancak Yüksek Temsilcinin bu görevi için adım atmadığı görülmektedir. Bunun sebebi ise siber güvenlikten daha hayati önem taşıyan göçmen sorunu gibi sorunların öncelikli gündem olarak değerlendirilmesidir.

AB siber olayların güvenlikleştirilmesinde siber güvenlik için endüstriyel ve teknolojik kaynakları geliştirmeyi hedeflemiştir. Bununla birlikte Ar-Ge çalışmalarının bu alanda yoğunlaştırmayı da strateji belgesinde özel olarak değerlendirmiştir. Siber güvenlik ürünleri için tek pazarın oluşturulması için ilk adımlar “Dijital Tek Pazar” ile 2015 yılında atılabilmiştir. AR-Ge çalışmaları için Horizon 2020 kapsamında bilgi ve iletişim teknolojileri ürünlerinin geliştirilmesi de 80 milyar Euro bütçeye sahip bu çerçeve program dahilinde değerlendirilmiştir. Avrupa standardizayson kuruluşları ile iş birliği geliştirilerek yenilikçiliği teşvik amaçlanmıştır. Güvenlikleştirmede esas olan tehditin kabul ettirilmesinden sonraki aşamada önlemlerin ivedi olarak alınmasıdır. AB’deki tek pazarın oluşması için Birlik düzeyinde uygulamaya başlamada durum ise strateji belgesi oluştuktan yaklaşık üç yıl sonrasında başlayabilmiştir.

Siber güvenlik stratejisinde AB için tutarlı bir uluslararası siber güvenlik politikasının oluşturulması ve AB temel değerlerinin teşvik edilmesi hedeflenmiştir. Bunun için de siber güvenliği AB dış ilişkilerine entegre ederek OGSP kapsamında değerlendirmeyi amaçlamıştır. Ayrıca üçüncü ülkeler ile de siber güvenlik ve kritik bilgi

altyapı alanlarında iş birliği geliştirmeyi hedeflemişlerdir. 23 Haziran 2016'da Birleşik Krallık'ta gerçekleştirilen "Brexit"[48] referandumundan Birleşik Krallık'ın AB'den ayrılması yönünde sonuç çıkması üzerine AB temel değerlerinin de sorgulanmasına ve yeniden değerlendirilmesi gündeme gelmiştir. Bu bakımdan stratejide belirtilen temel değerlerin teşvik edilmesi amacı sekteye uğramıştır. Üçüncü ülkeler ile de kalıcı anlamda siber güvenlik alanında ilişkiler geliştirilememiştir. İsviçre, İzlanda ve Norveç ile ENISA çatısı altında ortak politikalar geliştirilebilmektedir ancak diğer ülkeler ile belirgin bir işbirliği yoktur.

Stratejinin son bölümünde belirtilen Roller ve Sorumluluklar ile ağ ve bilgi güvenliği siyasetinin etkin bir şekilde tesis edilebilmesi için AB kurumları, Üye devletler, Akademi ve sektörler arasındaki görev paylaşımları ve bunların nasıl gerçekleştirileceği açıklanmıştır. AB'de stratejide belirtildiği şekilde üye devletten başlayan ve AB düzeyinde devam eden hiyerarşik bir yapılanma henüz tam olarak oluşturulamamıştır. Üye devletlerin kolluk kuvvetleri ile AB nezdindeki kolluk kuvvetleri arasındaki bilgi akışı sürekli ve hızlı bir şekilde sağlanamamaktadır. Bunun önemli bir sebebi üye devletlerin kolluk kuvvetlerinin ve yetkili NIS makamlarının aynı bilgi ve teknolojiye sahip olmamasından kaynaklanmaktadır. Bu açıdan roller ve sorumluluklar strateji belgesinde belirtildiği şekilde hiyerarşik ve sıralı şekilde ilerleyememektedir.

Yukarıda belirtilen sebeplerden dolayı AB'nin müşterek anlamda, siber güvenlik strateji belgesinde belirtilen politikaların tamamını henüz uygulamaya koyamadığı görülmektedir. AB düzeyinde ve uluslararası düzeyde, koordinasyon ve iş birliği geliştirilerek uygulamalar istikrarlı bir şekilde varlığını sürdürebilir. Strateji belgesi bu bağlamda rehber bir belge olarak örnek olabilecek nitelikte olmasına rağmen uygulamada tam olarak karşılığınıı bulamamıştır. Dünyadaki tüm ülkelerin bu politikalardan yola çıkarak kendi siber güvenlik politikalarını oluşturması beklenebilir. Fakat doğru olan, oluşturulan stratejiyi işleyerek, eklemeler çıkarmalar yaparak, onu daha de geliştirmek ve kendi ülkeleri için bunları uygulanabilir düzeye çıkarmaktır.

Sonuç olarak, siber güvenlik konusunun çok önem verilmesi ve yatırım yapılması gereken bir alan olduğunu söylemek yerinde olacaktır. Bu sektöre yapılacak yatırımların amacı ileride oluşabilecek her türlü siber saldırıyı engelleyerek, önceden sistemlerin

[48] Birleşik Krallık'ın Avrupa'dan çıkmasına, "Britanya" ve "exit" kelimeleri birleştirilerek oluşturulmuş olan kelimeye "Brexit" denilmektedir.

tehditlere hazır olması ve gelecek siber saldırıları da bertaraf etmeye olanak sağlaması olmalıdır. Nasıl ki bir depremin önceden olacağını bilemiyorsak, burada da yani yapılacak herhangi bir siber saldırı sonrasında, eğer önlemini almışsak, sistem ve bilgilerimiz bu sayede korunmuş olacak ve herhangi bir veri kaybı yaşamadan maddi hasara yol açılmadan tehlike ve saldırılar bertaraf edilebilecektir. AB'nin de strateji belgesinde öne çıkardığı bu uygulamaları hayata geçirererek siber uzayda daha güvenli bir ortamı vatandaşlarına sunabileceğini söyleyebiliriz.

KAYNAKÇA

Açıkmeşe, S. A. (2008). Kopenhag Okulu Realist Güvenlik Çalışmalarında Aktör, Tehdit ve Politika: Avrupa Güvenliği Üzerine Bir Değerlendirme. Ankara: Yayımlanmamış Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Avrupa Birliği ve Uluslararası Ekonomik İlişkiler Anabilimdalı.

Ahi, M. (2011). *Anonymous ve Siber Ataklara Hukuksal bir Yaklaşım*. Bilişimhukuk, 19 Haziran 2011: http://www.bilisimhukuk.com/2011/06/anonymous-ve-siber-ataklara-hukuksal-bir-yaklasim/ adresinden alındı

AlJazeera. (2015). *Charlie Hebdo Saldırısı: Bilinenler, Bilinmeyenler*. Al Jazeera, 8 Ocak 2015: http://www.aljazeera.com.tr/haber/charlie-hebdo-saldirisi-bilinenler-bilinmeyenler adresinden alındı

Altınörs, A. (2003). *Dil Felsefesine Giriş.* İstanbul: İnkılap Kitabevi.

Amos, J. (2014). *Horizon 2020: UK Launch for EU's £67bn Research Budget*. BBC, 31 Ocak 2014: http://www.bbc.com/news/science-environment-25961243 adresinden alındı

Andress, J. ve Winterfeld, S. (2011). *Cyber Warfare Techniques, Tactics and Tools for Security Practitioners.* Londra: Elsevier.

APWG. (2015). *Phishing Activity Trends Report, 4th Quarter 2014.* https://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf adresinden alındı

Aras, B. ve Polat, R. K. (2008). From Conflict to Cooperation: Desecuritization of Turkey's Relations with Syria and Iran. *Security Dialogue, 39*(5), 495-515.

Arı, T. (2013a). *Uluslararası İlişkiler Teorileri : Çatışma, Hegemonya, İşbirliği (8. Baskı).* Bursa: MKM Yayınları.

Arı, T. (2013b). *Uluslararası İlişkiler ve Dış Politika (10. Baskı).* Bursa: MKM Yayınları.

Arı, T. (der.) (2014). *Uluslararası İlişkilerde Postmodern Analizler 2: Uluslararası İlişkilerde Eleştirel Yaklaşımlar.* Bursa: Dora.

Austin, J. L. (1975). *How to Do Things with Words (ed. James Opie Urmson).* Massachusetts: Harvard University Press.

Avrupa Birliği (1995). The Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. *Official Journal of the European Union, L*(281), 31-50.

Avrupa Birliği (2002). Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications). *Official Journal of the European Union, L*(201), 37-47.

Avrupa Birliği (2005). COUNCIL FRAMEWORK DECISION 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems. *Official Journal of the European Union, L*(69), 67-71.

Avrupa Birliği (2006). The Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC. *Official Journal of the European Union, L*(105), 54-63.

