AYTUĞ, K. H. – İ. F. POZAN (2023). "Gelişen Hibrit Savaş Ortamında NATO-AB İş Birliği".
***Karadeniz Araştırmaları*. XX/77: 1-27.**

GELİŞEN HİBRİT SAVAŞ ORTAMINDA NATO-AB İŞ BİRLİĞİ

H. Kutay AYTUĞ[*]
İ. Fatih POZAN[**]

ÖZ

İnsanlık tarihi boyunca politik, askerî, siyasi, ekonomik ve diğer nedenlerle mücadele alanları oluşmuştur. Bu mücadele alanları kimi zaman savaşlara dönüşmüştür. Teknolojinin gelişmesi ve küreselleşme savaşan aktörlerin ve yöntemlerin de değişmesine neden olmuştur. Özellikle, İkinci Dünya Savaşı'ndan sonra, devletlerin ana aktör olarak görev aldıkları güvenlik ortamı yerini çok aktörlü (askerî birlikler, terörist unsurlar, yabancı savaşçılar, organize suç örgütleri vb.), daha az maliyetli ve istenen sonuca daha az sürede ulaşmayı amaçlayan, bulanık, hibrit savaş ortamına bırakmıştır. Bu çalışmanın amacı, hibrit savaş olgusunun Avrupa Birliği (AB) ile NATO iş birliğine etkisini incelemektir. Bu kapsamda çalışmada ilk önce hibrit savaş olgusu açıklanmıştır. Daha sonra, tarihsel arka planı, hibrit savaşın getirmiş olduğu değişimler, hibrit savaş ve Rusya örnekleri üzerinden anlatılmıştır. İzleyen bölümde AB'nin hibrit tehditlere yanıtı incelenmiştir. Daha sonra, hangi faaliyet alanlarında iş birliğinin artırıldığı incelenmiştir. İzleyen değerlendirme bölümünde iş birliği alanı NATO ve AB'nin yayımladığı raporlar, belgeler çerçevesinde incelenmiş, sonuç bölümünde bulguların değerlendirilmesi yapılmıştır. Yapılan inceleme sonucunda, gelişen hibrit savaş ortamında NATO ve AB'nin birbirinin alternatifi değil, aksine tamamlayıcısı olduğu ve NATO'nun tehditlere karşı kullanabileceği sert gücü ile ön plana çıkarken, AB'nin daha çok yumuşak gücü ile ön plana çıktığı değerlendirilmiştir.

Anahtar Kelimeler: Hibrit Savaş, Hibrit Tehditlere Karşı AB'nin Yanıtı, AB-NATO İş birliği.

NATO-EU COOPERATION IN THE EMERGING HYBRID WARFARE ENVIRONMENT

ABSTRACT

Throughout the history of humanity, there has always been political, military, economic strife. That sometimes has turned into full-scale war. Advances in technology coupled with globalization changed who goes to war and how. Following World War II, the security environment in which states have been main actors have led to emergence of a hybrid warfare environment in which multiple actors (e.g. military units, terrorists, foreign fighters, organized crime units) are used to reach the goal faster, and for cheaper. In this study, we shall attempt to examine the effects of hybrid warfare on the cooperation between the European Union (EU) and NATO. First, we well talk about the phenomenon of hybrid warfare, followed by its historical background and the changes it has sparked – particularly in the case of Russia. Next, we will explore the EU's response to hybrid threats. Third, we will look cooperation and reports published by NATO and the EU on the matter. Our preliminary findings indicate that NATO and the EU are not alternatives of but rather complementary to one another in the ever-evolving hybrid war environment. Moreover, NATO it appears is a hard power against Russian threats, whilst the EU is a soft power.

Keywords: Hybrid Warfare, The EU's Response to Hybrid Threats, The EU-NATO Cooperation.

Araştırma Makalesi
Makale Gönderim Tarihi: 23.12.2022; Yayına Kabul Tarihi: 01.03.2023

[*] Doç. Dr., Manisa Celal Bayar Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, MANİSA; ORCID: 0000-0002-6353-7468, E-posta: kutayaytug@yahoo.com

[**] Yüksek Lisans Öğrencisi, Manisa Celal Bayar Üniversitesi, Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, MANİSA; ORCID: 0000-0002-9508-7852, E-posta: ifpozan@hotmail.com

Giriş

İnsanlık tarihi boyunca politik, askerî, siyasi, ekonomik ve diğer nedenlerle mücadele alanları oluşmuştur. Mücadeleler kimi zaman diplomatik yollarla çözülebilirken kimi zaman askerî güç kullanarak çözülebilmiştir. Teknolojinin gelişmesi sadece savaş alanlarında kullanılan silah ve araç gereçlerin değişmesine neden olmamış, aynı zamanda savaş alanında yer alan aktörlerin ve yöntemlerin değişmesine neden olmuştur. Örneğin, İkinci Dünya Savaşı'ndan sonra yaşanan küreselleşmenin ve teknolojinin etkisiyle, devletlerin ağırlıklı olarak güvenlik aktörü olarak görev aldıkları güvenlik ortamı yerini çok aktörlü (askerî birlikler, terörist unsurlar, yabancı savaşçılar, organize suç örgütleri vb.), daha az maliyetli ve istenen sonuca daha az sürede ulaşmayı amaçlayan, sınırları, cephesi ve muharebe sahası belli olmayan, sivil ve asker ayrımının olmadığı, hibrit savaş ortamına bırakmıştır.

Herakleitos'un belirttiği gibi "değişmeyen tek şey değişimin kendisidir". Değişen çevre koşulları hayatta kalmaya çalışan her canlı gibi örgütleri de etkilemektedir. Örgütler de değişen çevre koşullarına ayak uydurmak için, kurumlar oluşturmakta, düzenlemeler yapmaktadır. Değişeme ayak uyduramayan yapılar kurumlarını ve düzenlemelerini tekrar gözden geçirmektedir.

Bu çalışmanın amacı, hibrit savaş olgusunun ve beraberinde getirdiği değişimin Avrupa Birliği (AB) ile NATO iş birliği üzerinde yapmış olduğu etkiyi incelemektir. Bu kapsamda çalışmada önce bir kavramsal çerçeve çizilerek hibrit savaş olgusu açıklanacak; daha sonra hibrit savaşın gelişimi, tarihsel arka planı, hibrit savaşın getirmiş olduğu değişimler, hibrit savaş ve Rusya örnekleri üzerinden anlatılacaktır. İzleyen bölümde AB'nin hibrit tehditlere yanıtı incelenerek Birlik kurumlarında ve üye devletlerde hibrit tehditler bağlamında nasıl sorgulamalar yapıldığı incelenecektir. Sonraki bölümde, AB ve NATO iş birliği kapsamında atılan adımlar incelenerek hangi faaliyet alanlarında iş birliğinin artırıldığı incelenecektir. İzleyen değerlendirme bölümünde iş birliği alanında yaşanılan gelişmeler özellikle NATO ve AB'nin yayımladığı raporlar, belgeler çerçevesinde incelenecek, sonuç bölümünde ise elde edilen bulguların değerlendirilmesi yapılacaktır.

Kavramsal Çerçeve

İnsanlık tarihi kadar eski olan savaş olgusu farklı dönemlerde temelinde güç mücadelesi olacak biçimde farklı şekillerde kavramsallaştırılmıştır. Çalışmanın bu kısmında kavramsal tutarlılık sağlamak amacıyla savaş ve hibrit savaş kavramları ele alınacaktır.

