Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi Yıl: 2023/1, Sayı: 45, s. 391-412
Journal of Süleyman Demirel University Institute of Social Sciences Year: 2023/1, Number: 45, p. 391-412
Kabul/Accepted: 26.04.2023 Online Yayın/Online Published: 30.04.2023

HİBRİT TEHDİTLER ve AVRUPA BİRLİĞİ

Eda ÜNAL[1]
Selim KANAT[2]
Muharrem GÜRKAYNAK[3]

ÖZET

Günümüzün çok aktörlü, çok yönlü, çok faktörlü ve çok boyutlu güvenlik ortamında hibrit tehditler güvenlik politikalarının vazgeçilmez bir faktörü haline gelmiştir. Gündelik yaşantıda da giderek artan dijitalleşme, hibrit tehditler arasında siber saldırıları ayrı bir konuma yükseltmektedir. Avrupa Birliği üyesi devletler için de durum farklı değildir. Bu durum açısından, araştırmanın sorusu da Avrupa Birliği'nin hibrit tehditler ile mücadelede nasıl bir ortak politika ürettiğidir. Araştırmada test edilecek hipotez ise Avrupa Birliği'nin hibrit tehditler ile, ulusal emniyet teşkilatları, istihbarat servisleri, Europol, ENISA (Avrupa Birliği Siber Güvenlik Ajansı) gibi resmî kurumlar haricinde siber güvenlik kurumları, siber güvenliğe dair özel şirketler vasıtasıyla bilhassa istihbarat paylaşımı ile mücadele etmeyi seçtiği yönündedir. Çalışmanın hipotez testinde bir konuyu geniş kapsamlı ele alıp değerlendirmede avantajlı olduğundan nitel yöntemler tercih edilmiştir. Bilhassa yabancı literatür temel ve resmi kaynaklar üzerinden taranmıştır. Elde edilen bulgular sayısal veriler ve örnek olaylarla da test edilerek hipotez ispatında kullanılmıştır. Araştırma neticesinde ulaşılan sonuç ise Avrupa Birliği'nin, yürürlükte olan Siber Güvenlik Kanunuyla (The EU Cybersecurity Act) birlikte, ENISA için yeni bir dönemin başlamış olduğudur. Bu kanun ENISA'ya Avrupa Birliği üye ülkelerinin hibrit tehditlerle mücadelesinde yardımcı olmasını sağlayan daha fazla sorumluluk yüklenmiş ve kaynak ayrılmıştır. ENISA Avrupa Birliği'nin hibrit tehditlere karşı geliştirdiği politikaların merkezi konumunu önümüzdeki dönemler de sürdürecektir.

Anahtar Kelimeler: *Hibrit Tehditler, AB Siber Güvenlik Kanunu, ENISA, EEAS, ECSO*

[1] Eda Ünal, Doktora Öğrencisi, Süleyman Demirel Üniversitesi Avrupa Birliği Çalışmaları Anabilimdalı MEB İngilizce Öğretmeni. d1940262002@ogr.sdu.edu.tr ORCID: 0000-0003-1886-2058, (Sorumlu Yazar).

[2] Selim Kanat, Doç. Dr., Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Uluslararası İlişkiler Bölümü, selimkanat@yahoo.com, ORCID: 0000-0003-2663-3757.

[3] Muharrem Gürkaynak, Prof. Dr., Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Uluslararası İlişkiler Bölümü, muharremgurkaynak@sdu.edu.tr, ORCID: 0000-0002-5371-0474.

HYBRID THREATS and the EUROPEAN UNION

ABSTRACT

In today's multi-actor, multi-directional, multi-factor and multi-dimensional security environment, hybrid threats have become an indispensable factor of security policies. Increasing digitalization in daily life has elevated cyber-attacks to a special position among hybrid threats. The situation is no different for the member states of the European Union. In view of this situation, the question of the research is how the European Union produces a common policy in the fight against hybrid threats. The hypothesis to be tested in the research is that the European Union has chosen to combat hybrid threats through cyber security institutions, cyber security institutions, cyber security private companies, especially intelligence sharing, apart from official institutions such as national law enforcement agencies, intelligence services, Europol, ENISA (European Union Cyber Security Agency). In the hypothesis testing of the study, qualitative methods were preferred as they are advantageous in addressing and evaluating an issue comprehensively. In particular, foreign literature was reviewed through primary and official sources. The findings were tested with numerical data and case studies and used to prove the hypothesis. The conclusion of the research is that a new era has begun for ENISA with the EU Cybersecurity Act. This law has given ENISA more responsibilities and resources to help European Union member states combat hybrid threats. ENISA will continue to be at the center of the European Union's policies against hybrid threats for the foreseeable future.

Keywords: *Hybrid Threats, EU Cyber Security Act, ENISA, EEAS, ECSO.*

1. GİRİŞ

Hibrit tehdit kavramı ilk kez Hoffman tarafından 2007 yılında "Hibrit Savaş" tanımlaması yapılırken ortaya atılmıştır. Hoffman bildiğimiz manada savaşı konvansiyonel savaş olarak niteleyip asimetrik çatışma, siber savaş, çatışma sırasında sahte haberler gibi yöntemlerle harmanlanan bir askeri strateji olarak hibrit savaş kavramını tanımlamıştır (2007: 28-31). Bu manada hibrit tehditler ilk olarak silahlı çatışma hallerine varmayan ancak silahlı çatışmalar sırasında veya önsesi ya da sonrasında kullanılan askeri çatışma taktikleri olarak nitelenmişlerdir. Hibrit tehditlerin, tehdit oluşturabilme potansiyelleri ile savaşın veya toplumsal yaşantının dijitalleşmesi arasında doğru bir korelasyon vardır. Hayatın dijitalleşmesin uluslararası güvenlik aktörlerinin de çeşitlenmesi, yani tehdidin ve güvenliğin yegâne aktörünün devletler olmaktan çıkması eşlik edince geleceğin dünyasında artık tehditlerin giderek artan oranda hibrit olması muhtemeldir.

Güvenlik kavramı tehditler ile tanımlanan bir kavramdır. Tehditler değiştikçe güvenlik politikalarının, tanımlamalarının da değişmesi söz konusu olur. Avrupa Birliği Bakanlar Konseyi de bu değişimin farkında olarak hibrit tehditlerle mücadele kapasitesinin artırılmasını; bunu yaparken de üye ülkelerin siber, stratejik iletişim ve karşı istihbarat gibi konularda hibrit tehditlerin belirlenmesi, önlenmesi ve bunlara karşılık verilmesi yönünde çalışmalara hız vermeleri gerektiğini belirtmektedir (EU Comission, 2018). Çünkü hibrit tehditlere yenilikçi bir güvenlik anlayışı ile müdahale edilmelidir (Portman, 2018: 41). Avrupa Birliği (AB) hibrit tehditlerin günümüzde daha yoğun bir şekilde siber alem vasıtasıyla gerçekleştiği ön kabulünden hareketle, bu tehditler ile mücadelede ön cephe olarak da siber güvenlik önlemlerini görmektedir demek çok da yanlış olmayacaktır.

Avrupa Birliği'ne göre üye devletlerde internetin güvenilirliğini ve karşılıklı çalışabilirliğini sürdürmek, çevrimiçi dünyada temel haklara saygının devamlılığını ve bu hakların korunmasını sağlamak, ayrıca internete güvenli olarak erişimin ve bilgilerin gizliliğinin garantisini vermek gibi özgürlük ve güvenlik konularında önemli rolleri bulunmaktadır (European Comission, 2013). Diğer bir değişle Avrupa Birliği için yeni bir güvenlik konusu olarak belirtilen siber âlem, hibrit tehditlerin de öncelikli saldırı alanıdır (Eren, 2016: 51). Bu varsayımdan hareketle araştırmada cevap aranan soru hibrit tehditlere karşı Avrupa Birliği'nin savunma stratejisi nedir? Sorusudur. Bu soruya dair araştırmada test edilen temel hipotez Avrupa Birliği'nin hibrit tehditlerle büyük ölçüde siber güvenlik politikaları geliştirerek mücadele ettiğidir. Bu genel soru ve genel hipotez yanında araştırmada hibrit tehditlere karşı siber güvenliğin geliştirilmesinde nasıl bir hareket tarzı benimsenmektedir sorusuna cevap aranacaktır. Bu alt soruya dair test edilecek alt hipotez ise Avrupa Birliği'nin siber güvenlik politikalarını önlemede bilhassa aktörler arası istihbarat paylaşımı yöntemini tercih edip etmediğidir.