Avrupa Birliği (2007). *Consolidated version of the Treaty on the Functioning of the European Union.* Lizbon: Avrupa Birliği. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A12012E%2FTXT adresinden alındı

Avrupa Birliği (2011). Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography. *Official Journal of the European Union, 16*, 261-274. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:jl0064 adresinden alındı

Avrupa Birliği (2012). Regulation (EU) No 1025/2012. *Official Journal of the European Union*. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R1025 adresinden alındı

Avrupa Birliği (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union, OJL 194*, 1-30. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG adresinden alındı

Avrupa Birliği Dış İlişkiler, (2014). *Fact Sheet EU-US Cooperation on Cyber Security and Cyberspace*. Avrupa Birliği Dış İlişkiler, 26 Mart 2014: http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf adresinden alındı

Avrupa Birliği Konseyi (2015). *General Data Protection Regulation.* Brüksel: Avrupa Birliği Konseyi, 11 Haziran 2015: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf adresinden alındı

Avrupa Birliği Konseyi (2015a). *Data Protection: Council Agrees on a gGneral Approach*. Avrupa Birliği Konseyi, 15 Haziran 2015: http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/ adresinden alındı

Avrupa Birliği Konseyi (2015b). *EU Cybersecurity Strategy: Road Map Development.* Brüksel: Avrupa Birliği Konseyi. http://www.statewatch.org/news/2015/apr/eu-council-cyber-security-roadmap-6183-rev1-15.pdf adresinden alındı

Avrupa Birliği Konseyi (2015c). *Improving Cyber Security Across the EU.* European Council, 18 Aralık 2015: http://www.consilium.europa.eu/en/policies/cyber-security/ adresinden alındı

Avrupa Komisyonu (2001a). *The Repercussions of the Terrorist Attacks in the United States on the Air Transport Industry.* Brüksel: Avrupa Komisyonu. http://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-574-EN-F1-1.Pdf adresinden alındı

Avrupa Komisyonu (2001b). *Network and Information Security: Proposal for A European Policy Approach.* Brüksel: Avrupa Komisyonu. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298 adresinden alındı

Avrupa Komisyonu (2004). *Gree Critical Infrastructure Protection in the fight against terrorism [COM(2004) 702 final.* Avrupa Komisyonu, 20 Ekim 2004: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33259 adresinden alındı

Avrupa Komisyonu (2005). *Green Paper on a European programme for critical infrastructure protection.* Avrupa Komisyonu, 17 Kasım 2005: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52005DC0576 adresinden alındı

Avrupa Komisyonu (2006). *A Strategy for a Secure Information Society: "Dialogue, Partnership and Empowerment"*. Brüksel: Avrupa Komisyonu. http://ec.europa.eu/information_society/doc/com2006251.pdf adresinden alındı

Avrupa Komisyonu (2009a). *Communication from the Commission to the European Parliament and the Council.* Brüksel: Avrupa Komisyonu.

Avrupa Komisyonu (2009b). *Critical Information Infrastructure Protection.* Brüksel: Avrupa Komisyonu. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF adresinden alındı

Avrupa Komisyonu (2009c). *DIRECTIVE 2009/49/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 June 2009 amending Council Directives 78/660/EEC and 83/349/EEC as regards certain disclosure requirements for medium-sized companies and the obligation to draw up consolidated accou.* Brüksel: Avrupa Komisyonu. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:164:0042:0044:EN:PDF adresinden alındı

Avrupa Komisyonu (2009d). *Action Plan and a Communication on Critical Information Infrastructure Protection (CIIP).* Brüksel: Avrupa Komisyonu. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF adresinden alındı

Avrupa Komisyonu (2010a). *Commission Suggests Tougher Measures against Cyber Attacks*. Avrupa Komisyonu, 30 Eylül 2010: http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2010/20100930_en.htm adresinden alındı

Avrupa Komisyonu (2010b). *Concerning the European Network and Information Security Agency (ENISA).* Brüksel: Avrupa Komisyonu. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF adresinden alındı

Avrupa Komisyonu (2010c). *EU-U.S. Summit 20 November 2010, Lisbon - Joint Statement.* 2010: Avrupa Komisyonu. http://europa.eu/rapid/press-release_MEMO-10-597_en.htm adresinden alındı

Avrupa Komisyonu (2010d). *EU-US Summit Joint statement*. Avrupa Komisyonu, 20 Kasım 2010: http://europa.eu/rapid/press-release_PRES-10-315_en.htm?locale=en adresinden alındı

Avrupa Komisyonu (2011a). *Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security.* Brüksel: Avrupa Komisyonu. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0163&from=EN adresinden alındı

Avrupa Komisyonu (2011b). *Smart Grid Mandate Standardization Mandate to European Standardisation Organisations (ESOs) to Support European Smart Grid Deployment.* Brüksel: Avrupa Komisyonu. https://ec.europa.eu/energy/sites/ener/files/documents/2011_03_01_mandate_m490_en.pdf adresinden alındı

Avrupa Komisyonu (2011c). *Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats*.

Avrupa Komisyonu, 14 Nisan 2011: http://europa.eu/rapid/press-release_MEMO-11-246_en.htm adresinden alındı

Avrupa Komisyonu (2011d). *A renewed EU strategy 2011-14 for Corporate Social Responsibility.* Brüksel: Avrupa Komisyonu. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0681:FIN:en:PDF adresinden alındı

Avrupa Komisyonu (2012). *European Strategy for a Better Internet for Children.* Brüksel: Avrupa Komisyonu. http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0196 adresinden alındı

Avrupa Komisyonu (2013a). *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM/2013/048 final - 2013/0027 (COD).* European Commission. Brüksel: Avrupa Komisyonu, 7 Şubat 2013: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN adresinden alındı

Avrupa Komisyonu (2013b). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Avrupa Komisyonu, 7 Şubat 2013: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667 adresinden alındı

Avrupa Komisyonu (2013c). *Policy on Critical Information Infrastructure Protection (CIIP).* 7: Şubat. https://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip adresinden alındı

Avrupa Komisyonu (2014). *Prevention of and Fight against Crime (ISEC).* Brüksel: Avrupa Komisyonu. http://ec.europa.eu/dgs/home-affairs/financing/fundings/security-and-safeguarding-liberties/prevention-of-and-fight-against-crime/index_en.htm adresinden alındı

Avrupa Komisyonu (2015a). *Connecting Europe Facility*. Avrupa Komisyonu, 4 Kasım 2015: https://ec.europa.eu/digital-agenda/en/connecting-europe-facility adresinden alındı

Avrupa Komisyonu (2015b). *Horizon 2020 The EU Framework Programme for Research and Innovation*. Avrupa Komisyonu, 15 Aralık 2015: https://ec.europa.eu/programmes/horizon2020/ adresinden alındı

Avrupa Komisyonu (2016a). *Digital Single Market*. Avrupa Komisyonu, 22 Ocak 2016: https://ec.europa.eu/digital-agenda/en/digital-single-market adresinden alındı

Avrupa Komisyonu (2016b). *ICT Policy Support Programme as part of the Competitiveness and Innovation framework Programme (CIP)*. Avrupa Komisyonu, 3 Ocak 2016: http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm adresinden alındı

Avrupa Komisyonu (2016c). *Critical Infrastructure Warning Information Network (CIWIN).* Avrupa Komisyonu, 3 Haziran 2016: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm adresinden alındı

Avrupa Komisyonu (2016d). *Direective (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* Avrupa Komisyonu, 6 Temmuz 2016: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC adresinden alındı

Avrupa Konseyi (2001). *Convention on Cybercrime (European Treaty Series - No. 185).* Budapeşte: Avrupa Konseyi. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf adresinden alındı

Avrupa Parlamentosu (2012). *Critical information infrastructure protection: towards global cyber-security.* Strazburg: Avrupa Parlamentosu. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167 adresinden alındı

Avrupa Politika Merkezi. (2010). *The Economic Impact of a European Digital Single Market.* Brüksel: Avrupa Politika Merkezi - EPC. http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf adresinden alındı

Avusturya Cumhuriyeti Federal Başbakanlık (2013). *Austrian Cyber Security Strategy.* Viyana: Avusturya Cumhuriyeti Federal Başbakanlık. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AT_NCSS.pdf adresinden alındı

Baldwin, D. (1995). Security Studies and the End of the Cold War. *World Politics, 48*(1), 117-141.

Balta, E. (2014). *Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler.* İstanbul: İletişim.

Balzacq, T. (2005). The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations, 11*(2), 171-201.

Başbakanlık (2013). *The National Security Strategy.* Madrid: Başbakanlık. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_ESen.pdf adresinden alındı

Başbakanlık (2015). *French National Digital Security Strategy.* Paris: Başbakanlık. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf adresinden alındı

BBC. (2007a). *UN's website breached by hackers*. BBC News, 12 Ağustos 2007: http://news.bbc.co.uk/2/hi/technology/6943385.stm adresinden alındı

BBC. (2007b). *Estonia hit by 'Moscow cyber war'*. BBC News, 17 Mayıs 2007: http://news.bbc.co.uk/2/hi/europe/6665145.stm adresinden alındı

BBC. (2015a). *Ukraine Blames Russia for German Hack.* BBC News, 8 Ocak 2015: http://www.bbc.com/news/technology-30724168 adresinden alındı

BBC. (2015b). *German Parliement Cyber-attack Still 'live'*. BBC News, 11 Haziran 2015: http://www.bbc.com/news/technology-33093895 adresinden alındı

BBC. (2015c). *Charlie Hebdo Attack: Three Days of Terror*. BBC News, 14 Ocak 2015: http://www.bbc.com/news/world-europe-30708237 adresinden alındı

BBC. (2016). *Russia 'was behind German Parliement Attack'*. BBC News, 13 Mayıs 2016: http://www.bbc.com/news/technology-36284447 adresinden alındı

Bloomfield, A. (2007). *Estonia calls for Nato cyber-terrorism strategy*. The Telegraph, 18 Mayıs 2007: http://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html adresinden alındı

Bölinger, M. (2016). *Was Russia behind 2015's cyber attack on the German Parliament?*. Deutche Welle, 2 Şubat 2016: http://www.dw.com/en/was-russia-behind-2015s-cyber-attack-on-the-german-parliament/a-19017553 adresinden alındı

Bıçakçı, S. (2013). *21. Yüzyılda Siber Güvenlik (Ed. Mustafa Aydın).* İstanbul: Bilgi Üniversitesi Yayınları.

Bican, C. (2008). *Sosyal Mühendislik Saldırıları*. TÜBİTAK BİLGEM, 20 Mayıs 2008: http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari-3.html adresinden alındı

BİLGEM. (2015). *Tehditler ve Korunma Yöntemleri: Sosyal Mühendislik*. TÜBİTAK BİLGEM, 4 Aralık 2015: http://www.bilgimikoruyorum.org.tr/?b324_yasanmis_sosyal_muhendislik_ornekleri adresinden alındı

Birleşmiş Milletler. (2016). *Cyberspace*. UNTERMS, 12 Haziran 2016: https://unterm.un.org/UNTERM/display/Record/UNHQ/NA/c328692 adresinden alındı

Bisson, J. ve Saint-Germain, R. (2005). *Implementation of Security Policies Based on the BS7799 / ISO 17799 Standard For a better approach to information security.* ISO.