Türk Dil Kurumu (TDK) sözlüğüne göre; savaş devletlerin diplomatik ilişkilerini keserek giriştikleri mücadeleyi ifade etmektedir (2022). Savaş üzerine yazılmış en kadim eserlerden olan Sun Zi (Sun Tzu) 'nin "Savaş Sanatı" adlı eserinde "*savaş bir ülkenin baş sorunu, ölüm kalım yeri, var olma ya da yok olma yoludur; muhasebesiz olmaz*." (Zi, 2020, s. 1) şeklinde açıklanmıştır. Orijinali 1831 yılında basılan ve birçok dile çevrilen felsefi derinlikte savaşın işlendiği "Savaş Sanatı" adlı eserinde Prusyalı General Carl von Clausewitz, savaşı "*Savaş sadece politikanın başka araçlarla devamıdır."* (2019, s. 46) şeklinde tanımlamıştır. Clausewitz savaşı her somut durumda doğasını biraz daha değiştiren bir bukalemuna benzetirken; ulus, komutan ve ordu, hükümet ve siyasi iradeden oluşan üç yanlı (boyutlu) şaşırtıcı bir olay olarak betimlemektedir. Ona göre savaş irademizi düşmana zorla kabul ettirmek için kuvvet kullanma eylemidir (2019, s. 49-50).

Soğuk Savaş sonrasında ortaya çıkan teknolojik, iktisadi ve siyasi gelişmelerin etkisiyle savaşın işleyişinin ve doğasının değişmesi de kaçınılmaz bir gerçeklik olarak karşımıza

çıkmaktadır. Bu dönüşüm çerçevesinde günümüz savaşlarını tanımlamak için bilimsel yazında farklı kavramlar kullanılmaktadır. Öte yandan bu kavramların terminolojiyi değiştirmekten öte bir etkisinin olmadığını savunan yazarlar da bulunmaktadır (Horn, 2016, s. 1; Gök, 2019). Gayrinizami harp, sınırsız savaş, asimetrik savaş, bileşik savaş, dördüncü nesil savaş, dolaylı yaklaşım, bileşik savaş, düşük yoğunluklu savaş gibi kavramlar aslında yirmi birinci yüzyılda gerçekleşen birçok savaşı benzer şekilde tanımlamak için kullanılan kavramlardır (Horn, 2016, s. 1). Bu bağlamda Boot ve Doran (2013, s. 2) 'politik savaş', Maxwell (2014) 'geleneksel olmayan savaş', Perry (2015) 'lineer olmayan savaş', Münkler (2010, s. 13) ve Kaldor (2012, s. 1) 'yeni savaş', Liang ve Xiangsui (1999) 'sınırsız savaş', Kinross (2004) 'düşük yoğunluklu çatışma' Huber (2002, s. 2) düzenli birliklerle gerilla birliklerinin düşmana karşı birlikte kullanıldığı savaşlar için 'bileşik savaş' kavramlarını kullanmayı tercih etmektedirler. Bununla birlikte bilimsel yazında en çok kullanılan kavram olarak "hibrit savaş" öne çıkmaktadır. Türkçe yazında genel olarak hibrit savaş kavramı kullanılmakla beraber "Karma Savaş" (Varlık, 2013, s. 124; Erol vd. 2018) ve "Melez Savaş" kavramları da kullanılmaktadır (Karaosmanoğlu, 2015).

Hibrit savaş kavramı bugün genel kabul gördüğü çerçevede ilk kez Frank Hoffman tarafından James Mattis ile yazdığı 2005 tarihli "Geleceğin Savaşı: Hibrit Savaşların Yükselişi" (Mattis vd. 2005) adlı çalışmada kullanılmıştır (Käihkö, 2021, s. 115). Bununla birlikte hibrit savaş kavramını bu tarihten daha önce kullanan çalışmalar da mevcuttur. Örneğin William J. Nemeth, "Gelecek Savaş ve Çeçenistan: Bir Hibrit Savaş Örneği" adlı tezinde, Çeçen toplumunu klan ve aile bağları temelinde inşa edilmiş modern öncesi ve çağdaş devlet arasında melez bir yapı olarak tanımlamıştır. Nemeth, bu melez toplumsal yapıdan düzenli ve düzensiz savaş unsurlarını oldukça esnek ve verimli bir şekilde birleştiren hibrit bir savaş biçiminin ortaya çıktığını ve Çeçen İsyanının hibrit savaş için bir model olacağını iddia etmiştir (2002, s. v).

Hofmann'a göre hibrit savaş ortamında sadece konvansiyonel savaş veya devletlerarası çatışmalarda düşüş olmamıştır; düzenli ve düzenli olmayan savaş türlerini bulanıklaştıran bir birleşim ortaya çıkmıştır (2007, s. 7). Hofmann hibrit savaşları, konvansiyonel imkân ve kabiliyetleri (yetenekler), düzensiz taktikler ve örgütlenmeleri, ayrım gözetmeyen şiddet ve zorlamayı, terörist eylemler ve suç düzensizliğini ve bir dizi farklı harekât çeşitlerini içeren bir savaş türü olarak tanımlamıştır (2007, s. 7). Bilimsel yazında hibrit savaş konusunda çalışmalar yapan araştırmacılardan Bowers (2012, s. 39), Kofman ve Rojansky (2015, s. 2), Mansoor (2012, s. 2), Wijk (2012, s. 358) gibi yazarlar Hofmann'ın tanımlamasını takip etmişlerdir.

Jacobs ve Lasconjarias'a göre hibrit savaşı tanımlamak göründüğünden daha zordur. Çünkü hibrit savaş olgusu birçok yazar tarafından keyfi bir şekilde açık bir kavramsallaştırma olmadan kullanılmaktadır. Mevcut kullanımlarda kavram genel olarak askerî ve sivil ayrımının bulanıklaştığı durumları ifade etmektedir. Hibrit savaş kavramı kullanılırken birçok analist öncelikle oldukça geniş bir spektrumda askerî gücün kullanımı, teknoloji, suç, terörizm, iktisadi baskı, insani ve dinî faaliyetler, istihbarat, sabotaj ve dezenformasyon gibi araçların çeşitlendirilmesini işaret eder (2015, s. 2). Tüm bu tanımlamalara ilaveten NATO tarafından yapılan bir çalışmada ise konvansiyonel olmayan yöntemlerin her çağdaki savaşlarda kullanılmasına rağmen, bilginin savaşa yeni bir boyut eklemesi ve gelişen teknoloji ile bu bilginin küresel düzeyde yayılabilmesi hibrit savaşı özgün kılmaktadır (2016, s. 10).

Avrupa Komisyonu ise hibrit tehditler üzerinden bir tanımlama yapmayı tercih etmiştir. Komisyona göre, hibrit tehditler kavramı, belirli hedeflere ulaşmak için devlet veya devlet dışı aktörler tarafından koordineli bir şekilde kullanılabilecek geleneksel ve geleneksel olmayan,

askerî ve askerî olmayan, açık ve örtülü eylemlerin karışımından oluşan ancak resmen ilan edilmiş savaş eşiğinin altında kalan eylemleri tanımlamak için kullanılmaktadır. Bu tür bir savaşta rakip unsurlar hızlı ve etkili karar vermeyi engellemek için kritik güvenlik açıklarını hedefler ve belirsizlik yaratmaya çalışırlar. Hibrit bir savaşın parçası olarak uygulanan önlemler yelpazesi; kritik bilgi sistemlerine yönelik siber saldırılardan, enerji kaynakları veya finansal hizmetler gibi kritik hizmetlerin kesintiye uğramasına, kamu kurumlarına olan güvenin sarsılmasına veya sosyal güvenlik açıklarının istismar edilmesine kadar çok geniş olabilir (European Commission, 2016, s. 1).

