AVRUPA BİRLİĞİ'NİN SİBER GÜVENLİK STRATEJİSİ İÇİN KURAMSAL ÇERÇEVE VE STRATEJİ BELGESİ ÖNCESİ AB'NİN EYLEMLERİ

Mehmet Eren*

ÖZET

Bilgi ve iletişim teknolojilerindeki gelişme ile önem kazanan siber güvenlik ve AB'nin geliştirmiş olduğu siber güvenlik politikası makalenin ana temasını oluşturmaktadır. Kapsamlı bir siber güvenlik tanımı ile başlayan makalede, siber güvenlik, Barry Buzan ve Ole Wæver'ın başını çektiği Kopenhag Ekolünün gündeme getirdiği güvenlikleştirme kavramı ile teorik çerçeveye oturtulmuştur. Avrupa Birliği'ni doğrudan etkileyen siber saldırılardan Estonya 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 politikalara ve yol haritalarına gelen süreçteki AB'nin eylemleri çalışmanın ana konusunu oluşturmuştur. Makalenin ana argümanı, AB siber güvenlik stratejisinin oluşturulması sürecinin kuramsal temel olarak güvenlikleştirme yaklaşımı ile açıklanabileceği ve strateji belgesi öncesi gelişmelerin bu savı güçlendirdiğidir.

Anahtar Kelimeler: Siber Uzay, Güvenlikleştirme, Siber Saldırılar, Siber Güvenlik, AB'nin Siber Güvenlik Politikası.

CONCEPTUAL FRAMEWORK FOR THE EUROPEAN UNION'S CYBER SECURITY STRATEGY AND EU ACTIONS BEFORE STRATEGY DOCUMENT

ABSTRACT

The subject of this article is the EU's cyber security policy. Cyber security gets more important with advancements in information and communications technology. The article starts with a comprehensive explanation of cyber security. The conceptual framework of this article is securitization, a concept developed by the Copenhagen School, especially by Ole

*Doktora Adayı, Marmara Üniversitesi, Kuveyt Türk Katılım Bankası, mehmeteren@outlook.fr adresinden ulaşılabilir.

Wæver and Barry Buzan. Cyber-attacks on Estonia is examined as example of cyber attacks that directly affected the European Union. “Cybersecurity Strategy of the European Union” is the basis of the EU's cyber security policy. This article throughly examines the major goals and policies/actions that this strategy outlines. The major argument of this article that the process of setting up the EU Cyber security strategy can be explained by the securitization approach as the conceptual framework, and the pre-strategy actions of EU strengthen this argument.

Key Words: Cyberspace, Securitization, Cyber Attacks, Cyber Security, Cyber Security Policy of the EU.

GİRİŞ

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 siber 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.

[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)

Çalışmanın amacı, Avrupa Birliği'nin siber güvenlik stratejisi belgesinin oluşturulmasına gelen süreci güvenlikleştirme perspektifinden değerlendirerek, stratejinin hangi kuramsal çerçeve ile açıklanabileceğine ve bu süreçteki AB'nin eylemlerine bir perspektif sunmaktır.

Bu makalede 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.

Makalenin cevap aradığı temel soruları ise şu şekilde sıralamak mümkündür:

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

"AB'nin siber uzayı güvenlikleştirmesine dair en önemli belge olan siber güvenlik stratejisi hangi kuramsal çerçevede değerlendirilebilir?",

"AB'nin siber güvenlik strateji belgesi öncesinde AB'nin siber güvenliğin sağlanması için eylemleri nelerdir?".

Yukarıdaki sorulardan yola çıkılarak yapılan araştırmalar neticesinde bu makalenin ana argümanı, AB siber güvenlik strateji belgesinin oluşturulması sürecinin kuramsal temel olarak güvenlikleştirme yaklaşımı ile açıklanabileceği ve strateji belgesi öncesi gelişmelerin bu savı güçlendirdiğidir.

Makalede Avrupa Birliği'nin strateji belgesine gelinen süreçteki 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 analitik 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.

Makalede, siber güvenlik kavramı açıklanarak, güvenlik algısının değişimi ve güvenlikleştirme kuramı detaylandırılmış, siber güvenliği anlamlandırmakta nasıl kullanılabileceği ortaya konulmuştur. Avrupa Birliği'nin siber güvenlik politikasının oluşmasında ve etkili bir gelişim göstermesinde AB üyesi devletleri doğrudan etkileyen siber saldırı olarak, Estonya örneği değerlendirilmiştir. Strateji belgesine gelinen süreçte AB'nin siber güvenlik politikaları, AB kurumları tarafından yayınlanan raporlar, bildiriler ve eylem planları çerçevesinde analiz edilerek sunulmuştur. 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. Ayrıca AB'nin yayınlamış olduğu dokümanlar üzerinden nasıl bir siber güvenlik stratejisinin oluşturulmaya çalışıldığı, atılan adımlar ve pratik hayattaki uygulamalar sunulmuştur.