Bölükbaş, C. (2014). *Yeni Nesil Teknolojik Silahlar: DoS/DDoS*. Siberbülten, 22 Aralık 2014: https://siberbulten.com/makale-analiz/yeni-nesil-teknolojik-silahlar-dosddos/ adresinden alındı

Buzan, B. (1983). *People, States, and Fear: The National Security Problem in International Relations.* Brighton: Harvester Wheatsheaf.

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

Buzan, B. (1997). Rethinking Security after the Cold War. *Cooperation and Conflict, 32*(1), 5-28.

Buzan, B. ve Wæver, O. (2003). *Regions and Powers: The Structure of International Security.* Cambridge: Cambridge University Press.

Buzan, B. (2004). *The United States and the Great Powers.* Cambridge: Polity.

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.

Carr, J. ve Shepherd, L. (2010). *Inside Cyber Warfare.* Sebastopol: O'reilly Media.

CEPOL. (2016). *European Police College An Agency of the European Union*. CEPOL, 3 Ocak 2016: https://www.cepol.europa.eu/who-we-are/european-police-college/about-us adresinden alındı

CERT. (2015). *CERT-EU*. CERT-EU, 25 Aralık 2015: https://cert.europa.eu/cert/plainedition/en/cert_about.html adresinden alındı

Christensson, P. (2016). *Malware Definition*. TechTerms, 5 Ocak 2016: http://techterms.com/definition/malware adresinden alındı

Chen, P. Desment, L. ve Huygens, C. (2014). *A Study on Advanced Persistent Threats.* Communications and Multimedia Security, 63-72.

CISCO. (2013). *A Cisco Guide to Defending Against Distributed Denial of Service Attacks.* Cisco Security Intelligence Operations, 25 Aralık 2014 tarihinde http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html adresinden alındı

CMR. (2012). *Cyber Security Strategy: Securing Cyberspace.* Belçika: CMR. https://www.b-ccentre.be/wp-content/uploads/2013/03/cybersecustra_fr.pdf adresinden alındı

Collins, K. (2014). *Anonymous and LulzSec targeted by GCHQ DDoS attacks*. Wired, 5 Şubat 2014: http://www.wired.co.uk/news/archive/2014-02/05/gchq-ddos-attack-anonymous adresinden alındı

Cumarsaide, R. (2015). *National Cyber Security Strategy: Securing our Digital Future.* Department of Communication, Energy and Natural Resources. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS_IE.pdf adresinden alındı

Çek Cumhuriyeti Milli Güvenlik Kurumu (2015). *National Cyber Security Strategy of the Czech Republic for the period from 2015-2020.* Prag: Çek Cumhuriyeti Milli Güvenlik Kurumu. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf adresinden alındı

Çelebi, V. (2014). Gündelik Dil Felsefesi ve Austin'in Söz Edimleri Kuramı, *Beytulhikme An International Journal of Philosophy, 4(1), 73-89.*

Çifci, H. (2013). *Her Yönüyle Siber Savaş.* Ankara: TÜBİTAK.

Çitlioğlu, E. (2008). *Gri Tehdit Terörizm.* Ankara: Destek Yayınları.

Danimarka Siber Güvenlik Merkezi (2015). *The Danish Cyber and Information Security Strategy.* Danimarka: Siber Güvenlik Merkezi. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/DK_NCSS.pdf adresinden alındı

Dedeoğlu, B. (2003). *Uluslararası Güvenlik ve Strateji,.* İstanbul: Derin Yayınları.

Dülger, M. V. (2004). *Bilişim Suçları.* Ankara: Seçkin Yayıncılık.

Easttom, C. ve Taylor, J. (2011). *Computer Crime, Investigation, and the Law.* Boston: Course Technology.

Ekonomik İşler ve İletişim Bakanlığı (2014). *Cyber Security Strategy 2014-2017.* Estonya: Ekonomik İşler ve İletişim Bakanlığı. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf adresinden alındı

ENISA. (2010). *Cyber Europe 2010 – Evaluation Report.* Heraklion: ENISA. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010/ce2010report/at_download/fullReport adresinden alındı

ENISA. (2014). *Advanced Persistent Threat Incident Handling.* Heraklion: ENISA. https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/advanced_persistent_threat_incident_handling_toolset adresinden alındı

ENISA. (2015a). *Cyber Atlantic 2011*. ENISA, 25 Aralık 2015: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011 adresinden alındı

ENISA. (2015b). *Cyber Security Month*. Cyber Security Month, 25 Aralık 2015: https://cybersecuritymonth.eu/ adresinden alındı

ENISA. (2016a). *About ENISA*, ENISA, 9 Haziran 2016: https://www.enisa.europa.eu/about-enisa adresinden alındı

ENISA. (2016b). *Topics*, ENISA, 9 Haziran 2016: https://www.enisa.europa.eu/topics adresinden alındı

ENISA. (2016c). *National Cyber Security Strategies in the World*. ENISA, 9 Ocak 2016: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-

cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world adresinden alındı

Eurobarometer. (2012). *Special Eurobarometer 390 Cyber Security.* Brüksel: European Commission. http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf adresinden alındı

Europol (2015). Conference on Cyber-related Research & Development. Hague: Europol. https://www.europol.europa.eu/latest_news/upcoming-event-conference-cyber-related-research-development adresinden alındı

Europol (2016a). *Th European Cybercrime Centre (EC3)*. Europol, 2 Ocak 2016: https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837 adresinden alındı

Europol (2016b). *EC3 Programme Board*. Europol, 3 Ocak 2016: https://www.europol.europa.eu/ec/ec3-board adresinden alındı

Europol (2016c). *Joint Cybercrime Action Taskforce (J-CAT).* Europol, 3 Ocak 2016: https://www.europol.europa.eu/ec3/joint-cybercrime-action-taskforce-j-cat adresinden alındı

Europol (2016d). *Cyber Operations*. Europol, 3 Ocak 2016: https://www.europol.europa.eu/ec3/cyber-operations adresinden alındı

Eurostat (2015). *National Accounts and GDP*. European Commission, 28 Mayıs 2015: http://ec.europa.eu/eurostat/statistics-explained/index.php/National_accounts_and_GDP adresinden alındı

Eurostat (2016). *9 February: Safer Internet Day 1 out of 4 internet users in the EU experienced security related problems in 2015 Security concerns limited uptake of certain activities,* 8 Eylül 2016, http://ec.europa.eu/eurostat/documents/2995521/7151118/4-08022016-AP-EN.pdf/902a4c42-eec6-48ca-97c3-c32d8a6131ef

Federal İçişleri Bakanlığı (2011). Cyber Security *Strategy for Germany.* Berlin: Federal İçişleri Bakanlığı. https://www.itu.int/en/ITU-

D/Cybersecurity/Documents/National_Strategies_Repository/Germany_2011_Cyber_Security_Strategy_for_Germany.pdf adresinden alındı

Fire Eye (2014). *APT 28: A Window into Russia's Cyber Espionage Operations?.* Fire Eye, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf adresinden alındı

Fox, J. (2014). *Don't fall for bank and credit-card e-mail scams in wake of Target breach Playing on consumers' fears, some deliver malicious software*. Consumerreports, 7 Şubat 2014: http://www.consumerreports.org/cro/news/2014/02/don-t-fall-for-bank-and-credit-card-e-mail-scams-in-wake-of-target-breach/index.htm adresinden alındı

Gavrila, R., Ogée, A., Trimintzios, P. ve Zacharis, A. (2014). *After Action Report.* Heraklion: ENISA. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/ce2014-after-action-report/at_download/fullReport adresinden alındı

Gercke, M. (2009). *Understanding Cybercrime: A Guide for Developing Countries.* Geneva: ITU Development Sector.

Gibson, W. (1984). *Neuromancer.* New York: Ace Books.

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.

Gözen, R. (2014). *Uluslararası İllişkiler Teorileri.* İstanbul: İletişim.

Gragner, S. (2001). Social Engineering Fundamentals, Part I: Hacker Tactics. *Security Focus*, 18 Aralık 2001. http://www.123seminarsonly.com/Seminar-Reports/021/19676093-Social-Engineering-Fundamentals.doc adresinden alındı

Greenfield, R. (2012). *A Complete Guide to Flame, the Malicious Computer Virus Ravaging Iran*. The Wire, 30 Mayıs 2012:

http://www.thewire.com/technology/2012/05/complete-guide-flame-malicious-computer-virus-ravaging-iran/52949/ adresinden alındı

Grove, J. (2011). *'Triple miracle' Sees Huge Rise in EU Funds for Frontier Research*. THE (Times Higher Education), 28 Temmuz 2011: https://www.timeshighereducation.com/news/triple-miracle-sees-huge-rise-in-eu-funds-for-frontier-research/416952.article adresinden alındı

Güvenlik ve Savunma Komitesi Sekreterliği (2013). *Finland´s Cyber Security Strategy.* Helsinki: Güvenlik ve Savunma Komitesi Sekreterliği. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf adresinden alındı

Güvenlik ve Terörle Mücadele için Ulusal Koordinatörlüğü (2011). *National Cyber Security Strategy (NCSS) 2.* Lahey: (Güvenlik ve Terörle Mücadele için Ulusal Koordinatörlüğü. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf adresinden alındı

Haberler.com. (2015). *Botnet, Ddos, Zombi Nedir Tüm Detaylarıyla İnceliyoruz,* 5 Temmuz 2015. Haberler.com: http://www.haberler.com/botnet-ddos-zombi-nedir-tum-detaylariyla-7479165-haberi/ adresinden alındı

Hansen, L. ve Nissenbaum, H. (2009). Dijital disaster, Cyber Security, and the Copenhagen School. *Uluslararası International Studies Quarterly, 53*, 1155-1175.

Hekim, H. ve Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4*(2), 135-158. http://kutuphane.dogus.edu.tr/mvt/pdfac.php?pdf=0015050 adresinden alındı

Hogben, G. (2011). *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport adresinden alındı

IBP. (2014). *EU Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Regulations.* Washington: International Business Publications.