Tüm bu yapılan tanımlar çerçevesinde bu çalışma hibrit savaş kavramını olabildiğince geniş bir kapsamda tanımlamayı tercih etmektedir. Bu çalışmada hibrit savaş; belirli hedeflere ulaşmak için devlet veya özel askerî şirketler ve/veya terörist örgütler gibi devlet dışı aktörler tarafından koordineli bir şekilde kullanılabilecek geleneksel ve geleneksel olmayan, askerî ve kritik bilgi sistemlerine yönelik siber saldırılardan, enerji kaynakları veya finansal hizmetler gibi kritik hizmetlerin kesintiye uğramasına, kamu kurumlarına olan güvenin sarsılmasına veya sosyal güvenlik açıklarının istismar edilmesine kadar çok geniş askerî olmayan, açık ve örtülü eylemlerin karışımından oluşan ancak resmen ilan edilmiş savaş eşiğinin altında kalan eylemleri ifade etmek için kullanılacaktır.

Tarihsel Arka Plan

Son 3500 yıllık insanlık tarihi incelendiğinde sadece 275 yılda savaşın yaşanmadığı, bu sürenin de kesintisiz olarak birbirini takip etmediği görülmektedir (Dedeoğlu, 2014, s. 32). Bu tarihsel akışta savaşın icrası yaşanan gelişimlere göre sürekli olarak değişim göstermiştir. Clausewitz'e göre her çağın kendine ait siyasi, iktisadi ve sosyal yapısı, savaş şekilleri ve o çağa özgü düşünceleri bulunmakta, söz konusu değişkenlerdeki gelişmeler de savaşın karakterine etki etmektedir. Böylelikle Clausewitz savaşı bukalemuna benzetmekte, her dönemin savaşının kendine özgü olacağını, savaşlarda yaşanılacak değişimlerin kaçınılmaz olacağı ve savaşların doğasının bunu gerektirdiğine işaret etmektedir (Clausewitz, 2019, s. 49).

Savaşın doğası ve evrimini inceleyen çalışmalar ve aşamaları ele alındığında bilimsel yazında farklı kuramsal değerlendirmelerin ve sınıflandırmaların olduğu görülmektedir (Gürcan, 2012, s. 76). Örneğin Martin van Creveld (1999) savaşın aşamalarını, Aletler Çağı, Makineler Çağı, Sistemler Çağı, Otomasyon Çağı olarak gruplandırırken; Toffler (1993) bu aşamaları, Tarım Toplumu, Endüstri Toplumu, Bilgi Toplumu olarak ve Liang ve Xiangsui (1999, s. 22) ise savaşın aşamalarını Sınırlı Ortaçağ Savaşları, Sınırlı İmparatorluk ve Ulus Devlet Savaşları, Sınırsız Post-Modern savaşlar olarak ele almıştır.

Bu çalışmanın takip edeceği sınıflandırma ise William S. Lind ve diğerleri (1989, s. 22-26) tarafından Marine Corps Gazette'de 1989 yılında ortaya atılan ve savaşı dönemlere ayırarak aşamalı olarak yorumlayan "Savaşın Nesilleri Yaklaşımı"dır. Lind'e göre; teknolojide ve stratejide meydana gelen değişimler savaşın da değişmesine yol açmaktadır. Lind'in Savaşın Nesilleri modeline göre;

- Birinci aşama ulus devlet öncesi savaşları,
- İkinci aşama, birinci nesil savaş, Klasik Savaşları (1648-1830),
- Üçüncü aşama, ikinci nesil savaş, Topyekûn Endüstri Savaşları (1830-1918),
- Dördüncü aşama, üçüncü nesil savaş, (Manevra Savaşları) (1918-1948),

- Beşinci aşama, dördüncü nesil savaş, siyasi, sosyal, ekonomik ve askerî konuları kapsayan ağ merkezli savaşlardan oluşmaktadır (1948'den günümüze).

Birinci nesil savaşlar, çok sayıda piyadenin çizgisel düzende hareket ettiği ve süvarinin kullanıldığı, en çok ateş gücünün arzu edildiği, çok sınırlı teknolojinin kullanılabildiği, hedefin cephedeki düşmanın imha edilmesinin esas amaç olduğu savaşlardır. İkinci nesil savaşlar endüstri devrimi ve teknolojinin gelişmesiyle makineli tüfeklerin ve topçuların kabiliyetlerinin daha da arttığı, deniz ve tren ulaşım olanaklarının artmasıyla kuvvet kaydırma imkânlarının da arttığı savaşlardır. Bu savaşa örnek olarak Birinci Dünya Savaşı verilebilmektedir. Üçüncü nesil savaşlara gelindiğinde, Birinci Dünya savaşıyla birlikte yaşanan yıkım sonrasında barışı sağlamak için, uluslararası iş birliği ortamı tesis edilmeye çalışılmıştır. Ancak, devletlerarası anlaşmazlıkların devam etmesi, silahlanma yarışını da beraberinde getirerek, var olan sorunların daha da artmasına yol açmıştır. Bu nedenle 1930'lu yıllardan itibaren uluslararası ortamdaki iş birliği yerini güvensizliğe bırakmıştır. Birinci Dünya Savaşı sonrasındaki alınan tedbirlerin başarısız olması, İkinci Dünya Savaşının çıkmasına yol açmıştır. İkinci Dünya Savaşı sırasında füze, roket, havacılık ve denizcilik alanında yaşanan ilerlemeler, tankın kullanımının yaygınlaşması, nükleer silahların geliştirilmesi gibi gelişmeler savaş alanlarına da yansımış ve ülkelerin askerî güç kapasitelerinde değişimler meydana getirmiştir. Bu değişimler ülkelerin savaş taktiklerine de yansıyarak savaşın kısa sürede bitirilmesini hedefleyen "Yıldırım Harbi" gibi öğretilerin geliştirilmesini sağlamıştır. İnisiyatif kullanma ön plana çıkarken yakınlaş ve yok et stratejisi yerine, etrafından dolaş ve savunmasını çökert stratejisi önem kazanmıştır. Üçüncü nesil savaşa ikinci dünya savaşı esnasındaki muharebeler örnek verilebilmektedir. Dördüncü nesil savaşlar, ikinci dünya savaşı sonrasında teknolojik gelişmelerle devletlerin artan konvansiyonel güç ve kapasitelerine ek ve alternatif olabilecek, siber savaş, gerilla harbi, psikolojik savaş, gibi asimetrik savaş unsurlarının önem kazandığı savaş neslidir. Dördüncü nesil savaşlarda, savaş barış dönemleri arasında ayırım bulanıklaşmakta ve düşman ülkenin askerî güç unsurlarının yanında diğer kabiliyetleri de hedef alınmaktadır. Ayrıca büyük birliklerin yerini küçük ancak daha etkin birlikler ve devlet dışı aktörler almıştır. Savaşlar medyanın gözetiminde icra edilmekte ve yerleşim yerlerine yakın bölgeler de savaş alanı olabildiğinden asker sivil ayrımı zorlaşmaktadır. Dördüncü nesil savaşlarda teknolojiye bağımlılık bir dezavantaj olarak ön plana çıkmaktadır (Lind, 2004, s. 13-14).

İkinci Dünya Savaşı'ndan sonra yaşanan küreselleşmenin ve teknolojinin etkisi, nükleer silah kapasitelerinin ve savaşın yıkıcı etkisinin artması nedeniyle, devletlerin güvenlik aktörü olarak görev aldıkları güvenlik ortamı yerini çok aktörlü (askerî birlikler, terörist unsurlar, yabancı savaşçılar, organize suç örgütleri vb.), daha az maliyetli ve istenen sonuca daha az sürede ulaşmayı amaçlayan, sınırları, cephesi ve muharebe sahası belli olmayan, sivil ve asker ayrımının olmadığı, savaş ortamına bırakmıştır. Savaşın ekonomik boyutunu değerlendiren Çinli Albaylar Liang ve Xiangshui'ye göre devletler maliyetli olan konvansiyonel güç kullanmak yerine, daha az maliyetli yöntemlerle hedeflerini elde edebiliyorlarsa, savaş yeni bir formda değerlendirilmelidir (1999, s. 6). Böylelikle Soğuk Savaş sonrası dönemde devletler konvansiyonel savaşta karşılaşabilecekleri yüksek maliyetler yerine daha az kaynak ayırabilecekleri stratejiler üzerine odaklanmışlardır.