Bu araştırmada soruların cevaplanmasında ve hipotezlerin test edilmesinde nitel araştırma yöntemleri tercih edilmiştir. Bu tercihin altında nitel yöntemlerin, toplumsal bilimlerde ihtiyaç duyulan esnekliği karşılaması ve sosyal konularda genel durumun nitelenmesi hususunda kolaylık sağlaması yatmaktadır. Hipotezlerin test edilmesinde kullanılan bilimsel veriler kapsamlı bir literatür araştırması ile elde edilmiştir. Bu konudaki temel veri kaynağı olarak Avrupa Birliği'nce yapılan kurumsal açıklamalar, çalışma raporları ve alınan hukuki kararlar dikkatlice tasnif edilerek ve değerlendirilerek yerli literatüre de bu hususta ek bir katkı

yapılması hedeflenmiştir. Çalışmada öncelikli olarak birincil kaynaklara ulaşılarak güncel ve somut bilgilere yer verilmiştir. Belgesel kaynak incelemelerinde, daha önce yapılan çalışmalarda AB ve siber güvenlik politikalarının hibrit tehditler kapsamında değerlendirilmediği görülmüştür. Dolayısıyla bu çalışma, AB Çalışmaları disiplinindeki bu eksik yönleri güncel bilgilerle tamamlamak adına, gelecekte yapılacak araştırmalara katkıda bulunmayı hedeflemektedir

Bu çerçevede ilk başlık altında hibrit tehdit kavramı ele alınmaya çalışılmıştır. Kavramsal tanımlamanın ötesinde bu kısımda AB'nin hibrit tehdit tanımı nedir sorusu da cevaplanmaya çalışılmıştır. İkinci başlık altında ise AB'nin hibrit tehditlerle mücadele amacıyla yaptığı çalışmalar nelerdir, bu çalışmaların kapsamı nedir ve siber güvenlik ile hibrit tehditlerle mücadele arasında nasıl bir bağlantı vardır sorularına yanıt aranmıştır. Üçüncü başlıkta ise, hibrit tehditlerle öncelikli bir mücadele tercihi olarak benimsendiği söylenebilecek siber güvenlik politikalarının dayandığı Avrupa Birliği'nin Siber Güvenlik Kanun ele alınarak siber güvenlik anlamında hibrit tehditlerle mücadelede neler öngörülmüş, nasıl düzenlemeler geliştirilmiş sorularına yanıtlar ortaya konuşmaya çalışılmıştır.

2. HİBRİT TEHDİT KAVRAMI

Hibrit tehditler, çoğu zaman savaş olarak nitelenemeyen, ancak belirli amaçlara ulaşmak için devletlerin ya da devlet dışı aktörlerin hem savaş hem de barış zamanlarında kullanabildiği diplomatik, askeri, ekonomik, teknolojik vb. geleneksel ya da geleneksel olmayan metotların bir araya getirildiği, aynı zamanda da çeşitli şekillerde şiddet içeren ve yıkıcı eylemleri nitelemek için kullanılmaktadır (Giannapoulos, 2023). Barış dönemlerinde gerçekleştirilen suikastlar, casusluklar, topluma yönelik yapılan manipülasyonlar, dezenformasyonlar, ekonomik saldırılar, her türlü siber saldırılara kadar birçok örnek hibrit tehditlerin ne olduğu konusunda bize bilgi verebilir (Gressel, 2019). Hibrit tehditler terimi ile bir bakıma günümüz dünyasının etkili ve belki de öngörülemez saldırılarını nitelemektedir. Bir sınıflama yapmaya çalışacak olursak aslında üç tür hibrit tehditten bahsetmek mümkündür. Bunlardan birincisi devletlere yönelik olarak gerçekleştirilen, ekonominin kullanılarak demokratik toplumları baskılamak için kullanılan tehditlerdir. İkincisi, askeri olarak yapılan ve kurumları, ulaşım ağlarını, limanları, iletişim kanallarını etkileyen tehditlerdir. Üçüncüsü ise, en ucuz yöntemlerin kullanıldığı, toplumları kutuplaştırmayı ve zayıflatmayı amaçlayan, güvensizlik ve korku ortamı yaratan yasadışı teşebbüslerdir. Özellikle, sosyal bütünlüğün temel unsurlarından olan özgür ve adil seçimlere,

kritik altyapılara, Bilişim Teknolojilerine, haber ve bilgi güvenirliğine, mali işlemlere karşı yürütülen planlı saldırılardır (Shea, 2018: 6).

Hibrit tehditleri tanımlamak aslında oldukça güç bir iştir. Bu güçlüğün altında aslında iki sebep yatmaktadır denilebilir. Bunlarda birincisi bu tehdit yöntemlerinde kullanılan araçların gelişen teknoloji ile paralel bir şekilde her geçen gün değişmesi var farklılaşması gerçeği. İkincisi ise bu tehditlerin siyasi, ekonomik, askeri, sivil ya da siber, aynı zamanda da kasıtlı olarak demokratik devletlerin ve kurumların güçsüz taraflarını hedef alan eş güdümlü ve eş zamanlı eylemler olabilme olasılığıdır. Aynı zamanda hibrit tehditler, yerel, bölgesel veya kurumsal düzeyde ve hatta devlet içinde karar alma mekanizmalarını etkilemek ya da onlara zarar vermek amacıyla yapılan eylemler şeklinde de olabilirler. Özellikle hibrit tehditler bir ülkede genellikle yaşanmış olumsuzlukları, etkili olmayan yasal yapıyı, geçmişte başarısız olan uygulamaları, jeostratejik faktörleri, toplumda var olan güçlü kutuplaşmaları, ideolojik farklılıkları, teknolojik olarak geri kalmışlığı, kısacası güçsüzlükleri ve psikolojik olarak savunmasızlıkları hedef almaktadır (Hybrid Coe, 2023).

Diğer devletlerin ve uluslararası örgütlerin olduğu kadar hibrit tehditler, giderek artan oranda Avrupa Birliği'nin en kritik güvenlik sorunlarından birisi haline gelmektedir (Fiott & Parkes, 2019: 2). Bu çerçevede Avrupa Birliği'nin hibrit tehditlerle mücadele politikasının ilk adımı bu tehditlerin tanımlanmasına yönelik adımlar atılması şeklide olmuştur. Ancak Birlik, hibrit tehditlerin doğaları gereği tanımlarının değişiklik gösterdiğini ve devamlı gelişen doğalarına sabit, sınırlandırıcı bir tanımın karşılık veremeyeceğini kabul ederek bu konuyu ele almaktadır. Bu yaklaşımda yapılan ilk tanımlarından birisini 2016 yılında Avrupa Komisyonu tarafından hazırlanıp yayınlanan "2016 Hibrit Tehditlere Karşı Ortak Çerçeve" raporunda (2016 Joint Framework on Countering Hybrid Threats) yer almaktadır. Avrupa Birliği'ne göre hibrit tehdit kavramı geleneksel ve geleneksel olmayan (örneğin diplomatik, askeri, ekonomik, teknolojik) yöntemlerin bir karışımının zorlayıcı ve yıkıcı faaliyetlerde kullanılmasını ifade eder. Buna göre hibrit tehdit olarak kabul edilebilecek eylemler savaşa varmayan yöntemler olarak belli birtakım hedeflere ulaşmak için devletler veya devlet dışı aktörler tarafından yer yer koordineli bir şekilde gerçekleştirirler. Avrupa Birliği'ne göre hibrit tehditler genellikle hedefin açıklarının üzerine gitmeyi, toplum içinde belirsizlik yaratmayı ve karar verme süreçlerini engellemeyi hedefler. Siyasi söylemleri yönlendirmek veya radikalleştirmek, vekil aktörler kullanmak, kitlesel dezenformasyon için sosyal medyayı kullanmak gibi araçlar kullanılabilir (European

Commission, 2016a). Ancak hibrit tehditleri yine de ve bu şekilde basitçe nitelemek oldukça zordur. Çünkü bu tehditler, kritik ve hassas noktaları hedef alırken, aynı zamanda da etkili ve hızlı karar almayı engellemek için kargaşa ortamı yaratmaya çalışırlar ve tabiidir ki yöntemleri ve hedefleri konjonktüre göre her zaman değişmektedir (EEAS, 2018a).