İdare ve Dijitalleştirilme Bakanlığı. (2013). *Cyberspace Protection Policy of the Republic of Poland.* Varşova: İdare ve Dijitalleştirilme Bakanlığı. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_PO_NCSS.pdf adresinden alındı

İnternethaber. (2008). *Akılalmaz Sanal Dolandırıcılık*. İnternethaber, 26 Temmuz 2008: http://www.internethaber.com/akilalmaz-sanal-dolandiricilik-150405h.htm adresinden alındı

İskoçya Hükümeti (2015). *Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland.* Edinburg: İskoçya Hükümeti. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ScotlandNCSS.pdf adresinden alındı

İtalya Bakanlar Kurulu (2013). *National Strategic Framework for Cyberspace Security.* İtalya Bakanlar Kurulu. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/IT_NCSS.pdf adresinden alındı

Jancewski, L. J. ve Colarik, A. M. (2008). *Cyber Warfare and Cyber Terrorism*, New York: Information Science Reference.

Kabine Ofisi (2011). *The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World.* Londra: Kabine Ofisi. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/UK_NCSS.pdf adresinden alındı

Kaliber, A. (2005). Türkiye'de Güvenlikleştirilmiş Bir Alan Olarak Dış Politikayı Yeniden Düşünmek: Kıbrıs Örneği. *Uluslararası İlişkiler, 2*(7), 31-60.

Karabacak, B. (2011). Kritik Altyapılar: Dünya ve Türkiye Özeti . *Bilgem, (*5), 19-31.

Karabağlı, A. U. (2015). *16 Maddede "Bastır 10 Doları, Çökertelim Siteyi" Botnet, DoS, DDoS Nedir?* Onedio, 13 Ocak 2015: http://onedio.com/haber/16-

maddede-internette-saati-10-dolara-kiralanabilen-siber-ordular-gercegi-435279 adresinden alındı

Karagülmez, A. (2011). *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Ankara: Seçkin Yayıncılık.

Karspersky. (2015). *What is Flame Malware?* Karspersky, 20 Aralık 2015: http://www.kaspersky.com/flame adresinden alındı

Kıbrıs Elektronik Haberleşme ve Posta Yönetmeliği Komiserliği (2012). *Cybersecurity Strategy of the Republic of Cyprus Network and Information Security and Protection of Critical.* Kıbrıs: Elektronik Haberleşme ve Posta Yönetmeliği Komiserliği (OCECPR). https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf adresinden alındı

Klimburg, A. (2012). *National Cyber Security Framework Manual.* Tallin: NATO CCD COE Publications.

Kocher, P. (1996), *Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems,* CRYPTO'96, vol. 1109, 104-113.

Koenders, B. ve Mogherini, F. (2015). *Cyber Space Needs Stronger Rule of Law*. EU Observer, 16 Nisan 2015: https://euobserver.com/opinion/128342 adresinden alındı

Kroes, N. (2013). *Towards a Coherent International Cyberspace Policy for the EU*. European Commission, 30 Ocak 2013: http://europa.eu/rapid/press-release_SPEECH-13-82_en.htm adresinden alındı

Lee, D. (2012). *Flame: Massive cyber-attack discovered, researchers say*. BBC News, 28 Mayıs 2012: http://www.bbc.com/news/technology-18238326 adresinden alındı

Levine, J. R. (2016). *Written Comments of Dr. John R. Levine*. commerce.senate, 2 Ocak 2016: http://www.commerce.senate.gov/pdf/levine032304.pdf adresinden alındı

Litvanya Cumhuriyeti Devlet Güvenlik Bakanlığı (2011). *Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019.* Litvanya: Litvanya Cumhuriyeti Devlet Güvenlik Bakanlığı. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Lithuania_Cyber_Security_Strategy.pdf adresinden alındı

Lonardo, A. (2015). *EU's Cyber Security Strategy and the proposal of Directive for high level of security*. Global Cyber Security Center, 18 Aralık 2015: http://www.gc-sec.org/blog/%E2%80%9Ceu%E2%80%99s-cyber-security-strategy-and-proposal-directive-high-level-security%E2%80%9D-alessandra-lonardo-%E2%80%93- adresinden alındı

Lord, K. M. (2011). *America's Cyber Future: Security and Prosperity in the Information Age (Volume II).* Zurich: Center for New American Studies.

Lüksemburg Hükümet Büyük Dükalığı (2011). *National Cybersecurity Strategy.* Lüksemburg: Lüksemburg Hükümet Büyük Dükalığı. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Luxembourg_Cyber_Security_strategy.pdf adresinden alındı

Malmström, A. C. (2010). *Commission to boost Europe's Defence against Cyber-attacks*. Avrupa Komisyonu, 30 Eylül 2010: http://europa.eu/rapid/press-release_SPEECH-10-506_en.htm adresinden alındı

Maurice, E. (2015). *Cyber Attack on French TV Finds EU Unprepared*. EU Observer, 10 Nisan 2015: https://euobserver.com/news/128285 adresinden alındı

McElroy, D. ve Williams, C. (2012). *Flame: world's most complex computer virus exposed*. The Telegraph, 28 Mayıs 2012:

http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html adresinden alındı

Mearsheimer, J. (1994-95). The False Promise of International Institutions. *International Security, 19,* 5-49.

Memiş, T. (2001). Hukuki Açıdan Kitlelere E-posta Gönderilmesi. *Ankara Üniversitesi Hukuk Fakültesi Dergisi, 5*(1-4), 431-444. http://www.erzincan.edu.tr/birim/HukukDergi/makale/2001_V_20.pdf adresinden alındı

Meral, M. (2015). *Uluslararası Kuruluşların Gündeminde Siber Güvenlik,* Mehmetmeral.com, 27 Aralık 2015: https://mehmetmeral.wordpress.com/2015/12/27/uluslararasi-kuruluslarin-gundeminde-siber-guvenlik/ adresinden alındı

Microsoft (2016). *Microsoft Security Intelligence Report*, 27 Aralık 2015: https://www.microsoft.com/security/sir/story/default.aspx# adresinden alındı

Milanović, Z. (2015). *Nacionalna strategija i Akcijski plan sastavni su dio ove Odluke.* Zagreb. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CR_NCSS.pdf adresinden alındı

Miller, B. (2001). The Concept of Security: Should it be Redefined? *The Journal of Strategic Studies, 24*(2), 13-42.

Milliyet. (2011). *Korkutan Botnet Gerçekleri*. Milliyet, 6 Mayıs 2011: http://www.milliyet.com.tr/korkutan-botnet-gercekleri/bilisim/haberdetayarsiv/06.05.2011/1386840/default.htm adresinden alındı

Nakashima, E., Miller, G. ve Tate, J. (2012). *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*. The Washington Post, 19 Haziran 2012: https://www.washingtonpost.com/world/national-security/us-

israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html adresinden alındı

NIST (U.S. National Institute of Standards and Technology). (2011). *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf adresinden alındı

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* (s. 1-95). Sofia: ITU. Aralık 21, 2015 tarihinde http://docplayer.net/756920-Modern-trends-in-the-cyber-attacks-against-the-critical-information-infrastructure.html adresinden alındı

OECD. (2006). *Report of The OECD Task Force on Spam: Anti-spam Toolkit of Recommended Policies and Measures.* OECD. http://www.oecd.org/sti/consumer/36494147.pdf adresinden alındı

OECD. (2008). *Report OECD: Protection of "Critical Infrastructure" and the Role of Investment Policies Relating to National Security*, 1 Mayıs 2008.

of The OECD Task Force on Spam: Anti-spam Toolkit of Recommended Policies and Measures. OECD. http://www.oecd.org/sti/consumer/36494147.pdf adresinden alındı

OECD. (2009). Computer Viruses and Other Malici*ous Software: A Threat to the Internet Economy.* OECD Publishing. Aralık 25, 2015 tarihinde http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en#page1 adresinden alındı

Optimo. (2015). *Malware Infections Set New Records in Q1 of 2015.* Philadelphia: Optimo AV. Aralık 25, 2015 tarihinde http://www.optimoav.com/blog/malware-infections-set-new-records-in-q1-of-2015/ adresinden alındı

Pawlak, P. (2015). *Cyber Diplomacy: Confidence-Building Measures.* European Parliament. Brüksel: EPRS European Parliamentary Research Service. http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571302/EPRS_BRI(2015)571302_EN.pdf adresinden alındı

Rabesandratana, T. (2013). *E.U. Leaders Agree on Science Budget*. Science Mag, 27 Haziran 2013: http://www.sciencemag.org/news/2013/06/eu-leaders-agree-science-budget adresinden alındı

Reimsbach-Kounatze, C. (2012). *IMPROVING THE EVIDENCE BASE FOR INFORMATION SECURITY AND PRIVACY POLICIES Understanding the opportunities and challenges related to measuring information security, privacy and the protection of children online.* OECD. Aralık 25, 2015 tarihinde http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2011)10/FINAL&docLanguage=En adresinden alındı

Richards, J. (2009). *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security*. International Affairs Review, 4 Nisan 2009: http://www.iar-gwu.org/node/65 adresinden alındı

Romanya Hükümeti (2013). *Strategia De Securitate Cibernetica A Romaniei.* Romanya: Romanya Hükümeti. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/StrategiaDeSecuritateCiberneticaARomaniei.pdf adresinden alındı

Rouse, M. (2010). *Advanced Persistent Threat (APT).* Techtarget. http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT adresinden alındı

Slovak Cumhuriyeti Hükümeti (2008). *National Strategy for Information security in the Slovak Republic.* Slovakya: Slovak Cumhuriyeti Hükümeti. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf adresinden alındı

Sophos. (2013). *Security Threat Report New Platforms and Changing Threats.* Sophos. November 25, 2015 tarihinde https://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf adresinden alındı

SophosLabs. (2008). *Barack Obama exploited in malware spam attack*. Naked Security by Sophos, 5 Kasım 2008: https://nakedsecurity.sophos.com/2008/11/05/obama-based-malware-spam-distribution/ adresinden alındı

Sönmezoğlu, F. (2010). *Uluslararası İlişkiler Sözlüğü (3. Baskı).* İstanbul: Der Yayınları.