Soğuk savaş sonrası dönemde değişen güvenlik anlayışını değerlendiren Creveld (1991, s. 216) Clausewitz'in görüşlerine dayanan ulus, ordu ve siyasi irade arasındaki bölünmeye/ilişkiye dayanan savaş türünün sona yaklaştığını, düşük yoğunluklu çatışma olgusunun yükselişe geçtiğini ve uzun vadede farklı türden savaşan örgütlerin devletlerin

yerini alacağını iddia etti. Creveld'e göre gelecekte, savaş ordular tarafından değil, bugün teröristler, gerillalar, haydutlar ve soyguncular olarak adlandırılan, ancak gelecekte kendilerini tanımlamak için daha resmî unvanlar kullanacak olan, profesyonellikten ziyade fanatik, ideolojik temelli bağlılıklarla motive edilmesi olası gruplar tarafından yürütülecektir (1991, s. 221).

Barry Buzan "Askerî Güvenliğin Değişen Gündemi" adlı çalışmasında, 11 Eylül sonrası dönem için yaptığı değerlendirmede teröre karşı savaş şeklinde oraya çıkan yeni güvenlikleştirmenin klasik devlet merkezli, askerî güvenlik konularının ötesinde geçtiğini vurgulamaktadır. Yeni yapıda küresel düzlemde tanımlanan güvenlikleştirme, toplumun hem sivil hem de sivil olmayan taraflarını da içine alan devlet dışı aktörlerin de yer aldığı bir çerçeveye doğru genişlemekte ve bu genişlemiş alanda dört farklı şiddet yapısı bulunmaktadır. Söz konusu yapılar; 'devlet devlete karşı', 'devlet sivil olmayan topluma karşı', 'devlet ve sivil toplum karşı karşıya', 'sivil ve sivil olmayan toplum karşı karşıya' şeklide kategorize edilmiştir (2008, s. 121-123). Bu yaklaşıma göre günümüzdeki tehditlerin kaynakları arasında devlet dışı aktörlerin yer alması klasik güvenlik yaklaşımlarının yeniden gözden geçirilmesine neden olmaktadır.

Günümüzün savaşları birçok akademisyen ve yazar tarafından "Türeyen Savaşlar" (Arquila, 2005), "Yeni Nesil Savaşlar", (Kaldor, 2003) "Sınırsız Post Modern Savaş" (Liang & Xiangsui, 1999) ve "Hibrit Savaş" (Hoffmann, 2006) gibi tanımlarla ifade edilmeye çalışılmıştır. Bunun nedeni belirtilen terimlerin askerî kaynaklardan türemesi, ABD ve müttefiklerinin soğuk savaş ertesinde yer aldığı savaşların farklı olarak kavramsallaştırılmasıdır (McFate & Jackson, 2006). ABD ve koalisyon güçlerinin Irak ve Afganistan'da karşılaştığı geleneksel ve geleneksel olmayan tehdit unsurları söz konusu devletleri yeni stratejiler geliştirmeye sevk etmiştir. Hoffman tarafından 2006 yılında İsrail ve Lübnan savaşını (2007) açıklamakta kullanılan, izleyen süreçte diğer yazarlar tarafından da Rusya-Gürcistan (2008), Rusya-Ukrayna (2013) savaşlarını açıklamakta kullanılan "Hibrit Savaş" kavramı diğer kavramlara göre daha fazla kullanılmaya başlanmıştır.

Hibrit Savaş'ın Getirdiği Değişimler

Hoffman'a göre Hibrit Savaşın en açık örneğini 2006 yılında yaşanan İsrail-Hizbullah çatışması teşkil etmiştir (2007, s. 35). Bu çatışma, daha önce 1948, 1956, 1967, 1973 yıllarında Arap Devletleri ve İsrail arasında meydana gelen devletlerarası bir çatışma şeklinde gerçekleşmemiş, devlet olarak İsrail ve devlet dışı aktör olan Hizbullah arasında gerçekleşmiş olması nedeniyle farklılık göstermektedir. Belirtilen çatışmada Hizbullah'ın konvansiyonel ve konvansiyonel olmayan savaş araçlarını bir arada kullanması ile teknolojik ve askerî kabiliyet bakımından üstün olan İsrail'e karşı başarı kazanması ön plana çıkmıştır (2007, s. 17-34).

Hibrit savaşın getirdiği birinci değişim savaşan aktörlerdeki belirsizliktir. Devletler güvenlik ortamında baş aktör olarak devam etmelerine rağmen, devlet dışı aktörler (terörist örgütler, organize suç örgütleri, yabancı savaşçılar vb.) çatışmaların tarafları hâline gelmişlerdir (Türkgenci vd., 2018, s. 64). Belirtilen aktörlerin ulusal ve uluslararası normların dışında hareket etmeleri sorunu daha da karmaşık hale getirmiştir. Kaldor'a göre savaşan aktörlerin mevcut normların dışında hareket etmelerinin bir nedeni de savaş ekonomisi geliştirme niyetleridir. Söz konusu aktörler savaş çevresinde soygun, talandan, tarım ve petrol arazilerinin kontrol edilmesine kadar birçok yasadışı faaliyeti yerine getirmektedir (2013, s. 3). Hibrit savaşın karmaşıklığı ve boyutları, politik, askerî, hukuki, sosyolojik ve psikolojik

unsurları kapsadığından sadece askerî gücün tepkisi yetersiz kalmakta, kapsamlı yaklaşımla[1] sorunun ele alınmasını ve yumuşak, sert ve akıllı[2] güç unsurlarının kullanılmasını gerekli kılmaktadır.

Hibrit savaşın getirdiği ikinci değişim savaş ve barış arasındaki çizginin kaybolmasıdır (Gerasimov, 2013, s. 25). Savaş ve barış zamanı arasında belirginlik azaldığından, savaşın meşru sayılabileceği "Haklı Savaş[3]" kavramı sorgulanmaya başlanmıştır. Savaşlar, savaş ilanın olmamasıyla düşük yoğunluklu çatışma şeklinde sürdürülmüştür. Bu yüzden dünyanın birçok yerinde çatışma sayısında artış meydana gelirken, devletlerarasında meydana gelen savaşlar azalmıştır (Gürcan, 2012). Gerasimov'a göre günümüz savaşları, uluslararası hukukun bağlayıcılığı nedeniyle yabancı unsurların desteklenmesi ve örtülü operasyonlar gerçekleştirmek suretiyle seferberlik ve yığınaklanma olmasına gerek kalmadan gerçekleştirilebilmektedir (2013, s. 25).