Ancak yine de tanımlama konusundaki bu karmaşıklıktan şikayet etmek yerine hibrit tehditler karşısında AB ülkeleri ve kurumları, bir yandan teriminin içeriğini somutlaştırma konusunda adımlar atarken, aynı zamanda da bu tehditlerle nasıl mücadele edilmesi gerektiği konusunda çalışmalar yapmaktadırlar (Fiott & Parkes, 2019: 4). Birlik, Ortak Güvenlik ve Savunma Politikası (OGSP), Özgürlük, Güvenlik ve Adalet Alanları, son olarak da Güvenlik Birliği üzerine yapılan çalışmalarda hibrit tehditleri oldukça kritik bir konu olarak ele almaktadır (European Commission, 2017a). Avrupa Birliği hibrit tehditler ile mücadele adına farklı seviyelerde oldukça çeşitli politikalar üretmektedir. Üretilen bir politikalara alınan önlemlere bakıldığında, bunların çoğunlukla ve ilk etapta siber güvenlik alanında olduğu görülebilir. Yani diğer bir değişle hibrit tehditler Birliğe göre ağırlıklı olarak siber uzay üzerinden gerçekleşmektedir bir diğer ifadeyle AB'ye göre siber uzay hibrit tehditlerin temel hareket alanı olarak ele alınmalıdır (Eren, 2016: 51). Bu nedenle Birliğin siber güvenlik politikalarına hibrit tehditler gözlüğü ile bakmakta yarar vardır.

3. AVRUPA BİRLİĞİ'NİN HİBRİT TEHDİTLERLE MÜCADELE POLİTİKASI AÇISINDAN SİBER GÜVENLİK

Avrupa Birliği'nin siber güvenlik politikasının kurumsal yapılanması olarak 2004 yılında "AB Siber Güvenlik Ajansı" (ENISA) kurulmuştur. ENISA, iki ya da daha fazla AB üye ülkesini eşzamanlı etkileyen sınır ötesi siber olaylara müdahale edilmesine katkı sağlayan bir AB kurumudur. Avrupa Parlamentosu ve Bakanlar Konseyi Kararı ile kurulan özerk bir Birlik organı olarak ENISA, üye ülkelerle yakın iş birliği içinde, siber suçların hibrit tehditlerin aracı olarak kullanılmasına karşı, bu ülkelerin mücadele kapasitelerini artırmaya yönelik tavsiye ve çözümler üretmektedir ve uygulamaların takibinde de bulunmaktadır (ENISA, 2023). Kurulduğu dönemde hibrit tehdit kavramı henüz literatürde yer almadığından ENISA 2007 sonrası dönemde kademeli olarak siber güvenlik açısından hibrit tehditlere yönelik politikaların yürütülmesinde de aktif roller üstlenecektir.

2007 yılında "hibrit tehdit" kavramının da literatürde tanımlanmasının ardından 2009 yılında Kritik Bilgi Yapılarının

Korunması Üzerine Bildirim (CIIP) ile Birlik hibrit tehditlere karşı siber güvenlik politikalarını güncellemeye çalışmıştır. CIIP, AB'yi geniş çaplı siber saldırılardan ve yıkımlardan korumayı amaçlayan, bunu yaparken de güvenliği, hazır bulunurluğu ve hibrit tehditlere karşı toplum direncini artırmayı hedefleyen bir politika ilanı olarak tanımlanabilir. Bilgi ve iletişim teknolojisi yapıları olarak nitelenebilecek kritik bilgi yapılarının korunması üzerine yapılan bildirim, Birliğin CIIP'i hedef alan suç ve terör faaliyetlerini önlemek, onlarla mücadele etmek ve bu suçları yargıya taşımak için çalışan bir yapıya sahip olmasını öngörmektedir (Commission of the European Communities, 2009).

Bu konudaki bir sonraki adım AB Komisyonu ve AB Dış İlişkiler ve Güvenlik Politikası Yüksek Temsilcisi tarafından 2013'te Birlik için bir "Siber Güvenlik Stratejisi", ilan edilmesidir. Bu Strateji ile AB, çevrimiçi platformlarda Avrupa Birliği vatandaşlarının haklarını, güçlü ve etkin bir şekilde korumayı hedeflemiştir. Bunun yanında, siber uzayda yüksek risk alanlarının belirlenerek, bunlarla mücadelede özel eğitimlerin verilmesine odaklanan stratejiye göre, üye devletlerin savunma ve ulusal güvenlik çıkarlarını desteklemesi, bilgi ve iletişim sistemleri konusunda vatandaşların bilinçlendirmesi, bu suçlara karşı psikolojik direncin artırması da önemli bir faktör olduğu belirtilmiştir (European Commission, 2013).

2015 yılına gelindiğinde ise Birlik "Avrupa Güvenlik Gündemi"ni oluşturmuştur. Gündem ile AB'nin var olan güvenlik politikalarının etkinliğinin artırılması için, kilit öneme sahip beş ilke belirlenmiştir. Bunlardan birincisi, güvenlik ve temel hakların korunmasının birbirinin alternatifi gibi görülmemesi ve sanal âlemdeki hakların da aynı şekilde korunarak güvenlik önlemlerinin hayata geçirilmesidir. İkincisi, herkesin aynı oranda çevrimiçi platformlara ulaşabildiği, daha fazla açıklığın, ulaşılabilirliğin, demokratik kontrolün olduğu sanal bir özgürlük, güvenlik ve adalet alanının oluşturulmasıdır. Üçüncüsü, var olan Birlik hukuk kurallarının daha iyi bir şekilde uygulanabilir olduğunu garanti edilmesidir. Bu ilke ile AB, var olan bilgi paylaşım araçlarının tamamen kullanıldığı konusunda üye ülkelerin karşılıklı güven ortamının oluşturulmasına yardımcı olmaktadır. Dördüncüsü, AB'nin güvenliğin tüm kurumlar ve sektörler katılımı ile sağlanacağı yaklaşımının benimsemesidir. Bu ilke bir bakıma siber güvenliğin çok aktörlü ve çok boyutlu yapısının kabul edilerek onaylanmasıdır. Beşinci ve son ilkede, güvenliğin iç ve dış boyutlarının bir araya getirilmesine yer verilmiştir. Buna göre, güvenlik demek yalnızca, AB'nin dış sınırlarının güvenliği anlamına gelmemelidir

(European Commission, 2015). Ulusal sınırları olmayan siber uzayda tehditlerin de bir ulusal niteliği yoktur (Bilecka, 2019: 67). Güvenlik Gündemi bu sınırsız siber uzayda AB güvenliği için üç önemli öncelikli mücadele alanı belirlemiştir: terörle, organize suçlarla ve siber suçlarla mücadele (European Court of Auditors, 2019).