Stafford, T. F. ve Urbaczewski, A. (2004). Spyware: The Ghost in the Machine. *Communications of the Association for Information Systems, 14*, 291-306. Aralık 26, 2015 tarihinde http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3274&context=cais adresinden alındı

Statista, (2016). *Countries with the highest rate of malware infected computers as of 1st quarter 2016*. Statista.com, 8 Haziran 2016: http://www.statista.com/statistics/266169/highest-malware-infection-rate-countries/ adresinden alındı

Symantec. (2015). *Internet Security Threat Report.* Symantec. Ocak 2, 2016 tarihinde https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf adresinden alındı

Terriff, T., Croft, S., James, L., & Morgan, P. M. (1999). *Security Studies Today.* Cambridge: Polity Press.

The Washington Post. (2002). *Text of President Bush's 2002 State of the Union Address*, 29 Ocak 2012. http://www.washingtonpost.com/: http://www.washingtonpost.com/wp-srv/onpolitics/transcripts/sou012902.htm adresinden alındı

Traynor, I. (2007). *Russia Accused of Unleashing Cyberwar to Disable Estonia*. The Guardian, 17 Mayıs 2007: http://www.theguardian.com/world/2007/may/17/topstories3.russia adresinden alındı

Trimintzios, P., Gavrila, R. ve Klejnstrup, M. R. (2012). *Cyber Europe 2012 Key Findings and Recommendations.* Heraklion: ENISA. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report/at_download/fullReport adresinden alındı

Türk Dil Kurumu (2016). *Güncel Türkçe Sözlük.* Ankara: Türk dil Kurumu. 18 Haziran 2016 tarihinde http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5787506177f698.11790157 adresinden alındı

Ullman, R. H. (1983). Redefining Security. *International Security, 8*(1), 129-153.

Ulusal Siber Güvenlik Koordinasyon Kurulu (2013). *Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary.* Macaristan: Ulusal Siber Güvenlik Koordinasyon Kurulu. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf adresinden alındı

Uluslararası Telekomünikasyon Birliği (2008). *ITU Botnet Mitigation Toolkit.* Cenevre: Uluslararası Telekomünikasyon Birliği. Aralık 18, 2015 tarihinde http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html adresinden alındı

Uluslararası Telekomünikasyon Birliği (2008). *X.1205 : Overview of cybersecurity.* Cenevre: Uluslararası Telekomünikasyon Birliği.

Uluslararası Telekomünikasyon Birliği (2015). *Global Cybersecurity Index & Cyberwellness Profiles.* Cenevre: Uluslararası Telekomünikasyon Birliği. http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf adresinden alındı

Uluslararası Telekomünikasyon Birliği Sekreteryası (2008). *Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts.* Cenevre: Uluslararası Telekomünikasyon Birliği. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf adresinden alındı

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler*. Bilgi Teknolojileri Üst Kurulu: http://www.cybersecurity.gov.tr/publications/sg.pdf adresinden alındı

Velasco, V. (2000). *Introduction to IP Spoofing.* SANS Institue, 25 Haziran 2016: https://www.sans.org/reading-room/whitepapers/threats/introduction-ip-spoofing-959 adresinden alındı

Wæver, O. (1995). *Securitization and Desecuritization.* New York: Columbia University Press.

Ward, M. (2010). *A decade on from the ILOVEYOU bug.* BBC, 4 Mayıs 2010: http://www.bbc.com/news/10095957 adresinden alındı

Westby, J. R. (2005). *International Guide to Cyber Security* . Chicago: American Bar Association.

Whittekar, J. (2004). *The Cyberspace Handbook.* Oxon: Routledge.

Wiener, N. (1965). *Cybernetics, Second Edition: or the Control and Communication in the Animal and the Machine.* Cambridge: The MIT Press.

Yıldırımoğlu, M. (2015). *Yarattığı Virüs ile Internet'i Felç Eden Adam*. Muratyildirimoglu, 19 aralık 2015: http://muratyildirimoglu.com/makaleler/hacker1.htm adresinden alındı

EKLER

EK: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

1. INTRODUCTION

1.1. Context

Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies - most strikingly during the Arab Spring.

For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace. Our freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish if private sector innovation and civil society drive its growth. But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role.

Information and communications technology has become the backbone of our economic growth and is a critical resource which all economic sectors rely on. It now underpins the complex systems which keep our economies running in key sectors such as finance, health, energy and transport; while many business models are built on the uninterrupted availability of the Internet and the smooth functioning of information systems.

By completing the Digital Single Market, Europe could boost its GDP by almost €500 billion a year[1]; an average of €1000 per person. For new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication[2], citizens will need trust and confidence. Unfortunately, a 2012 Eurobarometer survey[3] showed that almost a third of Europeans are not confident in their ability to use the internet for banking or purchases. An overwhelming majority also said they avoid disclosing personal information

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] For example, plants embedded with sensors to communicate to the sprinkler system when it is time for them to be watered.

[3] 2012 Special Eurobarometer 390 on Cybersecurity

online because of security concerns. Across the EU, more than one in ten Internet users has already become victim of online fraud.

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cybersecurity[4] incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

The EU economy is already affected by cybercrime[5] activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.

In countries outside the EU, governments may also misuse cyberspace for surveillance and control over their own citizens. The EU can counter this situation by promoting freedom online and ensuring respect of fundamental rights online.

All these factors explain why governments across the world have started to develop cyber-security strategies and to consider cyberspace as an increasingly important international issue. The time has come for the EU to step up its actions in this area. This proposal for a Cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.

1.2. Principles for cybersecurity

The borderless and multi-layered Internet has become one of the most powerful instruments for global progress without governmental oversight or regulation. While the private sector should continue to play a leading role in the construction and day-to-day management of the Internet, the need for requirements for transparency, accountability and security is becoming more and more prominent. This strategy clarifies the principles that should guide cybersecurity policy in the EU and internationally.

The EU's core values apply as much in the digital as in the physical world

The same laws and norms that apply in other areas of our day-to-day lives apply also in the cyber domain.

---

4 Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

5 Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).

Protecting fundamental rights, freedom of expression, personal data and privacy

Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks and systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field.

Access for all

Limited or no access to the Internet and digital illiteracy constitute a disadvantage to citizens, given how much the digital world pervades activity within society. Everyone should be able to access the Internet and to an unhindered flow of information. The Internet's integrity and security must be guaranteed to allow safe access for all.

Democratic and efficient multi-stakeholder governance

The digital world is not controlled by a single entity. There are currently several stakeholders, of which many are commercial and non-governmental entities, involved in the day-to-day management of Internet resources, protocols and standards and in the future development of the Internet. The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach[6].

A shared responsibility to ensure security

The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities which need to be properly defined, thoroughly analysed, remedied or reduced. All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity.

2. STRATEGIC PRIORITIES AND ACTIONS

The EU should safeguard an online environment providing the highest possible freedom and security for the benefit of everyone. While acknowledging that it is predominantly the task of Member States to deal with security challenges in cyberspace, this strategy proposes specific actions that can enhance the EU's overall performance. These actions are both short and long term, they include a variety of policy tools[7] and involve different types of actors, be it the EU institutions, Member States or industry.

The EU vision presented in this strategy is articulated in five strategic priorities, which address the challenges highlighted above:

- Achieving cyber resilience
- Drastically reducing cybercrime

[6] See also COM(2009) 277, Communication from the Commission to the European Parliament and the Council on "Internet Governance: the next steps"

[7] The actions related to information sharing, when personal data is at stake, should be compliant with EU data protection law.

- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

2.1. Achieving cyber resilience

To promote cyber resilience in the EU, both public authorities and the private sector must develop capabilities and cooperate effectively. Building on the positive results achieved via the activities carried out to date[8] further EU action can help in particular to counter cyber risks and threats having a cross-border dimension, and contribute to a coordinated response in emergency situations. This will strongly support the good functioning of the internal market and boost the internal security of the EU.

Europe will remain vulnerable without a substantial effort to enhance public and private capacities, resources and processes to prevent, detect and handle cyber security incidents. This is why the Commission has developed a policy on Network and Information Security (NIS)[9]. The **European Network and Information Security Agency ENISA** was established in 2004[10] and a new Regulation to strengthen ENISA and modernise its mandate is being negotiated by Council and Parliament[11]. In addition, the Framework Directive for electronic communications[12] requires providers of electronic communications to appropriately manage the risks to their networks and to report significant security breaches. Also, the EU data protection legislation[13] requires data controllers to ensure data protection requirements and safeguards, including measures related to security, and in the field of publicly available e-communication services, data controllers have to notify incidents involving a breach of personal data to the competent national authorities.

Despite progress based on voluntary commitments, there are still gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders, and in terms of private sector involvement and preparedness:. This strategy is accompanied by a proposal for **legislation** to notably:

- establish common minimum requirements for NIS at national level which would oblige Member States to: designate national competent authorities for NIS; set up a well-functioning CERT; and adopt a national NIS strategy and a national NIS cooperation plan. Capacity building and coordination also concern the EU institutions: a Computer Emergency Response Team responsible for the security of the IT systems of the EU institutions, agencies and bodies ("CERT-EU") was permanently established in 2012.

---

8 See references in this Communication as well as in the Commission Staff Working Document Impact Assessment accompanying the Commission proposal for a Directive on network and information security, in particular sections 4.1.4, 5.2, Annex 2, Annex 6, Annex 8,

9 In 2001, the Commission adopted a Communication on "Network and Information Security: Proposal for A European Policy Approach" (COM(2001)298); in 2006, it adopted a Strategy for a Secure Information Society (COM(2006)251). Since 2009, the Commission has also adopted an Action Plan and a Communication on Critical Information Infrastructure Protection (CIIP) (COM(2009)149, endorsed by Council Resolution 2009/C 321/01; and COM(2011)163, endorsed by Council Conclusions 10299/11).