Hibrit savaşın getirdiği üçüncü değişim özelliği savaş mekânında meydana gelen değişimdir. İletişim teknolojilerinin gelişmesiyle birlikte savaşın gerçekleştiği kara, hava, deniz boyutlarına, uzay ve siber uzayda eklenmiştir. Böylelikle düşmana karşı bilgi üstünlüğü, elektronik harp, siber savunma ve saldırı kabiliyetlerinin geliştirilmesi ve ağ merkezli harekât[4] önem kazanmıştır. Cebrowki ve Garstka'ya göre ağ merkezli harekât, sahip olunan bilgi teknolojileriyle komuta ve kontrolü hızlandırmakta, birliklerin komutanın niyetine göre kendilerini uyarlama yeteneklerini artırmaktadır (2022). Bunun savaş ortamına ilk yansımasının Birinci Körfez Savaşı olduğu değerlendirilmektedir. Söz konusu savaşta ABD ağ merkezli yeteneklerini kullanarak savaşı kısa sürede lehine sonuçlandırmıştır. Siber uzaysa, düşmanın bilgi üstünlüğünü elde etmesini engellemek, ağ merkezli yeteneklerini kullanmasını kısıtlamak için devletlerin hak ve menfaatlerini koruması gereken bir harekât ortamı hâline gelmiştir (Türkgenci vd., 2018, s. 65). İnternet teknolojisinin hayatın bütün alanlarını kapsamasıyla enerji santralleri, bankacılık sistemleri, sağlık, eğitim ve elektronik devlet uygulamaları gibi kritik altyapı unsurlarının korunması önem kazanmıştır. İnternet ortamının kullanılması devletlerin güçlerini artırdığı gibi, devlet olmayan aktörlerin de daha kolay organize olabilme, kitleleri yönlendirebilme, terörist örgütler için eleman temin etme gibi yeteneklere kavuşmasını sağlamıştır. Belirtilen altyapılar siber saldırıların hedefleri haline gelmekte, hedef toplumlarda kargaşaya neden olunması amaçlanmaktadır (Wheatly, 1996, s. 6). Mekân boyutunda meydana gelen bir diğer gelişme ise; savaşların yerleşim alanlarına kayması ve bunun sonucu olarak yaşanan kitlesel göç hareketlerinin gerçekleşmesidir. Böylece asker-sivil ayrımı zorlaşmaktadır.

Hibrit savaşın getirdiği dördüncü değişim harekât çeşitleri ve savaş tekniklerinde meydana gelen dönüşümdür (Türkgenci vd., 2018, s. 65). Sun Zi'ye göre savaş cephe ve sürpriz manevralardan oluşmaktaysa da cephe ve sürpriz manevraların bileşimleri sonsuzdur

[1] Kapsamlı Yaklaşım: Özellikle kriz ve harekât yönetim sürecinde yürütülen planlama ve icra faaliyetlerine sivil, askeri yetenek ve uzmanlıkların dâhil edilmesi, devletin diğer kamu kurum ve kuruluşları ve sivil toplum kuruluşları ile iş birliği ve koordinasyonun sağlanmasına yönelik süreçlerin geliştirilmesini ifade etmektedir (NATO, 2022).

[2] Akıllı güç: Devletlerin amaçlarına ulaşabilmesi için yumuşak ve sert güç unsurlarının bütünleştirilerek kullanılması esas alan stratejidir (Armitage vd. 2022, s. 7).

[3] Haklı Savaş: Savaşın meşru sayılabilmesi için son çare olarak başvurulması, savaşın başlamadan önce ilan edilmesi savaşanlar ve savaşmayanlar arasında ayrım gözetilmesi ve savaş hukukuna uygun hareket edilmesini ifade etmektedir (Akeker, 2019, s. 1)

[4] Ağ merkezli Harekât: Karar vericiler ile uygulayıcıları iletişim ağları ile birbirlerine bağlayarak muharebe gücünü en yüksek seviyeye çıkarmayı hedefleyen harekât türüdür (Mcconoly, 2022).

(2020, s. 20). Hibrit savaş ortamı, düzenli harekât çeşitlerinin yanında (taarruz, savunma, geri çekilme vb.), barışı destekleme harekâtı, insani yardım harekâtı gibi diğer harekât çeşitlerinin de eş zamanlı olarak kullanılmasını gerektirmektedir. Vekalet savaşları[5], siber savaş, ekonomik savaş, psikolojik savaş, göç hareketleri, kimyasal, biyolojik radyolojik ve nükleer silahlar gibi asimetrik savaş[6] tekniklerin kullanılması ön plana çıkmıştır. Belirtilen harekât çeşitlerinde hibrit savaşın aktörleri tarafından sosyal medya ve medyanın diğer unsurları araç olarak kullanılmıştır. Medya platformlarınca korku ve panik havası yaratılıp göç hareketleri tetiklenmiş, psikolojik harp unsurları kullanılarak, taraftar toplama ve propaganda icra edilmiş ve taraftar kesimlerin destekleri artırılmıştır (Eker, 2015, s. 60-61). General Patreus yeni dönemde bilginin esas unsur olduğuna dikkat çekmiştir. Patreus'a göre Irak ve Afganistan'da konvansiyonel yöntemleri kullanarak başarılı olamayan ABD, halk desteğini edinebilmek için önceliğini psikolojik harekâta ve kitlesel iletişim araçlarına kaydırmalıdır (2010, s. 116).

Hibrit savaş ortamında kuvvet, zaman ve mekândaki değişimlerden dolayı devletlerin tehdit algılamalarında değişimler yaşanmıştır. Hibrit savaş öncesindeki dönemlerde devletlerden gelebilecek tehditlerin takip edilmesi öncelikli olmuştur. Hoffman'a göre Hibrit savaş ortamında, devletlerden gelebilecek tehditlerin yanında, terör örgütleri ve suçlular gibi devlet dışı aktörler de savaş ortamını şekillendirmek ve politik amaçlara ulaşabilmek amacıyla kullanılmaktadır (2014). Devlet dışı aktörler uluslararası hukukun dışında, askerî olmayan ancak askerî etkilere eşdeğer ve üzerinde etki yaratan kimyasal, biyolojik, radyolojik ve nükleer (KBRN) maddeleri, siber saldırılar, zehirli gazlar, finansal araçlar gibi asimetrik vasıtaları kullanabilmektedir. Bu kapsamda belirtilen aktörlerin icra ettikleri terör eylemleri, göçmen kaçakçılığı ve sınır ihlalleri, uluslararası suçlar, siber korsanlık faaliyetleri ve bu unsurların finansmanının takip edilmesi gereken faaliyetler kapsamına alınmıştır.

Günümüz savaş ortamının değiştiğine dikkat çeken yazarlardan birisi de Rusya Genelkurmay Başkanı Valery Gerasimov'dur. Gerasimov "Öngörüde Bilimin Değeri" adlı makalesinde modern savaş ortamındaki değişimlerin ne olduğuna, ordunun bu değişimlere yönelik nasıl hazırlanması gerektiğine vurgu yaparken, bilimin önemine dikkat çekmiştir. Makalesinde savaş ile barışın arasındaki çizginin kaybolduğunu ifade etmiştir. Günümüzde politik hedeflerin elde edilebilmesi için asker ve asker olmayan kişiler tarafından, askerî ve askerî olmayan yöntemlerin kullanılabildiğini ifade etmiştir. İnsansız hava araçları, robotik uygulamalar gibi yapay zekâ teknolojilerinin geliştirilmesine dikkat çekerek, belirtilen unsurların etkilerinin konvansiyonel silahlardan daha fazla katkı sağlayacağını dile getirmiştir (2013, s. 24).

Sun Zi Savaş Sanatı adlı eserinde asıl zaferin savaşmadan kazanmak olduğunu belirtmiştir (2020, s. 7). Hibrit savaşın esas karakterini savaşmadan veya en az kayıpla kazanmak oluşturmaktadır. Bu amaca ulaşılabilmesi için bir strateji çerçevesinde, birbirini tamamlayan faaliyetler gerçekleştirilmektedir. Öncelikle hedef ülke, Rusya Estonya Krizinde olduğu gibi teknolojiye bağımlılık ve 2014, 2022 Rusya Ukrayna savaşlarında olduğu gibi yandaş azınlık unsurlar dâhil olmak üzere çeşitli hassasiyetler kullanılarak etki altına

[5] Vekâlet Savaşları: Devletlerin özellikle küresel güçlerin kendi çıkarlarını elde etmek ve nüfuz alanlarını genişletmek için, kendi askerlerini kullanmaktan ziyade, müttefiklerini, paralı askerlerini, edilgen ülkeleri, hedef ülkedeki parçalanmış yapıları ve yandaş unsurları savaştırdıkları savaş türüdür (Hoffman vd. 2021).