2016 yılı ise Avrupa Birliği'nin hibrit tehditlerle mücadele alt yapısı ve siber güvenlik stratejileri için adeta bir dönüm noktası olmuştur. Günümüzde var olan siber güvenlik yoluyla hibrit tehditlerle mücadele yaklaşımının kurumsal ve hukuksal temelleri bu sene içinde atılan pek çok adımla oluşturulmuştur denilebilir. Bu yıl içinde hibrit tehditlerle mücadele adına atılan ilk adım "AB Ağ ve Bilgi Güvenliği Direktifi" (NIS) olmuştur. AB Siber Güvenlik Stratejisi'nin bir parçası olan bu direktif, AB'nin kapsamlı siber güvenlik yasasının ilk aşaması olarak kabul edilebilir. Direktif, üç bölümden oluşmaktadır. Birincisi, ulusal mücadele kapasitelerinin artırılmasıdır. İkincisi, üye devletler arası ve birlik kurumları ile üye devletlerin kurumları sınır ötesi iş birliğinin geliştirilmesidir (European Parliament and Council, 2016a). Üçüncü bölümde ise kritik sektörlerin siber güvenlik açısından üye ülkeler tarafından izlenmesi gerektiği belirtilir (ENISA, 2016).

2016 yılında atılan ikinci adım ise "Hibrit Tehditlerle Mücadele Üzerine Ortak Çerçeve" metninin AB ve NATO tarafından kabulüdür. Ortak Çerçeve'nin amacı, AB ve üye ülkelerde hibrit tehditlerle mücadele etmek, bunu yaparken de hibrit tehditlerin hedefinde olan açıkları gidermek, psikolojik dayanıklılığı artırmak, krizleri önlemek ve yönetmek, bununla birlikte farkındalık oluşturmak ve NATO ile olduğu kadar diğer ortak örgütlerle de iş birliğinde bulunmaktır (European Commission, 2016b). Bu doğrultuda, yine hibrit tehditlerle etkili bir şekilde mücadele etmek için toplumların ve kritik yapıların dayanıklılığının (hem psikolojik hem teknik olarak) artırılması oldukça önemli bir adım olarak vurgulanmıştır (European Commission, 2016c). Ortak Çerçeve'de yer verilen Hibrit Füzyon Hücresi ise, devletlerin veya devlet dışı aktörlerin neden olduğu hibrit tehditlerle ilişkili güvenlik problemlerinin belirlenmesine yardımcı olan, aynı zamanda da AB'nin üye ülkelerle uyumlu çalışabilmesini sağlayan önemli bir çalışmadır. Çünkü, hibrit tehditlerle mücadelede etkili olabilmek için istihbarat ve bilgi paylaşımı oldukça gereklidir. Hibrit Füzyon Hücresi, üye devletler, Avrupa Dış İlişkiler Servisi (EEAS), AB Delegasyonları, AB Komisyonu ve diğer kurumları ile hibrit tehditlerle ilgili uyaranları çok önceden belirlemek, analiz etmek ve bilginin kaynağını bulmak için çalışır. Hibrit Füzyon Hücresi, AB İstihbarat ve Durum Merkezi (INTCEN)'in bir

parçası olarak kurulmuştur (European Commission, 2016a: 4). INTCEN, Hibrit Füzyon Hücresi'nin de AB'nin hibrit tehditlerle mücadeleyi siber güvenlik çalışmaları bağlamında ele aldığını gösteren bir politikadır. Şöyle ki, INTCEN üye ülkelerin hibrit tehditlere karşı güvenliğini medya, web siteleri, çevrimiçi bloglar, internet ağları gibi açık kaynaklardan elde ettiği bilgilere bağlı olarak sunduğu analitik raporlarla sağlamaktadır (EEAS, 2015). Dolayısıyla, yapılan istihbarat çalışmalarında artık ilk olarak siber uzaya başvurulmaktadır. Buradan elde edilen bilgilerle, hibrit tehditlerle mücadele edilmektedir. Ortak Çerçeve kapsamında yapılan diğer bir çalışma AB Hibrit Tehditlerle Mücadele Mükemmeliyet Merkezi'nin kurulmasıdır. Bu merkez, AB üyesi ülkelerin ve kurumlarının hibrit tehditleri önceden belirlemesi ve bunlara karşı bir savunma oluşturmasını amaçlamaktadır. Bu açıdan, alanında uzman kişilerden oluşan uluslararası bir yapısı vardır. Aynı zamanda, bu merkezin kuruluşunda AB ve NATO Ortak Bildirisi'nin uygulanması için bir dizi ortak hedef de belirlenmiştir (Hybrid CoE, 2023a). Bu noktada, siber savunma, stratejik iletişim, sivil ve askeri iş birliği, enerji ve kriz müdahalesi gibi alanlarda yakın iş birliği ile hibrit tehditlere karşı mücadele edilmesi amaçlanmıştır (European Commission, 2016a).

2016'da atılan üçündü adım ise Genel Veri Koruma Düzenlemesi'dir (GDPR) (European Commission, 2016d). Bu düzenleme siber uzayda şirketlerin ve kamu kurumlarının uyması gereken kuralları belirlerken, temel hak ve özgürlüklerin güçlendirilmesini amaçlamaktadır. Bununla birlikte GDPR, 1994 yılında yürürlüğe giren Avrupa Ekonomik Bölgesi Anlaşması (EEAA) ile de uyumludur (European Commission, 2018b). İnternet kullanımının artmasıyla birlikte hem kişisel verilere erişilmesi daha da kolay hale gelmiş hem de dezenformasyon yoluyla hibrit tehditlerin etki alanı artmıştır. Bu açıdan GDPR, özellikle hibrit tehditlerin hedefinde olan psikolojik dayanıklılığın en büyük düşmanı manipülasyonlar ve dezenformasyonlarla mücadelede, kişisel verilerin yanlış kullanımı ve doğru olmayan veri toplama eylemlerine karşılık önemli bir yaptırım mekanizması görevi görmektedir. Bu noktada verilen cezalar caydırıcı nitelikte olurken, bir şirketin yıllık cirosunun %4'ü kadardır. Bu da 20 milyon avrodan fazla olabilmektedir (Fiott & Parkes, 2019: 40).

2016'da atılan dördüncü adım Emniyet Yetkilileri Veri Koruma Direktifi'dir (European Parliament and Council, 2016b). Bu direktifin amacı, suç kurbanlarının, şahitlerin, şüphelilerin terörizm ve diğer suçlarda sınır ötesi iş birliği durumlarında emniyet yetkilileri tarafından kullanılan kişisel verilerinin güvenliğini sağlamaktır (European

Commission, 2018b). Buradan Veri Koruma Direktifi hibrit suçlarla mücadelede nasıl yardımcı olur? Sorusu akıllara gelebilir. Şöyle ki; AB'nin Güvenlik Gündemi, hibrit tehditlerle özellikle de terörizm, organize suçlar ve siber suçlarla mücadelesinde yeni bir strateji benimsemiştir. Bu strateji, hibrit tehditlerle mücadelede hem AB seviyesinde hem de uluslararası seviyede daha etkili olabilecek veri paylaşımını gerektiren aynı zamanda sınır ötesi güven ve yasal kesinliğini (hukuki güvenliği) sağlayacak bir çalışmadır. Bu süreçte ise hibrit tehditlerin belirlenmesi, soruşturulması, önlenmesi gibi aşamalarda zamandan ve paradan tasarruf edilirken, güçlü bir uluslararası iş birliği sağlanarak hem kişisel veriler korunmakta hem de daha etkili mücadele edilmektedir (Jourova, 2016).

2016'da atılan beşinci adım Yolcu İsim Kaydı Sistemi (PNR), sisteminin uygulamaya konulmasıdır. Terörist suçlarla birlikte diğer ciddi suçların kovuşturulmasında çok ciddi bir önleme, belirleme ve araştırma çalışması olarak belirtilen PNR, bu açıdan hibrit tehditlerle[4] de mücadele etmeyi amaçlamaktadır. PNR sistemi, uluslararası hava sahasında seyahat eden yolcuların, sadece kimlik bilgilerinin değil ayrıca iletişim bilgileri, kart bilgileri, uçuşlarının saati, bagaj numaraları ve sayısı, koltuk seçimleri, yanlarında varsa kişi sayıları ve hatta yolculuk esnasında yiyecekleri ve içecekleri her şeyi kayıt altına almaktadır (Ünal Sakallı, 2019: 93).