10 Regulation (EC) No 460/2004

11 COM(2010)521. The actions proposed in this Strategy do not entail amending the existing or future mandate of ENISA.

12 Article 13a&b of Directive 2002/21/EC

13 Article 17 of Directive 95/46/EC; Article 4 of Directive 2002/58/EC

- set up coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national NIS competent authorities. National NIS competent authorities will be asked to ensure appropriate EU-wide cooperation, notably on the basis of a Union NIS cooperation plan, designed to respond to cyber incidents with cross-border dimension. This cooperation will also build upon the progress made in the context of the "European Forum for Member States (EFMS)"[14], which has held productive discussions and exchanges on NIS public policy and can be integrated in the cooperation mechanism once in place.
- improve preparedness and engagement of the private sector. Since the large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cybersecurity is crucial. The private sector should develop, at technical level, its own cyber resilience capacities and share best practices across sectors. The tools developed by industry to respond to incidents, identify causes and conduct forensic investigations should also benefit the public sector.

However, private actors still lack effective incentives to provide reliable data on the existence or impact of NIS incidents, to embrace a risk management culture or to invest in security solutions. The proposed legislation therefore aims at making sure that players in a number of key areas (namely energy, transport, banking, stock exchanges, and enablers of key Internet services, as well as public administrations) assess the cybersecurity risks they face, ensure networks and information systems are reliable and resilient via appropriate risk management, and share the identified information with the national NIS competent authorities The take up of a cybersecurity culture could enhance business opportunities and competitiveness in the private sector, which could make cybersecurity a selling point.

Those entities would have to report, to the national NIS competent authorities, incidents with a significant impact on the continuity of core services and supply of goods relying on network and information systems.

National NIS competent authorities should collaborate and exchange information with other regulatory bodies, and in particular personal data protection authorities. NIS competent authorities should in turn report incidents of a suspected serious criminal nature to law enforcement authorities. The national competent authorities should also regularly publish on a dedicated website unclassified information about on-going early warnings on incidents and risks and on coordinated responses. Legal obligations should neither substitute, nor prevent, developing informal and voluntary cooperation, including between public and private sectors, to boost security levels and exchange information and best practices. In particular, the European Public-Private Partnership for Resilience (EP3R[15]) is a sound and valid platform at EU level and should be further developed.

---

14 The European Forum for Member States was launched via COM(2009) 149 as a platform to foster discussions among Member States public authorities regarding good policy practises on security and resilience of Critical Information Infrastructure

15 The European Public-Private Partnership for Resilience was launched via COM(2009) 149. This platform initiated work and fostered the cooperation between the public and the private sector on the identification of key assets, resources, functions and baseline requirements for resilience as well as cooperation needs and mechanisms to respond to large-scale disruptions affecting electronic communications.

The Connecting Europe Facility (CEF)[16] would provide financial support for key infrastructure, linking up Member States' NIS capabilities and so making it easier to cooperate across the EU.

Finally, cyber incident exercises at EU level are essential to simulate cooperation among the Member States and the private sector. The first exercise involving the Member States was carried out in 2010 ("Cyber Europe 2010") and a second exercise, involving also the private sector, took place in October 2012 ("Cyber Europe 2012"). An EU-US table top exercise was carried out in November 2011 ("Cyber Atlantic 2011"). Further exercises are planned for the coming years, including with international partners.

The Commission will:

- Continue its activities, carried out by the Joint Research Centre in close coordination with Member States authorities and critical infrastructure owners and operators, on identifiying NIS vulnerabilities of European critical infrastructure and encouraging the development of resilient systems.
- Launch an EU-funded pilot project[17] early in 2013 on **fighting botnets and malware,** to provide a framework for coordination and cooperation between EU Member States, private sector organisations such as Internet Service Providers, and international partners.

The Commission asks ENISA to:

- Assist the Member States in developing strong **national cyber resilience capabilities**, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure
- Examine in 2013 the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs) for the EU.
- Continue supporting the Member States and the EU institutions in carrying out regular **pan-European cyber incident exercises** which will also constitute the operational basis for the EU participation in international cyber incident exercises.

The Commission invites the European Parliament and the Council to:

- Swiftly **adopt** the proposal for a Directive on a **common high level of Network and Information Security (NIS)** across the Union, addressing national capabilities and preparedness, EU-level cooperation, take up of risk management practices and information sharing on NIS.

The Commission asks industry to:

- Take leadership in **investing** in a high level of cybersecurity and develop best practices and information sharing at sector level and with public authorities with the view of ensuring a strong and effective protection of assets and individuals, in

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. CEF Budget line 09.03.02 – Telecommunications networks (to promote the interconnection and interoperability of national public services on-line as well as access to such networks).

17 CIP-ICT PSP-2012-6, 325188. It has an overall budget of 15 Million Euro, with EU funding amounting to 7.7 Million Euro.

18 http://www.trustindigitallife.eu/

particular through public-private partnerships like EP3R and Trust in Digital Life (TDL)[18].

Raising awareness

Ensuring cybersecurity is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them.

Several initiatives have been developed in recent years and should be continued. In particular, ENISA has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships. Europol, Eurojust and national data protection authorities are also active in raising awareness. In October 2012, ENISA, with some Member States, piloted the "European Cybersecurity Month". Raising awareness is one of the areas the EU-US Working Group on Cybersecurity and Cybercrime[19] is taking forward, and is also essential in the context of the Safer Internet Programme[20] (focused on the safety of children online).

The Commission asks ENISA to:

- Propose in 2013 a roadmap for a "Network and Information Security driving licence" as a voluntary certification programme to promote enhanced skills and competence of IT professionals (e.g. website administrators).

The Commission will:

- Organise, with the support of ENISA, a cybersecurity **championship** in 2014, where university students will compete in proposing NIS solutions.

The Commission invites the Member States[21] to:

- Organise a yearly **cybersecurity month** with the support of ENISA and the involvement of the private sector from 2013 onwards, with the goal to raise awareness among end users. A synchronised EU-US cybersecurity month will be organised starting in 2014.
- **Step up national efforts on NIS education and training,** by introducing: training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations.

The Commission invites industry to:

- Promote cybersecurity **awareness at all levels**, both in business practices and in

19 This Working Group, established at the EU-US Summit in November 2010 (MEMO/10/597) is tasked with developing collaborative approaches on a wide range of cybersecurity and cybercrime issues.

20 The Safer Internet Programme funds a network of NGOs active in the field of child welfare online, a network of law enforcement bodies who exchange information and best practices related to criminal exploitation of the Internet in dissemination of child sexual abuse material and a network of researchers who gather information about uses, risks and consequences of online technologies for children's lives.

21 Also with the involvement of relevant national authorities, including NIS competent authorities and data protection authorities.

the interface with customers. In particular, industry should reflect on ways to make CEOs and Boards more accountable for ensuring cybersecurity.

2.2. Drastically reducing cybercrime

The more we live in a digital world, the more opportunities for cyber criminals to exploit. Cybercrime is one of the fastest growing forms of crime, with more than one million people worldwide becoming victims each day. Cybercriminals and cybercrime networks are becoming increasingly sophisticated and we need to have the right operational tools and capabilities to tackle them. Cybercrimes are high-profit and low-risk, and criminals often exploit the anonymity of website domains. Cybercrime knows no borders - the global reach of the Internet means that law enforcement must adopt a coordinated and collaborative cross-border approach to respond to this growing threat.

Strong and effective legislation

The EU and the Member States need strong and effective legislation to tackle cybercrime. The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, is a binding international treaty that provides an effective framework for the adoption of national legislation.

The EU has already adopted legislation on cybercrime including a Directive on combating the sexual exploitation of children online and child pornography[22]. The EU is also about to agree on a Directive on attacks against information systems, especially through the use of botnets.

The Commission will:

- Ensure swift transposition and implementation of the cybercrime related directives.
- Urge those Member States that have not yet ratified the **Council of Europe's Budapest Convention on Cybercrime** to ratify and implement its provisions as early as possible.

Enhanced operational capability to combat cybercrime

The evolution of cybercrime techniques has accelerated rapidly: law enforcement agencies cannot combat cybercrime with outdated operational tools. Currently, not all EU Member States have the operational capability they need to effectively respond to cybercrime. All Member States need effective national cybercrime units.

The Commission will:

- Through its funding programmes[23], support the Member States to **identify gaps and strengthen their capability** to investigate and combat cybercrime. The Commission will furthermore support bodies that make the link between

[22] Directive 2011/93/EU replacing Council Framework decision 2004/68/JHA

[23] For 2013, under the Prevention and Fight against Crime Programme (ISEC). After 2013, under the Internal Security Fund (new Instrument under MFF).

research/academia, law enforcement practitioners and the private sector, similar to the on-going work carried out by the Commission-funded Cybercrime Centres of Excellence already set up in some Member States.

- Together with the Member States, coordinate efforts to identify best practices and best available techniques including with the support of JRC to fight cybercrime (e.g. with respect to the development and use of forensic tools or to threat analysis)
- Work closely with the recently launched **European Cybercrime Centre (EC3), within Europol and with Eurojust** to align such policy approaches with best practices on the operational side.

Improved coordination at EU level

The EU can complement the work of Member States by facilitating a coordinated and collaborative approach, bringing together law enforcement and judicial authorities and public and private stakeholders from the EU and beyond.

The Commission will:

- Support the recently launched **European Cybercrime Centre** (EC3) as the European focal point in the fight against cybercrime. The EC3 will provide analysis and intelligence, support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders, and gradually serve as a voice for the law enforcement community[24].
- Support efforts to increase accountability of registrars of domain names and ensure accuracy of information on website ownership notably on the basis of the Law Enforcement Recommendations for the Internet Corporation for Assigned Names and Numbers (ICANN), in compliance with Union law, including the rules on data protection.
- Build on recent legislation to continue strengthening the EU's efforts to tackle child sexual abuse online. The Commission has adopted a European Strategy for a Better Internet for Children[25] and has, together with EU and non-EU countries, , launched a **Global Alliance against Child Sexual Abuse Online**[26]. The Alliance is a vehicle for further actions from the Member States supported by the Commission and the EC3.

The Commission asks Europol (EC3) to:

- Initially focus its analytical and operational support to Member States' cybercrime investigations, to help dismantle and disrupt cybercrime networks primarily in the

[24] On 28 March 2012, the European Commission adopted a Communication "Tackling Crime in a Digital Age: Establishing a European Cybercrime Centre"

[25] COM(2012) 196 final

[26] Council Conclusions on a Global Alliance against Child Sexual Abuse Online (EU-US Joint Statement) of 7th and 8th June 2012 and Declaration on the launch of the Global Alliance against Child Sexual Abuse Online (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)

areas of child sexual abuse, payment fraud, botnets and intrusion.