[6] Asimetrik Savaş: Düşmanın sahip olmadığı(asimetrik) silah ve tekniklerin kullanılmasıyla hassas taraflarından faydalanarak, kendi kaybını azaltırken, düşmana en fazla kayıp verdirmeyi amaçlayan savaş türüdür. Terörist taktikler, adam kaçırma, gerilla savaşı gibi eylemler asimetrik savaş içerisinde yer almaktadır (Sokullu, 2019, s. 6).

alınmaktadır. Bu sürecin uzun bir döneme yayılmasıyla yıpratma stratejisi oluşturulmakta ve savaşa başlamadan önce harekât ortamının kendi lehine çevrilmesi sağlanmaktadır.

Son yirmi yılda Rusya'nın uluslararası ortamda izlemiş olduğu dış politika Amerikan tek kutupluluğunun sona erdirilerek, çok kutuplu düzenin oluşturulmasını sağlamak ve bunun uluslararası aktörler tarafından kabul edilmesini sağlamak olmuştur (Özdal, 2021, s. 7). Bu amaca yönelik olarak hibrit savaş örnekleri ele alındığında; Rusya Estonya krizinde, Rusya Estonya'nın bankacılık sistemini siber saldırılarla işlevsiz hale getirmiştir. 2008 yılındaki Rusya Gürcistan Savaşı'nda Rusya Güney Osetya ve Abhazya'yı ayırabilmek için öncelikle siber saldırılarla teknoloji altyapısını çalışamaz duruma getirmiştir. Daha sonra kendini korumak için bu operasyonu düzenlediğini söyleyerek özel güçlerini bölgeye sevk etmiştir. İzleyen süreçte düzenli kuvvetleri göndermiştir. 2014 yılındaki Rusya'nın Kırımı ilhakında ise siber saldırılarla, Ukrayna'nın enerji ve teknoloji altyapısı çalışamaz hale getirilmiştir. Eş zamanlı olarak yandaş ayrılık yanlısı unsurlar desteklenmiştir. Kargaşa ortamı oluşturularak, Kırım'ın ilhakı sağlanmıştır (Bıçakçı, 2019, s. 5). Kırım'da istilayı işgal, işgali ise ilhak safhası takip etmiştir. Suriye'de yaşanan iç savaş esnasında Rusya'nın müdahalesi kara gücü konuşlandırmaktan ziyade özel askerî şirketleri, paramiliter[7] yapıları kullanmayı ve yerel güçlerin eğitimini esas almıştır. Bu güçler istihbarat ve hava gücü ile desteklenerek ulusal hedeflerin elde edilmesi amaçlanmıştır (Corbeil, 2022). 2022 yılında Rusya Ukrayna Savaşı'nda, Rusya savaş ilan etmemiştir. Savaşın ilk başından itibaren kendini koruma amacıyla operasyon düzenlediğini beyan etmiştir. Yandaş yerel unsurlar desteklenmiştir ve özel harekât güçlerinin kullanılmasını izleyen süreçte, düzenli birliklerle harekâta başlamıştır.

Belirtilen kriz ve savaşlarda kullanılan hibrit savaş taktik ve teknikleri uluslararası aktörlerin ilgisini daha da artırmasına neden olmuştur. Çalışmanın bundan sonraki kısmında bir uluslarüstü örgüt olan AB'nin hibrit savaş karşısındaki politikaları incelenecektir.

Hibrit Tehditlere Karşı Avrupa Birliği'nin Yanıtı

Avrupa Birliği'nin hibrit tehditlere yanıtı yeni bir olgu olmamakla beraber, özellikle Rusya'nın Kırım'ı ilhakı, Suriye İç Savaşı'ndan kaynaklanan düzensiz göçmen krizi ve yabancı terörist savaşçıların Birlik içerisinde yapmış olduğu eylemlerin artmasıyla hız kazanmıştır. AB Komisyonu'nun 6 Nisan 2016'da yayınlamış olduğu "Hibrit Tehditler Karşı Koyma Ortak Çerçevesi-Avrupa Birliği Yanıtı" ortak iletişim belgesinde dünyada tehdit ortamının değiştiğine vurgu yapılmıştır (European Commission, 2016). Adı geçen belge, günümüz hibrit ortamının AB tarafından nasıl algılandığını anlamak ve Birliğin tehditlere nasıl önlemler aldığını görmek açısından önemlidir. Belgede Balkanlar'da ve Avrupa'nın güneyinde yaşanan gelişmelerin Avrupa güvenliğini etkilediği belirtilmiş ve AB-NATO iş birliğine işaret edilmiştir. Üye ülkelerden tehditlerin tanımlanması, farkındalığın artırılması, dayanıklılığın inşası, önleme, krize cevap verme ve yenilenme adımlarını içerecek faaliyetlerin planlanarak uygulanması istenmiştir. İlk olarak tehditlerin tanımlanması kapsamında, üye ülkelerden hibrit risk araştırması yaparak zayıf taraflarını ortaya koyması istenmiştir (European Council, 2016).

Farkındalığın artırılması kapsamında Avrupa Birliği İstihbarat ve Durum Merkezi'ne (The European Union Intelligence and Situation Center)[8] bağlı olarak çalışacak Avrupa Birliği

[7] Paramiliter Gruplar: Bazı durumlarda ordunun görevlerini üstlenmek üzere hükümet tarafından kurdurulan, eğitilen ve teşkilatlandırılan düzenli ordulara yardımcı yapılardır (Erkmen, 2019, s. 4).

[8] The European Union Intelligence and Situation Center (Avrupa Birliği İstihbarat ve Durum Merkezi): 12.03.2012'de kurulmuştur. Avrupa Birliği Dış İlişkiler Servisi Başkanlığı'na bağlı olarak faaliyet göstermektedir.

Hibrit Birleştirme Hücresi (EU Hybrid Fusion Cell)[9] kurulmuştur (European Union External Action Service, 2018, s. 1). Üye ülkelerin temsilcileri bu hücrede görev yaparak, elde edilen gizli ve açık istihbaratları değerlendirebilmektedir. Böylece Birlik ülkeleri elde edilen istihbaratlardan ortak olarak faydalanabilmektedir. Ayrıca farkındalığı artırmak amacıyla, Hibrit Tehdit Mükemmeliyet Merkezi (Hybrid Center of Excellence) kurulmuştur. Bu merkez AB'ye siber güvenlik, stratejik iletişim, sivil asker iş birliği, enerji ve krize cevap verme yeteneklerinin kazanılması ve geliştirilmesi kapsamında katkı sağlamaktadır (Hybrid Coe, 2022).

Dayanıklılığın inşasının amacı üye devletlerde hibrit tehditlerle mücadele için kritik alt yapılarının, tedarik zincirlerinin ve toplumsal hassasiyetlerinin istismar edilmesine engel olunmasıdır. Kritik alt yapıların korunması kapsamında, enerji ağları ve nükleer tesisler, kara, hava ve deniz yollarını güvenliğinin güçlendirilmesine yönelik çalışmalar yapılmaktadır. Uzay altyapısında olabilecek bir hassasiyetin birçok sektörü etkileyebileceği göz önünde bulundurularak, Galileo gözlem uydusunun istenilen zamanda hibrit tehdidi gözlemleyecek yeteneği kazanması hedeflenmektedir. Ayrıca Birlik tarafından savunma kabiliyetlerinin geliştirilmesi kapsamında hibrit tehditlere karşı yeni teknolojilerin geliştirilmesinin önemi bir kez daha anlaşılmıştır. Halk sağlığının ve gıda güvenliğinin korunması kapsamında KBRN maddelerin kullanılarak, ortamın kirletilebileceği, hayvan ve bitki hastalıklarının kasten yayılarak gıda güvenliği dâhil olmak üzere birçok alanda tehlike yaratabileceği değerlendirilmektedir (European Commission, 2016, s. 4).