Sonuç olarak makalenin tezi, AB siber güvenlik stratejisinin oluşturulması sürecinin kuramsal temel olarak güvenlikleştirme yaklaşımı ile açıklanabileceği ve strateji belgesi öncesi gelişmelerin bu savı güçlendirdiğidir. Kopenhag Ekolünün güvenlikleştirme perspektifinden siber güvenlik analizinin mümkün olduğu, siber uzayın güvenlikleştirilmesindeki rollerin ve sorumlulukların AB'deki roller ve sorumluluklarla örtüştüğüdür.

KOPENHAG OKULU VE GÜVENLİK ÇALIŞMALARI

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). Güvenliğin 'esası tartışılan' bir kavram olarak nitelendirilmesi, aynı zamanda bu kavramın öznelliğine ve farklı şekillerde anlaşılmasına da ortam hazırlamaktadır. 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[2] (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 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)[3] 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

[2] "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'te 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)

[3] 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)

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. (Eren, 2017: 14) Örneğin, demokratik ülkelerde tehditleri ve güvenlik politikalarını belirleme yetkisi önceden seçimler yoluyla hükümetlere verilir. 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 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[4] için suistimal edilebilir. Bu

[4] 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

anlamda, güvenlik, her zaman sonuçları fayda sağlayıcı bir kavram değildir. Pozitif olmaktan çok negatif sonuçlar vermesi 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)

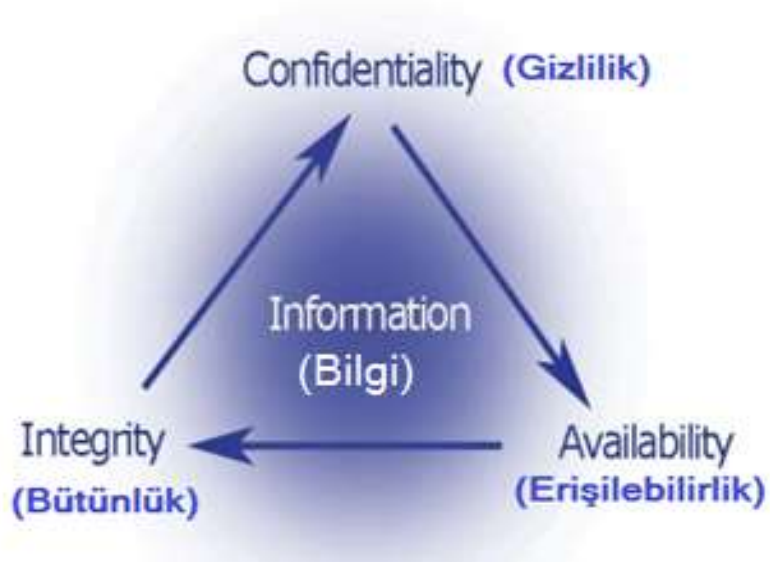
Bir söz edimi ile başlayan ve olağanüstü önlemler kullanılması ile sonuçlanan sürece Kopenhag Ekolü "güvenlikleştirme" (securitization) adını vermiştir (Buzan, Wæver ve Wilde, 1998: 24) Daha kolay bir analiz çerçevesi sunmak amacıyla Kopenhag Ekolü güvenliği sektörlere ayırmıştır. Gerçek hayatta bu sektörlerin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

SİBER GÜVENLİK KAVRAMININ ANALİZİ

Bilgi teknolojilerine ilişkin birçok kavramda olduğu gibi siber güvenlik kavramına ilişkin olarak da net bir tanım yapmak mümkün olmamaktadır. 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.

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)

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 hususun siber güvenliğin temel hedefleri olduğunu söylemek de 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 sızmalara ve yetkisiz kişilerin ulaşımına zemin hazırlayacaktır. Siber güvenlik de bu noktada devreye girmekte ve bu bileşenlerin ayrı

ayrı sağlanması için önlemler geliştirmektedir.

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)

SİBER GÜVENLİK VE GÜVENLİKLEŞTİRME İLİŞKİSİ

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 (Eren, 2017: 25). 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 makalede tercih edilen kuramsal çerçeve olmuştur. AB'nin siber güvenlik politikasını oluşturmasında geçen süreçte gerek Avrupa Komisyonu Başkanının, gerekse Avrupa Parlamentosu yetkililerinin söylemleri, demeçleri[5] 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.