AB'nin hibrit tehditlerle mücadelesinde, bir önemli sene 2018 yılıdır. Bu yıl içinde ilk olarak ENISA, EDA, Europol Siber Güvenlik Merkezi (EC3) ve AB kurumları, ajansları ve organları için çalışan AB Bilgisayar Acil Durum Müdahale Ekibi (CERT-EU) arasında Mutabakat Antlaşması (MoU) imzalanmıştır. Bu anlaşma, imzalayan taraflar arasında bilgi paylaşım ağını güçlendirirken aynı zamanda ortak eğitim ve tatbikat çalışmalarını artırmayı ve iş birliği çerçevesi oluşturmayı amaçlamaktadır.

İkinci olarak ise, siber savunma konusunda ortak eğitim ve tatbikat çalışmalarını artırmak amacıyla Avusturya Savunma Bakanı, EDA ve NATO'nun Çokuluslu Kapasite Geliştirme Girişimi (MCDC), aynı yıl haziran ayında Ortak Güvenlik ve Savunma Politikası (OGSP) misyonu ve operasyonları ile uyumlu olan müşterek bir siber savunma planı oluşturmuş ve tatbikat düzenlemişlerdir. Avusturya'nın Walls-

[4] Verilen tehditlerin listesi, EUROPEAN PARLIAMENT and COUNCIL, "Directive on Passenger Name Record", 2016, s. 18, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0681&from=EN (Erişim Tarihi: 08.10.2019).

Siezenheim şehrinde yapılan bu planın son şekli "Siber Falanks 2018"dir. Siber Falanks 2018, hem AB'nin hem de üye ülkelerin, somut siber tehditlerle mücadele kapasitesini artırmayı, birlikte çalışabilirliği sağlamayı, siber tehditlere karşı dayanıklılığı (resilience)[5] artırmayı, bununla birlikte yapılan operasyonlarda ve misyonlarda siber durum farkındalığının kritik öneminin anlaşılmasını amaçlamaktadır (EDA, 2018).

Üçüncü olarak bu yol içinde "AB Hibrit Tatbikatı" adıyla önemli bir sivil-askeri kriz yönetim tatbikatı daha oluşturmuştur. Bu tatbikatla birlikte, siber ve enerji kaynaklı olmak üzere ODGP için kritik olan iç ve dış güvenlik konuları ile bağlantılı hibrit tehditlere karşı birçok AB kurumu ve organı sözde kriz yönetim senaryolarına karşı bir araya gelmiştir. AB'nin yapmış olduğu bu tatbikat, NATO'nun yürüttüğü Paralel ve Eşgüdümlü Tatbikat olan PACE'e benzer niteliktedir ve onun güdümünde gerçekleşmiştir (Fiott & Parkes, 2019: 40). Avrupa Birliği, ilk defa bu ölçüde bir tatbikat ile kriz yönetimini ele almıştır. AB Entegre Siyasi Kriz Müdahale Mekanizması (IPCR), AB Sivil Koruma Mekanizması gibi mevcut tüm kriz mekanizmalarını kullanarak ciddi bir hibrit tehditle karşı karşıya olan hayali ülkeye yardımda bulunma kapasitelerini test etmişlerdir (EEAS, 2018c).

Dördüncü olarak 2018 yılı içinde Çevrimiçi Dezenformasyonlarla Mücadele Bildirimi, yayınlanarak AB vatandaşlarının çevrimiçi platformlardan yayılan dezenformasyonlara karşı toplum bilincinin artırılmasını, bu amaçla da bazı ilke ve amaçların belirlenerek, AB Komisyonu'nun bu bağlamda ele aldığı diğer spesifik önlemlere de rehber olmayı hedeflenmiştir (Fiott & Zeiss, 2019). Bu Bildirim ile ayrıca, vatandaşlar ve üçüncü ülke vatandaşları ile görüşmeler yapılarak geliştirilmiş olup, 2017 yılında oluşturulmuş olan Yüksek Seviye Uzman Grubu (HLEG) tarafından verilen tavsiyelerle de desteklenmektedir. Bu doğrultuda HLEG, 2018 yılında bir rapor yayınlamıştır (European Commission, 2018c). Bu rapora göre, sunulan analizlerle dezenformasyonu anlamamıza yarayan "sahte haberler" teriminin açıklaması yapılmıştır (European Commission, 2019a). Bununla birlikte, Avrupa haber medyası ekosisteminin çeşitliliğinin ve sürdürülebilirliğinin korunması, aynı zamanda da gerekli mücadelenin verilebilmesi için farklı aktörler tarafından alınan önlemlerin Avrupa'da değerlendirilmesini sağlayacak dezenformasyonların etkisi üzerine araştırmaların devam ettirilmesi gerektiğini belirtmektedir (European Commission).

[5] Burada geçen siber tehditlere karşı dayanıklılık (resilience) kavramı, psikolojik olarak güçlülüğü ve direnci ifade etmektedir.

Avrupa Birliği'nin uzun dönem proje temelli bir güvenlik yapılanması olan PESCO kapsamında da hibrit tehditlere karşı siber güvenlik çalışmaları yaptığını belirtmek gerekir. Özellikle PESCO ve AB ile NATO iş birliğindeki Hibrit Tehditlerle Mücadele Mükemmeliyet Merkezi günümüzde meydana gelen ve kademeli olarak artan aynı zamanda da değişen hibrit tehditlere karşı birlikte hareket eden çalışmalardır (EuropeNow Journal, 2018). PESCO'nun hibrit tehditlerle mücadele çalışmaları kapsamında değerlendirilebilecek olan Siber Tehditler ve Olaylara Müdahale Bilgi Paylaşım Platformu (PESCO Projects) üye ülkelerden oluşan istihbarat paylaşımını öngören bir internet platformudur. Bir diğer çalışma, yine internetin kötü amaçlarla kullanılmasını önlemeyi amaçlayan, Siber Güvenlik için Acil Müdahale ve Müşterek Yardım Ekipleri (CRRT) (PESCO Projects) ile üye ülkelerin ortak çalıştığı siber savunmanın güçlendirilmesi çalışmasıdır. Hibrit tehditlerle siber tehditlerin iç içe geçmiş yapısı bir dizi kapsamlı taktikle mücadeleyi gerektirmektedir. Bu açıdan CRRT Litvanya'nın öncülüğünde diğer sekiz AB üyesi ülke, Estonya, İspanya, Hırvatistan, Polonya, Hollanda, Fransa, Romanya ve Finlandiya'nın siber savunma alanında üye ülkeler arasında uzmanların bir araya getirilmesini amaçlamaktadır (Dowdall, 2019). Hibrit tehditlerin doğasının öngörülemez olduğu düşünüldüğünde yapılan bir diğer PESCO projesi, AB Askeri Uzay Gözetim Farkındalık Ağı olan EU-SSA-N'dır. Hatta belki de AB'nin hibrit tehditlerle mücadelede vizyonunun çok kapsamlı olduğunu gösteren bu çalışma, uzaydan gelebilecek hibrit tehditlere karşı geliştirilecek ve teknolojinin gelişmişliğinden son derece faydalanılacak uygun servislerin geliştirilmesini amaçlamaktadır (Ünal Sakallı, 2019: 133).

Anlaşılmaktadır ki Birlik açısından hibrit tehditlerle mücadelede öncelikli alan siber uzaydır. Bu nedenle Avrupa Birliği'nin siber güvenlik konusunda atmış olduğu ve politikalarının temelini oluşturan gelişmeye ayrı bir başlık açmakta yarar olduğuna inanmaktayız.

4. AVRUPA BİRLİĞİ SİBER GÜVENLİK KANUNU

Hibrit tehditler hem geleneksel hem de geleneksel olmayan eylemlerin bir araya geldiği, aynı zamanda da belirli siyasi amaçları başarmak amacıyla devletlerin ya da devlet dışı aktörlerin kullandığı bir yöntemdir. Bunun yanı sıra, hibrit eylemler politika oluşturma süreçlerini etkilemeyi, toplumları zayıflatmayı ve AB'nin bütünlüğünü baltalamayı amaçlamaktadır. Bunları gerçekleştirirken de hibrit tehditler, siber saldırıları, dezenformasyon kampanyalarını ve seçimlere müdahale etme yollarını kullanmaktadır (EU2019FI, 2019). Bu açıdan AB, hibrit

tehditlerle mücadele ederken siber güvenlik konusunu gündeminde tutmaktadır.