Siber güvenliğin sağlanması kapsamında; kritik altyapının kullanımını sağlayan dijital hizmetlerin hibrit tehditlerce baskı altına alınabileceği ön plana çıkmaktadır. Üye ülkelerce siber güvenlik kabiliyetlerinin geliştirilmesine yönelik olarak iş birliğinin ve bilgi değişiminin arttırılmasına ihtiyacı duyulmaktadır. Bu kapsamda Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı'nın (European Union Network and Information Security Agency)[10] ortak yaklaşımının esas alınması gerektiği önem kazanmıştır (The Computer Emergency Response Team for the EU institutions, 2022). Ayrıca üye ülkelerde bulunan Bilgisayar Güvenliği Vakaları Müdahale Timlerinin (Computer Security Incident Response Team)[11], Avrupa Birliği Kuruluşları için Bilgisayar Acil Durum Müdahale Timi (Computer Emergency Response Team for the EU insititutions)[12] ile eşgüdümün sağlanması gerektiği ortaya çıkmaktadır. Enerji tesislerinin siber saldırılara karşı korunarak, siber saldırıların nasıl önleneceği, hangi prosedürlerin uygulanacağı ve söz konusu saldırıların etkilerinin nasıl azaltılabileceğine yönelik

---

Merkezin görevi üye ülkelerden yönlendirilen ikaz ve istihbaratları değerlendirerek müşterek tehdit değerlendirmesi oluşturmaktır (Ray, 2022, s. 1).

[9]The EU Hybrid Fusion Cell (Avrupa Birliği Hibrit Birleştirme Hücresi): Avrupa Birliği İstihbarat ve Durum Merkezi'ne bağlı olarak faaliyete geçmiştir. Üye ülkelerden gelen hibrit tehdit bilgilerini birleştirerek erken ikaz ve durumsal farkındalığın arttırılmasını sağlar. Elde edilen müşterek bilgiler İstihbarat ve Durum Merkezi tarafından değerlendirilmelere dönüştürülerek istihbarat elde edilmektedir (Council of The European Union, 2020, s. 2).

[10] Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (European Union Network and Information Security Agency): 2004 yılında kurulmuştur ve merkezi Atina'dadır. Adı daha sonra Avrupa Birliği Siber Güvenlik Ajansı olarak değiştirilmiştir. Kurumun görevleri arasında Birlik bazında siber tehditlere karşı önleme ve müdahale prosedürlerinin geliştirilmesi, üye ülkelerle eşgüdüm ve siber güvenlik yeteneklerinin geliştirilmesi kapsamında danışmanlık sağlaması öngörülmüştür (ENISA, 2022).

[11] Bilgisayar Güvenliği Vakaları Müdahale Timi (Computer Security Incident Response Team): Siber güvenliği sağlayan kamu kurumlarına veya sivil kuruluşlara ait müdahale timleridir.

[12] Avrupa Birliği Kuruluşları için Bilgisayar Acil Durum Müdahale Timi (The Computer Emergency Response Team for the EU institutions) 2012 yılında kurulmuştur. Avrupa Birliği Kurum ve Kuruluşlarının siber güvenliğini sağlamakla görevlidir (CERT-EU, 2022).

uygulamalar geliştirilmektedir. Finansal kuruluşların da siber saldırılara hedef olabileceği ifade edilerek, ulusal ve uluslararası finansal kuruluşlarla iş birliğinin teşviki ve tehdit bilgi paylaşımı platform ve ağlarının kullanılmasına önem verilmiştir. Siber saldırılarda bir diğer hedefin ulaştırma sektörü olduğu ifade edilerek kara, hava ve demir yollarının dijital alt yapı dayanaklığının arttırılması hedeflenmiştir (CERT-EU, 2022).

Hibrit tehdit finansmanının engellenmesi kapsamında, teröristlere finansal destek sağlanarak istikrarsız alanlar oluşturulabileceği göz önünde bulundurulmaktadır. Bu kapsamda Finansal İstihbarat Birimleri (Financial Intelligence Units)[13] ile kara para aklamaya, şüpheli para transferlerinin takibi ve bilgi değişimi konusunda iş birliği önem kazanmıştır (Excellence, 2022).

Radikalleşme ve aşırı şiddete yönelik olarak dayanıklılığı inşası kapsamında, teröristlerin sosyal medya ve diğer internet platformlarını kullanarak masum insanları radikalleştirebildiği değerlendirilmektedir. Bu kapsamda, Radikalleşme Farkındalık Ağı'nın (Radicalisation Awareness Network)[14] kullanımına dikkat çekilerek, internet ortamındaki yasadışı içeriklerin kaldırılmasına yönelik önlem alınmasının önemi vurgulanmıştır (European Commission, Radicalisation Awareness Network, 2022).

Üçüncü ülkelerle iş birliğinin geliştirilmesi kapsamında, Avrupa Komşuluk Politikasında belirtildiği üzere güney ve doğu komşularla ilişkilerin geliştirilmesi önem kazanmaktadır. Bu kapsamda bir yandan organize suç, terörizm, düzensiz göç ve yasadışı hafif silah geçişinin engellenmesine yönelik iş birlikleri geliştirilirken, diğer taraftan da üçüncü ülkelerde istikrarsızlığın engellenmesine yönelik olarak, sağlıklı bir şekilde işleyen kurumların oluşturulması ve mali yardım yapılmasına yönelik çalışmalar yapılmaktadır. Böylece Avrupa güvenliği üçüncü ülkelerden gelebilecek saldırılara ve istikrarsızlıklara karşı koruma altına alınmıştır (European Commission, 2015, s. 14).

Krizi önleme, cevap verme ve yenilenme başlığı kapsamında kurulan Avrupa Hibrit Birleştirme Hücresinin hibrit tehdit değerlendirmelerini, Birlik seviyesinde tek çatı altında toparlayacağı ve karar organlarına bilgi aktarımını hızlandıracağı değerlendirilmektedir. Böylelikle krize koordineli ve daha hızlı müdahalenin mümkün olacağı beyan edilmiştir. Hibrit tehditlere yönelik olarak krize sivil müdahale yeteneklerinin geliştirilmesinin de önemli olduğu vurgulanarak, milli unsurların, Avrupa Acil Durum Müdahale Koordinasyon Merkezi ile (European Emergency Response Coordination Centre)[15] eşgüdümü sağlanmaktadır (European Commission, 2022).

---

[13] Finansal İstihbarat Birimleri (Financial Intelligence Units)): Amacı şüpheli para transferlerinin takip edilmesiyle, organize suç örgütlerinin, teröristlerin kara para aklaması ve terörizmin finansmanına engel olunmasıdır. Finansal İstihbarat Birimlerinin özelliği diğer ülkelerdeki eşdeğer örgütlerle ve devlet kurumlarıyla iş birliği yapabilmesidir (Excellence, 2022).

[14] Radikalleşme Farkındalık Ağı'nın (Radicalisation Awareness Network): Avrupa Birliği Göç ve İç ilişkiler komisyonuna bağlı olarak faaliyet gösterir. Ağ radikalleşmenin önüne geçilebilmesi için akademisyenleri, politikacıları ve konu hakkında bilgi sahibi olan uygulayıcıları bir araya getirerek bilgi değişiminin ve araştırmaların yapılmasını sağlar (European Commission, 2022).