- On a regular basis produce strategic and operational reports on trends and emerging threats to identify priorities and target investigative action by cybercrime teams in the Member States.

The Commission asks the European Police College (CEPOL) in cooperation with Europol to:

- Coordinate the design and planning of training courses to equip law enforcement with the knowledge and expertise to effectively tackle cybercrime.

The Commission asks Eurojust to:

- Identify the main obstacles to judicial cooperation on cybercrime investigations and to coordination between Member States and with third countries and support the investigation and prosecution of cybercrime both at the operational and strategic level as well as training activities in the field.

The Commission asks Eurojust and Europol (EC3) to:

- Cooperate closely, inter alia through the exchange of information, in order to increase their effectiveness in combating cybercrime, in accordance with their respective mandates and competence.
-

2.3. Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP)

Cybersecurity efforts in the EU also involve the cyber defence dimension. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyberdefence capability development should concentrate on detection, response and recovery from sophisticated cyber threats

Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development, and closer cooperation between governments, private sector and academia in the EU. To avoid duplications, the EU will explore possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures on which the members of both organisations depend.

The High Representative will focus on the following key activities and invite the Member States and the European Defence Agency to collaborate:

- Assess operational EU cyberdefence requirements and promote the development of EU cyberdefence capabilities and technologies to address all aspects of capability development - including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability;

- Develop the EU cyberdefence policy framework to protect networks within CSDP missions and operations, including dynamic risk management, improved threat analysis

and information sharing. Improve Cyber Defence Training & Exercise Opportunities for the military in the European and multinational context including the integration of Cyber Defence elements in existing exercise catalogues;

- Promote dialogue and coordination between civilian and military actors in the EU – with particular emphasis on the exchange of good practices, information exchange and early warning, incident response, risk assessment, awareness raising and establishing cybersecurity as a priority

- Ensure dialogue with international partners, including NATO, other international organisations and multinational Centres of Excellence, to ensure effective defence capabilities, identify areas for cooperation and avoid duplication of efforts.

2.4. Develop industrial and technological resources for cybersecurity

Europe has excellent research and development capacities, but many of the global leaders providing innovative ICT products and services are located outside the EU. There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers. It is key to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data.

Promoting a Single Market for cybersecurity products

A high level of security can only be ensured if all in the value chain (e.g. equipment manufacturers, software developers, information society services providers) make security a priority. It seems[27] however that many players still regard security as little more than an additional burden and there is limited demand for security solutions. There need to be appropriate cybersecurity performance requirements implemented across the whole value chain for ICT products used in Europe. The private sector needs incentives to ensure a high level of cybersecurity; for example, labels indicating adequate cybersecurity performance will enable companies with a good cybersecurity performance and track record to make it a selling point and get a competitive edge. Also, the obligations set out in the proposed NIS Directive would significantly contribute to step up business competitiveness in the sectors covered.

A Europe-wide market demand for highly secure products should also be stimulated. First, this strategy aims to increase cooperation and transparency about security in ICT products. It calls for the establishment of a platform, bringing together relevant European public and private stakeholders, to identify good cybersecurity practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions. A prime focus should be to create incentives to carry out appropriate risk management and adopt security standards and solutions, as well as possibly establish voluntary EU-wide certification schemes building on existing schemes in the EU and internationally. The Commission will promote the adoption of coherent approaches among the Member States to avoid disparities causing locational disadvantages for businesses.

Second, the Commission will support the development of security standards and assist with EU-wide voluntary certification schemes in the area of cloud computing, while taking in due

[27] See the Commission Staff Working Document Impact Assessment accompanying the Commission proposal for a Directive on network and information security, Section 4.1.5.2

account the need to ensure data protection. Work should focus on the security of the supply chain, in particular in critical economic sectors (Industrial Control Systems, energy and transport infrastructure). Such work should build on the on-going standardisation work of the European Standardisation Organisations (CEN, CENELEC and ETSI)[28], of the Cybersecurity Coordination Group (CSCG) as well as on the expertise of ENISA, the Commission and other relevant players.

The Commission will:

- Launch in 2013 a public-private **platform on NIS solutions** to develop incentives for the adoption of secure ICT solutions and the take-up of good cybersecurity performance to be applied to ICT products used in Europe.
- Propose in 2014 recommendations to ensure cybersecurity across the ICT value chain, drawing on the work of this platform
- Examine how major providers of ICT hardware and software could inform national competent authorities on detected vulnerabilities that could have significant security-implications.

The Commission asks ENISA to:

- Develop, in cooperation with relevant national competent authorities, relevant stakeholders, International and European standardisation bodies and the European Commission Joint Research Centre, **technical guidelines and recommendations for the adoption of NIS standards and good practices** in the public and private sectors.

The Commission invites public and private stakeholders to:

- Stimulate the development and adoption of industry-led **security standards**, technical norms and security-by-design and privacy-by-design principles by ICT product manufacturers and service providers, including cloud providers; new generations of software and hardware should be equipped with **stronger, embedded and user-friendly security** features.
- Develop industry-led standards for companies' performance on cybersecurity and improve the information available to the public by developing **security labels** or kite marks helping the consumer navigate the market.

Fostering R&D investments and innovation

R&D can support a strong industrial policy, promote a trustworthy European ICT industry, boost the internal market and reduce European dependence on foreign technologies. R&D should fill the technology gaps in ICT security, prepare for the next generation of security challenges, take into account the constant evolution of user needs and reap the benefits of dual use technologies. It should also continue supporting the development of cryptography. This has to be complemented by efforts to translate R&D results into commercial solutions by providing the necessary incentives and putting in place the appropriate policy conditions.

[28] Particularly under the Smart Grids Standard M/490 for the first set of standards for a smart grid and reference architecture.

The EU should make the best of the Horizon 2020[29] Framework Programme for Research and Innovation, to be launched in 2014. The Commission's proposal contains specific objectives for trustworthy ICT as well as for combating cyber-crime, which are in line with this strategy. Horizon 2020 will support security research related to emerging ICT technologies; provide solutions for end-to-end secure ICT systems, services and applications; provide the incentives for the implementation and adoption of existing solutions; and address interoperability among network and information systems. Specific attention will be drawn at EU level to optimising and better coordinating various funding programmes (Horizon 2020, Internal Security Fund, EDA research including European Framework Cooperation).

The Commission will:

- Use Horizon 2020 to address a range of areas in ICT privacy and security, from R&D to innovation and deployment. Horizon 2020 will also develop tools and instruments to fight criminal and terrorist activities targeting the cyber environment.
- Establish mechanisms for better coordination of the research agendas of the European Union institutions and the Member States, and incentivise the Member States to invest more in R&D.

The Commission invites the Member States to:

- Develop, by the end of 2013, good practices to use the **purchasing power of public administrations** (such as via public procurement) to stimulate the development and deployment of security features in ICT products and services.
- Promote early involvement of industry and academia in developing and coordinating solutions. This should be done by making the most of Europe's Industrial Base and associated R&D technological innovations, and be coordinated between the research agendas of civilian and military organisations;

The Commission asks Europol and ENISA to:

- Identify emerging trends and needs in view of evolving cybercrime and cybersecurity patterns so as to develop adequate digital forensic tools and technologies.

The Commission invites public and private stakeholders to:

- Develop, in cooperation with the insurance sector, **harmonised metrics for calculating risk premiums**, that would enable companies that have made investments in security to benefit from lower risk premiums.

2.5. Establish a coherent international cyberspace policy for the European Union and promote EU core values

Preserving open, free and secure cyberspace is a global challenge, which the EU should address together with the relevant international partners and organisations, the private sector and civil society.

[29] Horizon2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. Running from 2014 to 2020, the EU's new Framework Programme for research and innovation will be part of the drive to create new growth and jobs in Europe.

In its international cyberspace policy, the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyberspace. The EU will also work towards closing the digital divide, and will actively participate in international efforts to build cybersecurity capacity. The EU international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights.

Mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy

The Commission, the High Representative and the Member States should articulate a coherent EU international cyberspace policy, which will be aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and private sector. EU consultations with international partners on cyber issues should be designed, coordinated and implemented to add value to existing bilateral dialogues between the EU's Member States and third countries. The EU will place a renewed emphasis on dialogue with third countries, with a special focus on like-minded partners that share EU values. It will promote achieving a high level of data protection, including for transfer to a third country of personal data. To address global challenges in cyberspace, the EU will seek closer cooperation with organisations that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS. At bilateral level, cooperation with the United States is particularly important and will be further developed, notably in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime.

One of the major elements of the EU international cyber policy will be to promote cyberspace as an area of freedom and fundamental rights. Expanding access to the Internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance. The EU should promote corporate social responsibility[30], and launch international initiatives to improve global coordination in this field.

The responsibility for a more secure cyberspace lies with all players of the global information society, from citizens to governments. The EU supports the efforts to define norms of behaviour in cyberspace that all stakeholders should adhere to. Just as the EU expects citizens to respect civic duties, social responsibilities and laws online, so should states abide by norms and existing laws. On matters of international security, the EU encourages the development of confidence building measures in cybersecurity, to increase transparency and reduce the risk of misperceptions in state behaviour.

The EU does not call for the creation of new international legal instruments for cyber issues.

The legal obligations enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should be also respected online. The EU will focus on how to ensure that these measures are enforced also in cyberspace.

To address cybercrime, the Budapest Convention is an instrument open for adoption by third countries. It provides a model for drafting national cybercrime legislation and a basis for international co-operation in this field.

[30] *A renewed EU strategy 2011-14 for Corporate Social Responsibility***;** COM(2011) 681 final

If armed conflicts extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights law will apply to the case at hand. **Developing capacity building on cybersecurity and resilient information infrastructures in third countries**

The smooth functioning of the underlying infrastructures that provide and facilitate communication services will benefit from increased international cooperation. This includes exchanging best practices, sharing information, early warning joint incident management exercises, and so on. The EU will contribute towards this goal by intensifying the on-going international efforts to strengthen Critical Information Infrastructure Protection (CIIP) cooperation networks involving governments and the private sector.