Siber Güvenlik Kanunu'na kadar geçen süreçte yaşananlar kronolojik olarak ele alındığında ilk olarak 2014 yılında, AB ve Batı dünyasına karşı Rusya'nın sergilemiş olduğu saldırgan tutum ve Kırım'ı ilhak etmesi, AB çapında bir korku yaratmıştır. Bunun yanı sıra Türkiye'nin IŞİD'in eylemlerine maruz kalması, AB'nin hem bu olayların topraklarına sıçraması konusundan endişelerini artırmıştır. AB bu amaçla hareket ederken, tam da hibrit tehditlerin doğasına uygun bir şekilde siber güvenlik konusunda da somut iyileştirme adımları atması gerektiğini düşünmeye başlamıştır. Yani bir yandan sosyal medya araçlarının ve internet ağlarının teröristlerce kullanılarak, yaptıkları eylemlerin AB topraklarına yöneleceği düşüncesi ile, diğer yandan da Birlik vatandaşlarının internet ortamı üzerinden siyasi radikalleştirilmesi amacıyla kullanılacağı korkusu ile siber güvenlik konusunu gündeme almıştır (European Commission, 2017b).

2015 yılına gelindiğinde, AB Bakanlar Konseyi tarafından kabul edilen "Siber Diplomasi" kararları ile (Council of the European Union, 2015), AB ve üye ülkelere siber güvenlik kapsamında özgürlük, güvenlik ve refahın sağlanmasına uygun hareket edilmesini bağlayıcı şekilde kararlaştırmıştır. Bu bağlamda özellikle siber suçlarla mücadele, kapasite geliştirme, hükümet ve kritik altyapı sistemlerinin ve ağlarının korunması, uluslararası iş birliği, dijital pazarda rekabet edebilirlik, insan haklarının devamlılığı, kilit ortaklarla stratejik anlaşmaların yapılması ve internet yönetimi gibi konularda AB ve üye devletlere önemli sorumluluklar yüklenmiştir. 2017 yılında siber güvenlik konusunda aldığı kararla AB Bakanlar Konseyi mücadelenin ulusal değil küresel seviyede sürdürülmesinin gerekli olduğunun altını çizmiştir. Bu açıdan aynı yıl AB Bakanlar Konseyi, Kötü Niyetli Siber Eylemlere Karşı AB'nin Ortak Diplomasi Tepki Stratejisi ile "kötü niyetli siber eylemler, hibrit tehditler bağlamında değerlendirilmelidir" sonucuna ulaşılmıştır (Council of the European Union, 2017).

2018 yılında ise yine AB Bakanlar Konseyi, Siber Diplomasi Takımının pratikte kullanımına katkı sağlayacak aynı zamanda da siber saldırılarla mücadelede ek çalışmaların yapılmasına yardımcı olacak hibrit tehditlerle mücadele kapasitesini artırmayı hedefleyen, kötü niyetli siber eylemler üzerine bir sonuç bildirgesi kabul etmiştir. Bu bildirge, AB'nin ODGP kapsamında kötü niyetli siber eylemleri önleme ve bunlarla mücadele etme kapasitesini artıran kısıtlayıcı tedbirler oluştururken aynı zamanda da siber alemde yaşanan çatışmaları

önlemeyi, bu konuda iş birliği sağlamayı ve Birlik içinde istikrarın devamlılığını amaçlamaktadır (Council of the European Union, 2018).

2019 yılı mayıs ayına gelindiğinde AB Bakanlar Konseyi, hem Birlik üyesi devletleri hem de AB'yi tehdit eden ve hibrit tehditlerden biri olarak değerlendirilen siber saldırılara karşılık verilmesi için, gerekli yasal düzenlemelerin çerçevesini çizen bir taslak kabul etmiştir (European Parliament, 2019). 2019 yılı haziran ayında nihayet bu taslak düzenlenmiş ve Siber Güvenlik Kanunu olarak kabul edilmiştir. Bir tür düzenleme metni olan ve kanun (act) olarak adlandırılan bu metin, esasında ENISA'nın güncellenmesi anlamına gelmektedir. Bu düzenleme ile, öncelikli olarak siber güvenliğin sadece teknoloji ile ilgili bir konu olmadığı, aynı zamanda da insan davranışlarının önemli olduğu bir alan olduğunun altı çizilmektedir. Bu açıdan siber saldırılar, daha güçlü savunma gerektiren tehditlere ve saldırılara karşı savunmasız olan ekonomi ve topluma bağlı olarak gerçekleşmektedir. Ancak, siber saldırılar sınırlar ötesi meydana gelebilen tehditler olduğu için, siber güvenlik uzmanları ve emniyet yetkililerinin kabiliyetleri ve bu tehditlere verilen siyasi yanıtlar çoğunlukla ulusaldır. Bu yüzden, geniş çaplı olaylarda bazen Birlik hükümleri yıkılabilir, dolayısıyla Birlik seviyesinde etkili ve koordineli bir kriz yönetimi gerekir. Dahası, politika oluşturucular için de Birlik'in psikolojik açıdan zorlukları yenme gücü ve üye devletlerin siber güvenliklerinin düzenli olarak değerlendirilmesinin yapılması da oldukça önemlidir. Siber Güvenlik Kanunu'nda, siber güvenlik alanında ulusal kapasiteyi artırmak için gerekenler belirlenirken ilk olarak, üye ülkeler arasında stratejik ve operasyonel düzeyde iş birliğini geliştirecek mekanizmaların kurulması gerektiği belirtilmiştir. Sonrasında, enerji, ulaşım, içme suyu tedariki ve dağıtımı, bankacılık, mali pazar altyapıları, sağlık ve dijital altyapı sektörlerine yönelik güvenlik önlemlerinin alınması konusunda üye devletlerin yükümlülüklerinin olduğu vurgulanmıştır (European Parliament and the Council, 2019). Bu noktada, doğrudan bahsedilmemiş olsa da siber güvenlik sadece siber alemin güvenliğine ve oradan gelebilecek tehditleri önlemeye yönelik olarak değil, hibrit bir tehdit olarak diğer alanlarında güvenliğini ve oluşturabilecekleri tehditleri çok daha kapsamlı olarak ele almak amacıyla oluşturulmuştur.

2019 yılından bu yana, yani Siber Güvenlik Kanunu yürürlüğe girdiğinden beri ENISA, Dijital Tek Pazar'ı destekleyen ürünlerin ve hizmetlerin belgelendirilmesine temel oluşturmayı amaçlayan bir Avrupa Siber Güvenlik Sertifika Programı hazırlamakla görevlendirilmiştir. Ancak ENISA zaten, ağ ve bilgi sistemlerinin güvenliği ile ilgili