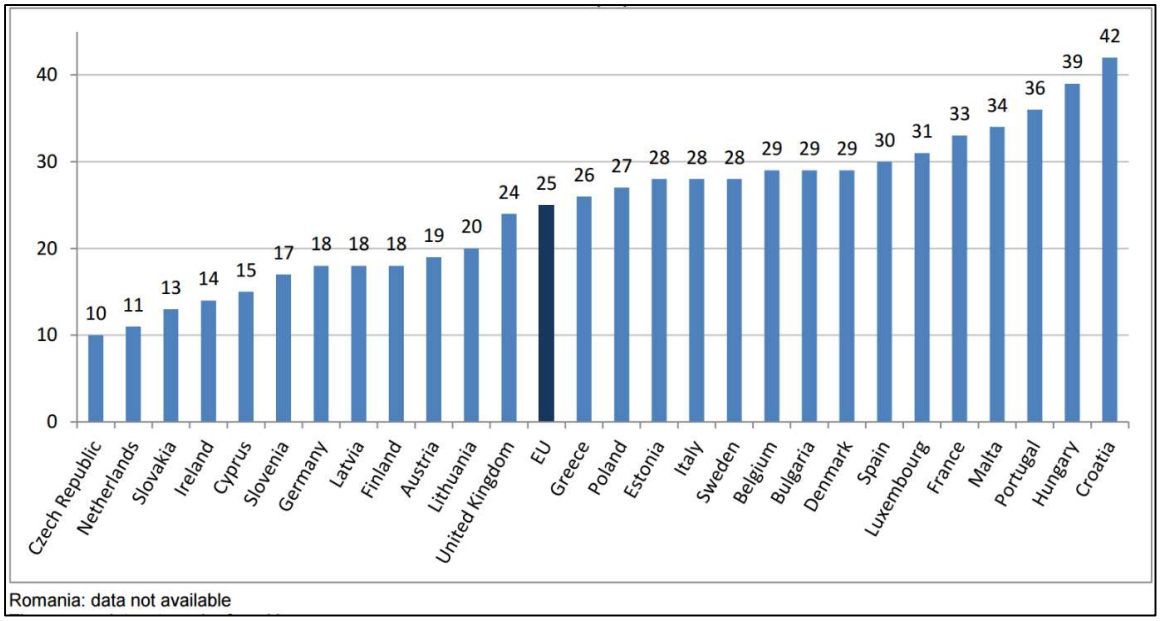
Kopenhag Ekolünde Hansen ve Nissenbaum gibi analizcilerin yayınları başta olmak üzere siber güvenliği ayrı bir sektör olarak değerlendiren çalışmalar da mevcuttur. (Hansen ve

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

Nissenbaum, 2009) 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 makalede başlı başına bir sektör olmaktan çok tüm sektörlerle bağlantılı bir güvenlik olgusu olarak değerlendirilmiştir.[6] Bu çalışmanın genelinde ana referans noktası siber güvenliğin tüm sektörleri kapsayan bir güvenlik olgusu olduğu yönündedir.

AB'Yİ DOĞRUDAN ETKİLEYEN SİBER SALDIRI: ESTONYA ÖRNEĞİ

AB'yi doğrudan etkileyen siber olaylar olarak Estonya devletine yönelik gerçekleştirilen siber saldırılar büyük öneme sahiptir. Bu örneği detaylandırmadan önce aşağıdaki istatistiki bilgiler ile AB'nin konuya verdiği öneme dikkat çekmek ve politikaların temelindeki kök nedenleri anlamak yerinde olacaktır.



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

Kaynak: (Eurostat, 2016: 1)

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

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

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, 2007).

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. Estonya hükümetine yönelik gerçekleştirilen siber saldırıların uğrattığı zararın 19-28 milyon Euro aralığında olduğu tahmin edilmektedir (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).

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).

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 her zaman AB için önemli referans kaynağı 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.

STRATEJİ BELGESİ ÖNCESİNDE AB'NİN EYLEM PLANI

Bu bölümde, AB'nin siber güvenlik politikasını oluşturan temel doküman olan "Cybersecurity Strategy for the European Union" (Avrupa Komisyonu, 2013) (Avrupa Birliği için Siber Güvenlik Stratejisi) belgesine gelinen süreçte AB'nin eylemleri ve AB düzeyinde yayınlanan yasal düzenlemeler 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. Gerek dünya genelindeki örneklerden ders almak, gerekse AB'yi doğrudan etkileyen örneklerle tekrar karşılaşmamak için siber güvenliğin sağlanması konusunda AB tarafından strateji belgesine kadar olan süreçte oluşturulan politikalar bu bölümün ana konusunu oluşturmaktadır.