Not all parts of the world benefit from the positive effects of the Internet, due to a lack of open, secure, interoperable and reliable access. The European Union will therefore continue to support countries' efforts in their quest to develop the access and use of the Internet for their people, to ensure its integrity and security and to effectively fight cybercrime.

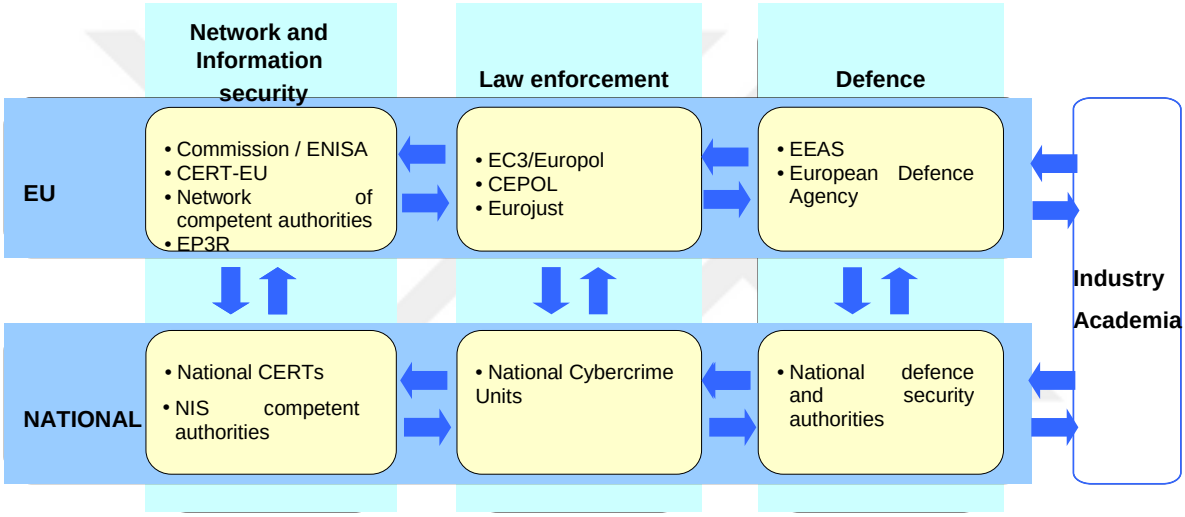
In cooperation with the Member States, the Commission and the High Representative will:

- Work towards a coherent EU International cyberspace policy to increase engagement with key international partners and organisations, to mainstream cyber issues into CFSP, and to improve coordination of global cyber issues;
- Support the development of norms of behaviour and confidence building measures in cybersecurity. Facilitate dialogues on how to apply existing international law in cyberspace and promote the Budapest Convention to address cybercrime;
- Support the promotion and protection of fundamental rights, including access to information and freedom of expression, focusing on: a) developing new public guidelines on freedom of expression online and offline; b) monitoring the export of products or services that might be used for censorship or mass surveillance online; c) developing measures and tools to expand Internet access, openness and resilience to address censorship or mass surveillance by communication technology; d) empowering stakeholders to use communication technology to promote fundamental rights;
- Engage with international partners and organisations, the private sector and civil society to support global capacity-building in third countries to improve access to information and to an open Internet, to prevent and counter cyber threats, including accidental events, cybercrime and cyber terrorism, and to develop donor coordination for steering capacity-building efforts;
- Utilise different EU aid instruments for cybersecurity capacity building, including assisting the training of law enforcement, judicial and technical personnel to address cyber threats; as well as supporting the creation of relevant national policies, strategies and institutions in third countries;
- Increase policy coordination and information sharing through the international Critical Information Infrastructure Protection networks such as the Meridian network, cooperation among NIS competent authorities and others.

3. ROLES AND RESPONSIBILITIES

Cyber incidents do not stop at borders in the interconnected digital economy and society. All actors, from NIS competent authorities, CERTs and law enforcement to industry, must take responsibility both nationally and at EU-level and work together to strengthen cybersecurity. As different legal frameworks and jurisdictions may be involved, a key challenge for the EU is to clarify the roles and responsibilities of the many actors involved.

Given the complexity of the issue and the diverse range of actors involved, centralised, European supervision is not the answer. National governments are best placed to organise the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks. At the same time, due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement. To address cybersecurity in a comprehensive fashion, activities should span across three key pillars—NIS, law enforcement, and defence—which also operate within different legal frameworks:



3.1. Coordination between NIS competent authorities/CERTs, law enforcement and defence

National level

Member States should have, either already today or as a result of this strategy, structures to deal with cyber resilience, cybercrime and defence; and they should reach the required level of capability to deal with cyber incidents. However, given that a number of entities may have operational responsibilities over different dimensions of cybersecurity, and given the importance of involving the private sector, coordination at national level should be optimised across ministries. Member States should set out in their national cybersecurity strategies the roles and responsibilities of their various national entities.

Information sharing between national entities and with the private sector should be encouraged, to enable the Member States and the private sector to maintain an overall view of different threats and get a better understanding of new trends and techniques used both to commit cyber-attacks and react to them more swiftly. By establishing national NIS cooperation plans to be activated in the case of cyber incidents, the Member States should be able to clearly allocate roles and responsibilities and optimise response actions.

EU level

Just as at national level, there are at EU level a number of actors dealing with cybersecurity. In particular, the ENISA, Europol/EC3 and the EDA are three agencies active from the perspective of NIS, law enforcement and defence respectively. These agencies have Management Boards where the Member States are represented, and offer platforms for coordination at EU level.

Coordination and collaboration will be encouraged among ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, risk assessment, training and sharing of best practices. They should collaborate while preserving their specificities. These agencies together with CERT-EU, the Commission and the Member States should support the development of a trusted community of technical and policy experts in this field.

Informal channels for coordination and collaboration will be complemented by more structural links. EU military staff and the EDA cyber defence project team can be used as the vector for coordination in defence. The Programme Board of Europol/EC3 will bring together among others the EUROJUST, CEPOL, the Member States[31], ENISA and the Commission, and offer the chance to share their distinct know-how and to make sure EC3's actions are carried out in partnership, recognising the added expertise and respecting the mandates of all stakeholders. The new mandate of ENISA should make it possible to increase its links with Europol and to reinforce links with industry stakeholders. Most importantly, the Commission's legislative proposal on NIS) would establish a cooperation framework via a network of national NIS competent authorities and address information sharing between NIS and law enforcement authorities.

International

The Commission and the High Representative ensure, together with the Member States, coordinated international action in the field of cybersecurity. In so doing, the Commission and the High Representative will uphold EU core values and promote a peaceful, open and transparent use of cyber technologies. The Commission, the High Representative and the Member States engage in policy dialogue with international partners and with international organisations such as Council of Europe, OECD, OSCE, NATO and UN.

3.2. EU support in case of a major cyber incident or attack

Major cyber incidents or attacks are likely to have an impact on EU governments, business and individuals. As a result of this strategy, and in particular the proposed directive on NIS, the prevention, detection and response to cyber incidents should improve and Member States and the Commission should keep each other more closely informed about major cyber incidents or attacks. However, the response mechanisms will differ depending on the nature, magnitude and cross-border implications of the incident.

If the incident has a serious impact on the business continuity, the NIS directive proposes that national or Union NIS cooperation plans be triggered, depending on the cross-border nature of the incident. The network of NIS competent authorities would be used in that context to share

[31] via representation within the EU Cybercrime Task Force, which is made up of the heads of the EU cybercrime Units of the Member States

information and support. This would enable preservation and/or restoration of affected networks and services.

If the incident seems to relate to a crime, Europol/EC3 should be informed so that they - together with the law enforcement authorities from the affected countries – can launch an investigation, preserve the evidence, identify the perpetrators and ultimately make sure they are prosecuted.

If the incident seems to relate to cyber espionage or a state-sponsored attack, or has national security implications, national security and defence authorities will alert their relevant counterparts, so that they know they are under attack and can defend themselves. Early warning mechanisms will then be activated and, if required, so will crisis management or other procedures. A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union).

If the incident seems having compromised personal data, the national Data Protection Authorities or the national regulatory authority pursuant to Directive 2002/58/EC should be involved.

Finally, the handling of cyber incidents and attacks will benefit from contact networks and support from international partners. This may include technical mitigation, criminal investigation, or activation of crisis management response mechanisms.

4. CONCLUSION AND FOLLOW-UP

This proposed cybersecurity strategy of the European Union, put forward by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, outlines the EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world.[32]

This vision can only be realised through a true partnership, between many actors, to take responsibility and meet the challenges ahead.

The Commission and the High Representative therefore invite the Council and the European Parliament to endorse the strategy and to help deliver the outlined actions. Strong support and commitment is also needed from the private sector and civil society, who are key actors to enhance our level of security and safeguard citizens' rights.

[32] The financing of the Strategy will occur within the foreseen amounts for each of the relevant policy areas (CEF, Horizon 2020, Internal Security Fund, CFSP and External Cooperation, notably the Instrument for Stability) as set out in the Commission's proposal for the Multi-Annual Financial Framework 2014-2020 (subject to the approval of the Budget Authority and the final amounts of the adopted MFF for 2014-2020). With regard to the need to ensure overall compatibility with the number of posts available to decentralised agencies and the sub-ceiling for decentralised agencies in each expenditure heading in the next MFF, the agencies (CEPOL, EDA ENISA, EUROJUST and EUROPOL/EC3) which are requested by this Communication to take on new tasks will be encouraged to do so in so far as the actual capacity of the agency to absorb growing resources has been established and all possibilities for redeployment have been identified.

The time to act is now. The Commission and the High Representative are determined to work together with all actors to deliver the security needed for Europe. To ensure that the strategy is being implemented promptly and assessed in the face of possible developments, they will gather together all relevant parties in a high-level conference and assess progress in 12 months.