konularda AB politikalarının ve kanunlarının geliştirilmesini ve uygulanmasını desteklemektedir (ENISA). Bu açıdan kısacası, ENISA'nın hibrit tehditlerle mücadelede sorumluluklarının kapsamı bu kanun ile genişletilmiştir. ENISA uygulamalar konusunda da üye ülkeleri desteklemektir. Bununla birlikte, siber tehditler küresel bir konudur. Dolayısıyla ENISA, siber güvenlik standartlarının geliştirilmesi, ortak küresel yaklaşımın benimsenmesi, uluslararası standartların kullanılması, bilgi paylaşımının artırılması için üçüncü ülkelerle iş birliği yapmaktadır. Hatta bu bağlamda üçüncü ülkelerin katılımına da açıktır. Ancak ENISA'nın, tam anlamıyla amaçlarına ulaşabilmesi için ilgili AB yönetsel yetkilileri, CERT-EU, EC3, EDA, Avrupa Küresel Navigasyon Uydu Kurumu (GNSS), Elektronik İletişimciler için Avrupa Düzenleyiciler Kurumu (BEREC), Avrupa Bankacılık Otoritesi (EBA), Avrupa Merkez Bankası (ECB), Avrupa Veri Koruma Kurumu, Avrupa Enerji Düzenleyicileri Kurumu (ACER), AB Havacılık Güvenliği Kurumu (EASA), Avrupa Birliği, Özgürlük, Güvenik ve Adalet Alanında Büyük Ölçekli Bilişim Teknolojileri Sistemlerinin Operasyonel Yönetimi Kurumu (eu-LISA) ve siber güvenlikle ilgili AB'in diğer kurum ve organları ile birlikte hareket etmesi gerektiği belirtilmiştir (European Parliament and the Council, 2019). Bununla birlikte, bahsedilen tüm bu kurumlar hibrit tehditlerle siber güvenlik çalışmaları doğrultusunda mücadele etmektedir. Siber Güvenlik Kanunu da hibrit tehditlerle siber güvenlik çalışmaları kapsamında mücadele ettiğini vurguladığımız, NIS Direktifi'ni desteklemekte, Ortak Çerçeve'yi güçlendirme yolları aramakta ve GDPR'nin çalışmalarını AB ülkelerinde daha etkili bir şekilde uygulamaktadır (Reuters, 2019: 1). Dolayısıyla, AB'nin hibrit tehditlerle büyük ölçüde siber güvenlik politikaları geliştirerek mücadele ettiğini söylemek mümkündür.

5. SONUÇ

Hibrit tehditler giderek artan oranda ulusal ve uluslararası güvenliğe yönelik ilk tercih edilen tehditler arasında üst sıralara yükselmektedir. Konvansiyonel tehditler artık yenilikçi güvenlik tehditleri ile harmanlandığı adeta desteklendiği oranda etki yaratmaktadır denilebilir. Bu hibrit tehditleri mümkün kılan ve her geçen gün güvenliğe yönelik risk olma potansiyelini artıran faktör ise her alanda yaşanan dijitalleşme ile insan hayatının adeta siber uzaya kademe kademe taşınmasıdır.

Artık insanlar siber uzayda sosyalleşmekte, siber uzayda finansal varlıklarını muhafaza etmekte, siber uzay üzerinden iletişim kurmakta, siber uzay üzerinden belli oranda diplomatik faaliyetler yürütülmekte,

terörizm eylemleri gerçekleştirilmekte ve hatta savaşlarda belli oranda ve yöntemlerle siber uzay üzerinden saldırılar gerçekleştirilmektedir. Öyle ki savaşlarda silahlar internet ve siber uzay üzerinde uzaktan yönetilebilirken savaş sırasında veya başka zamanlarda internet üzerinden saldırılar da gerçekleştirilmektedir. Diğer bir değişle yaşadığımız hayatta herkesin şu ya da bu şekilde bir dijital ayak izi de bulunmaktadır. İşte bu durum konvansiyonel güvenlik tehditleri arasına siber tehditlerin de eklenmesini doğurmaktadır.

Günümüzde, teknoloji artık uzaktan kontrollü kumandalar gibi yaşantımızı yönlendirmekte, hatta kullandığımız her cihaz birilerinin bizi uzaktan izlemesini mümkün kılmaktadır. Hatta ve hatta bizim işimizi kolaylaştırdığını düşündüğümüz e-banka, e-ticaret ve daha birçok "e" ön ekli (çevrimiçi) hizmetler giderek yaygınlaşmaktadır. Tüm bu hizmetler ise kişilerin, şirketlerin, kurumların ve devletlerin dahi verilerinin elimizdeki cihazlarla bu mobil servis merkezlerine akışı anlamına gelmektedir.

İşte bu nedenle Avrupa Birliği konvansiyonel tehditlerin yanında yeni tür tehditlerin kullanılması olarak nitelenebilecek "hibrit tehdit" kavramını öncelikli olarak dijital-siber tehditler olarak tanımlayarak çalışmalarına buradan başlamıştır. Bu nedenle Avrupa Birliği'nin hibrit tehditler ile mücadele politikasını hali hazırda ve öncelikle siber güvenlik politikalarının güçlendirilmesi olarak tanımlamış ve politikalarını bu yönde güçlendirici adımlar atmıştır.

Bu şekilde hibrit tehditler ile mücadele politikası olarak siber güvenliğin güçlendirilmesine odaklanan Avrupa Birliği, siber güvenliğin güçlendirilmesinde birtakım ilkeler ve yaklaşım tarzları belirleyerek hareket etmiştir. Bu noktada AB siber güvenliğin çok aktörlü ve çok boyutlu niteliğinin farkında olarak üye devletlerle sıkı bir iş birliği içinde çalışmanın ötesine geçerek NATO ile ve diğer devletler ile de iş birlikleri yaparak meseleye, tehdidin özüne uygun bir şekilde küresel olarak yaklaşmıştır.

Ayrıca Birlik siber güvenliğin temininde istihbaratın önemine vurgu yaparken bunun temel haklara ve özgürlüklere saygı gösterilerek yapılması gerektiği hususunda bir tavır geliştirmiştir. Bu çerçevede hibrit tehditler ile mücadelede siber güvenliğin güçlendirilmesine yönelik politikaları hayata geçirilirken göz ardı edilmemesi gereken husus insanların gerçek hayatlarında olduğu gibi siber uzayda da haklarına ve özgürlüklerine saygı gösterilmesi gerektiğinin altı çizilmiştir. Bu manada Avrupa Birliği'nin hibrit tehditler ile mücadelede güvenliğin insan hakları boyutunu da göz ardı etmediğini söylemek mümkündür.

Ancak bu çalışmada ele alınmaya çalışılan husus birliğin hibrit tehditler konusunda güvenlik alt yapısını nasıl oluşturduğudur. Oluşan bu alt yapı hibrit tehditlerin doğasına uygun bir şekilde değişmektedir. Tehditlerin değişken doğası gereği hibrit tehditler ile mücadele politikaları ve stratejileri de değişkendir. Göründüğü şekliyle siber dünyanın sınırsız hizmetleri gelecekte de durdurulamayacak bir hâl almaktadır. Bu da siber temelli hibrit tehditlerin de genişleyeceği ciddiyetini artıracağı şeklinde yorumlanmalıdır. Bu açıdan Avrupa Birliği, gelecekte belki de OGSP kapsamında daha çok oranda siber güvenlik önlemeleri üzerine politikalar üreten bir yapı haline gelecektir.

KAYNAKÇA

Bilecka, R. (2019). Creating a Safer World of Tomorrow. *European Cybersecuirty Journal, 5*(1), 66-68.

Commission of the European Communities. (2009, 03 30). *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* 10 08, 2019 tarihinde Eur-lex: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF adresinden alındı

Council of the European Union. (2015, 02 11). *Council Conclusions on Cyber Diplomacy (6122/15)*. 11 08, 2019 tarihinde data.consilium.europa.eu: https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf adresinden alındı

Council of the European Union. (2017, 10 09). *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (13007/17)*. 11 09, 2019 tarihinde data.consilium.europa.eu: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf adresinden alındı

Council of the European Union. (2018, 04 16). *Council conclusions on malicious cyber activities (7925/18)*. 11 09, 2019 tarihinde data.consilium.europa.eu: https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf adresinden alındı

Dowdall, B. (2019). *Cyber and Hybrid Threats to Canada and Its Allies.* Hot Topics in Security and Safety. Canada: The Conference Board of Canada.

EDA. (2018). *CYBER PHALANX 2018 to Enhance Cyber Resilience of CSDP Mission*. 10 06, 2019 tarihinde eda.europa.eu: https://eda.europa.eu/news-and-events/news/2018/05/31/cyber-phalanx-2018-to-enhance-cyber-resilience-of-csdp-missions adresinden alındı

EDA. (2018, 06 28). *Six Member States agree to pool & share cyber ranges capabilities*. 10 15, 2019 tarihinde da.europa.eu: https://eda.europa.eu/news-and-events/news/2018/06/28/six-member-states-agree-to-pool-share-cyber-ranges-capabilities adresinden alındı

EEAS. (2015). *EUINTCEN - Intelligence and Anaysis Centre.* Fact Sheet.