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 gruplandırılarak verilmiştir.

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. (Eren, 2017: 70)

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 değerlendirilebileceği söylenebilir. Nitekim güvenlikleştirmenin etkisi ve güç, başvuru nesnesinin önem derecesine göre şekillenmektedir. (Eren, 2017: 72) 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)[7] hakkında da bilgi verilmiştir.

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)

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

[7] 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, 2016)

geliştirmeye teşvik etmek amacıyla 2013 yılında AB için Endüstriyel Kontrol Sistemleri - Bilgisayar Güvenliği Olaylarına Müdahale Ekibi (ICS-CSIRTs)[8] 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.[9]

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)

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)

[8] Computer Security Incident Response Team(s) for Industrial Control Systems (Endüstriyel Kontrol Sistemleri - Bilgisayar Güvenliği Olaylarına Müdahale Ekibi)

[9] 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).

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 gerçekleşmiştir. Tehdit, çıkartılan yasal düzenlemeler ile pekiştirilmiş ve alımlayıcı kitleye kabul ettirilebilir hale gelmiş ve önlem alınması gereken bir durum olarak kabul ettirilmiştir. (Eren, 2017: 77)

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, 2013: 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[10])

[10] 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 makalede 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

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, 2013): 5). Katılımcıları üye devletlerin kamu otoriteleri olan bu forum kapsamında etkili bir NIS politikası için sorunların detaylı olarak tartışılması mümkün olmaktadır ve politika yapım sürecinde farklı bakış açılarına da yer verilebilmektedir (Avrupa Komisyonu, 2009).

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

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, 2009a) ve 2011 yılında "Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security'" (Avrupa Komisyonu, 2011) belgelerinde de yer bulmuştur.

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).

Tüm bu gelişmelerin sonucunda AB, 2013 yılında AB'nin siber güvenlik politikasının temelini oluşturan "Avrupa Birliği için Siber Güvenlik Stratejisi" belgesi ile Birliğin ortak siber güvenlik politikası kapsamında gerçekleştireceği temel politikaları ve yol haritalarını belirlemiştir. Ayrıca gerek AB kurumlarının sorumlulukları, gerekse üye devletlerin ulusal makamlarının üstleneceği roller bu strateji belgesi ile genel bir çerçeveye oturtulmuştur. Bu çerçevede ortaya çıkan bu strateji belgesinin Kopenhag Ekolünün analiz çerçevesi sunduğu güvenlikleştirme yaklaşımının en önemli çıktısı olarak değerlendirebiliriz.

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. Siber tehditlerin Avrupa Birliği tarafından nasıl değerlendirileceğine dair kavramsal bir çerçeve sunulmuş ve devamında AB'nin siber güvenlik strateji belgesine gelen süreçteki AB politikaları değerlendirilmiştir.

Güvenlikleştirme yaklaşımı temel alınarak 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. 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 stratejisinde 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.

AB'nin siber güvenlik anlayışı nasıl şekillendiğinin verildiği bu makalede, AB'nin siber uzayı güvenlikleştirmesine dair en önemli belge olan siber güvenlik stratejisinin güvenlikleştirme perspektifinden değerlendirilebileceği görülmektedir. AB'nin siber güvenlik strateji belgesi öncesinde AB'nin siber güvenliğin sağlanması için uyguladığı politikaların ve yasal düzenlemelerin de bu savı güçlendirdiğinin söylemek yerinde olacaktır. Nitekim Estonya örneğinden de yola çıkarak AB yetkililerinin söylemlerinin ve uygulamaya konulan

politikaların güvenlikleştirme zemininde değerlendirilebileceği ve strateji belgesinin de bu sürecin en önemli çıktısı olduğunu söylemek mümkündür.

Yapılan araştırmalar neticesinde özetle, AB siber güvenlik strateji belgesinin oluşturulması sürecinin kuramsal temel olarak güvenlikleştirme yaklaşımı ile açıklanabileceğini ve strateji belgesi öncesi gelişmelerin bu savı güçlendirdiğini 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

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 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). *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 (2009b). *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 (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 (2011). *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 (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 (2013). *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 (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 (2016). *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.htmadresinden 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.

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

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

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

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

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.

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

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

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

Eren, M. (2017). *Avrupa Birliği'nin Siber Güvenlik Politikası,.* İstanbul: Beta Yayınları.

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

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

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

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.

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

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

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

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

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

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

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.

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

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

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