EEAS. (2018a). *A Europe that Protects: Countering Hybrid Threats.* Factsheets, Bruxelles.

EEAS. (2018b, 02 14). *ESDC: Cyber platform for education, training, evaluation and exercise (ETEE)*. 10 09, 2019 tarihinde https://www.eeas.europa.eu/: https://www.eeas.europa.eu/node/39848_en adresinden alındı

EEAS. (2018c, 11 16). *Crisis preparedness: EU launches civil-military crisis management exercise*. 10 17, 2019 tarihinde www.eeas.europa.eu: https://www.eeas.europa.eu/node/53926_en adresinden alındı

ENISA. (2016). *NIS Directive*. 10 22, 2019 tarihinde https://www.enisa.europa.eu/: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new adresinden alındı

ENISA. (2023). *About ENISA - The European Union Agency for Cybersecurity*. 01. 02. 2023 tarihinde https://www.enisa.europa.eu/: https://www.enisa.europa.eu/about-enisa adresinden alındı

Eren, M. (2016). *Avrupa Birliği'nin Siver Güvenlik Politikası.* İstanbul: Marmara Üniversitesi.

EU2019FI. (2019). *General Background: Long – Term Challenge for the EU's societies and for Unity*. 11 15, 2019 tarihinde https://eu2019.fi/en/priorities/comprehensive-security/hybrid-and-cyber-threats adresinden alındı

European Commission. (2013, 02 07). *Cyber Security of the European Union: An Open, Safe and Secure Space.* 10 11, 2019 tarihinde

eeas.europa.eu: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf adresinden alındı

European Commission. (2015, 04 28). *The European Agenda on Security*. 10 08, 2019 tarihinde cepol.europa.eu: file:///C:/Users/Hp-Pc/Downloads/european-agenda-security.pdf adresinden alındı

European Commission. (2016a). *Joint Framework on countering hybrid threats a European Union response*. JOIN(2016) 18 final, Brussels.

European Commission. (2016b, 05 06). *Security: EU strengthens response to hybrid threats*. 10 25, 2019 tarihinde ec.europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1227 adresinden alındı

European Commission. (2016c, 04 06). *FAQ: Joint Framework on countering hybrid threats*. 10 26, 2019 tarihinde https://ec.europa.eu/: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250 adresinden alındı

European Commission. (2016d, 04 27). *General Data Protection Regulation - 2016/679*. 11 03, 2019 tarihinde eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679 adresinden alındı

European Commission. (2017a). *Joint Communication on Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*. JOIN/2017/0450 final. Brussels: Eur-lex.

European Commission. (2017b, 09 13). *Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (C(2017) 6100 final)* . 11 08, 2019 tarihinde home-affairs.ec.europa.eu: https://home-affairs.ec.europa.eu/pages/document/commission-recommendation-coordinated-response-large-scale-cybersecurity-incidents-and-crises-c2017_en adresinden alındı

European Commission. (2018a, 06 13). *Increasing resilience and bolstering capabilities to address hybrid threats*. 11 05, 2019 tarihinde www.eeas.europa.eu: https://www.eeas.europa.eu/sites/default/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf adresinden alındı

European Commission. (2018b, 04 26). *Communication - Tackling online disinformation: a European approach*. digital-strategy.ec.europa.eu: https://digital-strategy.ec.europa.eu/en/library/communication-tackling-online-disinformation-european-approach adresinden alınmıştır

European Commission. (2018c, 05 23). *Fundamental Rights.* 11 03, 2019 tarihinde commission.europa.eu: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en adresinden alındı

European Commission. (2019, 05 29). *A Europe that Protects: Good Progress on Tackling Hybrid Threats*. 11 23, 2019 tarihinde ec.europa.eu: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788 adresinden alındı

European Commission. (2019a). *Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (SWD (2019) 200).* ESO.

European Commission. (tarih yok). *Final Report of the High Level Expert Group on Fake News and Online Disinformation*. 10 02, 2019 tarihinde wayback.archive-it.org: https://wayback.archive-it.org/12090/*/https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation adresinden alındı

European Court of Auditors. (2019). *Challenges to effective EU cybersecurity policy.* Briefing Paper.

European Parliament. (2019, 10 21). *Parliamentary Questions (E-001323/2019)*. 11 08, 2019 tarihinde www.europarl.europa.eu: https://www.europarl.europa.eu/doceo/document/E-8-2019-001323-ASW_EN.pdf adresinden alındı

European Parliament and Council. (2016a, 07 19). *Directive on Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union.* 10 08, 2019 tarihinde Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN adresinden alındı

European Parliament and Council. (2016b, 05 04). *General Data Protection Regulation (2016/679).* 10 08, 2019 tarihinde eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 adresinden alındı

European Parliament and Council. (2016c, 04 27). *Directive on Passenger Name Record (PNR).* (O. J. Union, Dü.) 10 08, 2019 tarihinde eur-lex.europa.eu: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0681&from=EN adresinden alındı

European Parliament and the Council. (2019, 06 07). *Cybersecurity Act*. 11 09, 2019 tarihinde Official Journal of the European Union: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN adresinden alındı

EuropeNow Journal. (2018, 11 2). *Global Hybrid Threats and European Security in the Age of Trump, Growing Populism, and International Terrorism*. 11 20, 2019 tarihinde https://www.europenowjournal.org/: https://www.europenowjournal.org/2018/11/07/global-hybrid-threats-and-european-security-in-the-age-of-trump-growing-populism-and-international-terrorism/ adresinden alındı

Fiott, D., & Parkes, R. (2019). *Protecting Europe: The EU's Response to Hybrid Threats.* Luxembourg: European Union Institute for Security Studies (EUISS).

Fiott, D., & Zeiss, M. (2019). *Yearbook of European Security*. Paris: European Union Institute For Security Stuides (ISS).

Giannopoulos, G. (2019). *Introduction to the concept of Hybrid Threats*. 01 10, 2023 tarihinde www.ee-isac.eu: https://www.ee-isac.eu/introduction-to-the-concept-of-hybrid-threats/ adresinden alındı

Gressel, G. (2019). Protecting Europe Against Hybrid Threats. (ECFR/289). (E. C. Relations, Dü.)

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington, Virginia: Potomac Institute for Policy Studies.

Hybrid CoE. (2023). 09 27, 2019 tarihinde https://www.hybridcoe.fi/: https://www.hybridcoe.fi/ adresinden alındı

Hybrid Coe. (2023a). *Hybrid Threats as a Phenomenon*. 07 18, 2021 tarihinde hybridcoe.fi: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon adresinden alındı

Jourova, V. (2016). *How will the data protection reform help fight international crime.* European Commission.

PESCO Projects. (tarih yok). *Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT)*. 11 21, 2019 tarihinde www.pesco.europa.eu: https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/ adresinden alındı

PESCO Projects. (tarih yok). *Cyber Threats and Incident Response Information Sharing Platform (CTIRISP)*. 11 21, 2019 tarihinde https://www.pesco.europa.eu/: https://www.pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/ adresinden alındı

Portman, G. (2018). Managing the Threat: Foresight, Crisis Management and Damage Control. I. Andre, & R. Areanella içinde, *Hybrid and Transnational Threats* (s. 39-43). Friends of Europe.

Reuters, T. (2019). *Expert Q&A on the EU Cybersecurity Act.* Covington.

Sakallı, Ü. (2019). *Uluslararası Terörizmle Mücadele Bağlamında Avrupa Birliği'nin Ortak Dış ve Güvenlik Politikası.* Isparta: Süleyman Demirel Üniversitesi.

Shea, J. (2018). I. Andre, & R. Areanella içinde, *Hybrid and Transnational Threats.* Friends of Europe.