[15] Avrupa Acil Durum Müdahale Koordinasyon Merkezi (European Emergency Response Coordination Centre): Avrupa Birliği'nin herhangi bir doğal afet anında müdahale edecek gücünü oluşturmaktadır. Uzman sivil koruma timleri ve donanımları mevcuttur. Afet anında BM veya ülkeler nezdinde talep olduğu takdirde herhangi bir yerde doğal afetlerde yardım faaliyetini yerine getirir (European Commission, European Emergency Response Coordination Centre, 2022).

Krize cevap vermenin hukuksal altyapısını Avrupa Birliği'nin İşleyişi Hakkındaki Antlaşmanın (Treaty on the Functioning of the European Union) 222. maddesi (Dayanışma maddesi) oluşturmaktadır (European Union, 2007). Bu kapsamda üye ülkelerden birisi terörist saldırıların hedefi hâline gelirse, diğer üye ülkeler Avrupa Zirvesinin 2014/415/EU kararına dayanarak saldırıya maruz kalmış ülkeye destek verebilecektir. Hibrit tehditlere yönelik olarak kararın alınmasında gecikme bulunması halinde Zirve'nin karar alması beklenilmeyecek Komisyon ve Yüksek Temsilcilerin değerlendirme yapması istenecektir (European Commission, 2022). Yaşanan gelişmelere bağlı olarak büyük çoğunluğu NATO üyesi olan Birlik ülkelerince hibrit tehditlerle mücadele NATO bünyesinde de devam ettirilmiştir. NATO'nun 2014 yılında gerçekleşen Galler Zirvesi'nde siber saldırılara karşı 5. Madde kapsamına harekete geçilebileceği bildirilmiştir. NATO'nun 2021'de gerçekleşen Brüksel Zirve'sinde ise hibrit savaş kapsamında üye devletlere bir saldırı oluştuğunda 5. Madde kapsamında karşı harekete geçileceği bildirilmiştir.

Krize cevap vermenin askerî boyutunda ise, hibrit tehditlere yönelik olarak askerî birliklerin oluşturulması, teçhiz edilmesi ve eğitimlerinin yaptırılması gelmektedir. Ortak Güvenlik ve Savunma Politikası kapsamında;

- Sivil-asker müşterek eğitimlerin yapılması,
- Tehdit edilen ülke güvenliği ve savunma politikalarını geliştirmeye yönelik danışma görevlerinin yapılması,
- Hibrit tehditleri önceden belirleyecek yeteneklerin geliştirilmesine yönelik acil durum planlarının yapılması,
- Acil durumlarda sınır kontrol yönetimi,
- KBRN ve sivillerin tahliyesi gibi özellikli konulara önem verilmektedir (European Commission, 2016).

NATO ile iş birliğinin artırılması başlığında, hibrit tehditlerin sadece Birlik güvenliğini etkilemediği, AGİT, BM ve NATO gibi uluslararası organizasyonları da etkilediği ifade edilmiştir. Bu kapsamda NATO ile daha yakın ilişkiler kurulması hibrit tehditlere karşı etkili bir şekilde hazırlık yapılabilmesi ve müdahale edilebilmesi için önem kazanmaktadır (European Commission, 2016).

Görüleceği üzere AB'nin hibrit tehditlere yanıtı sadece askerî alanda sınırlı kalmayarak, gıdadan, enerjiye, sağlıktan, sınır kontrolüne, siber güvenlikten, ulusal, bölgesel ve uluslararası ilişkilere varacak şekilde birçok kurumunu ve prosedürünü sorgulamasına yol açmıştır.

Hibrit Tehditlere Karşı AB ve NATO İş birliği

Haziran 2016'da yayınlanan Avrupa Birliği Küresel Stratejinde NATO ile iş birliği ihtiyacı vurgulanmıştır (The European Union External Action Service, 2016). Temmuz 2016'da Varşova'da gerçekleştirilen NATO zirvesinde yayımlanan AB-NATO ortak bildirisinde;

- Hibrit tehditlere karşı koyma,
- Operasyonel iş birliğini genişletme ve uyarlama,
- Siber güvenlik ile savunma alanında koordinasyonu artırma,

- Tutarlı ve tamamlayıcı, karşılıklı çalışabilir savunma kabiliyetleri oluşturma,
- Daha güçlü savunma sanayi oluşturma ve tatbikatlara yönelik koordinasyonun artırılması,
- Savunma ve güvenlik kapasitelerinin oluşturulması,
- Ortak ülkelerin dayanımını artırma olmak üzere yedi alanda iş birliğine gidileceği bildirilmiştir (European Council, 2016).

NATO ve AB iş birliği kapsamında, 6 Aralık 2016'da yapılan ortak bildiride Hibrit Mükemmeliyet Merkezi'nin (Hybrid Center of Excellence) kurulmasını destekleyeceklerini bildiriştir. Ortak bildiride merkezin amacının hibrit tehditlerle mücadelede ülkelerin dayanıklılığını artırmak, kapasitelerini geliştirmek, uygulamaları yürütmek, eğitim ve tatbikatlar icra etmek olduğu ifade edilmiştir. Ayrıca özel şirketler ve kamu kurumları ile sivil, asker ve akademisyenleri bir araya getirerek fikir alışverişinin artırılması sağlanacağı belirtilmiştir. Merkez 11 Nisan 2017 tarihinde kurulmuştur (Hybrid Coe, 2022).

2016 ve 2017'de AB ve NATO Hibrit tehditlere karşı koyma, siber güvenlik savunma alanında iş birliğine yönelik olarak dört konu üzerinde durmuştur. Öne çıkan konular durumsal farkındalık, stratejik iletişim, krize müdahale ve dayanımın arttırılması, siber güvenlik ve savunmadır (2021, s. 4).

Hibrit tehditlere karşı koyma kapsamında geliştirilen uygulamalar ele alındığında birinci olarak, durumsal farkındalığın geliştirilmesi esas alınmıştır. Durumsal farkındalık[16] başlığı kapsamında, Mayıs 2017'den itibaren Avrupa Birliği Hibrit Birleştirme Hücresi ve NATO Hibrit Analiz Birimi (The NATO Hybrid Analysis Branch)[17] arasında iş birliğinin sağlanarak karşılıklı bilgi alışverişinin sağlanması kararlaştırılmıştır. Yayımlanan üçüncü ilerleme raporunda istihbarat birimleri arasında eşgüdümün sağlandığı ve böylelikle ortak durumsal resmin oluşturulabileceği bildirilmiştir. Aynı ilerleme raporunda Avrupa Birliği Hibrit Birleştirme Hücresi, NATO Hibrit Analiz Birimi ve Hibrit Mükemmeliyet Merkezi arasında bilgi alışverişinde bulunulduğu bildirilmiştir (2018, s. 2). Dördüncü ilerleme raporuna göre hibrit tehditlere yönelik olarak gerçekleştirilen tatbikatlar esnasında AB ve NATO irtibat subaylarının birbirlerinin karargâhlarına iştirak ettiği bildirilmiştir (2019, s. 2).

AB ve NATO Hibrit tehditlerle iş birliğine yönelik olarak tanımlanan ikinci başlık, stratejik iletişimdir. Stratejik iletişimin geliştirilmesi kapsamında, özellikle Hibrit Birleştirme Hücresi ve NATO Hibrit Analiz Biriminin dezenformasyonlar kapsamında resmi veya resmi olmayanlar görüşmeler yaparak, görüş alışverişinde bulundukları ve ortak resmi tanımladıkları bildirilmiştir. Ayrıca dezenformasyon konusunda Avrupa Dış İlişkiler Servisi yetkilileri ve NATO yetkilileri tarafından karşılıklı karar vericilere bilgi verilmektedir (The European Union, 2022, s. 2). Stratejik iletişim kapsamında iş birliğine yönelik olarak kabiliyetlerin AB ve NATO dışında olan Tunus, Moldova ve Bosna Hersek'te kapasite geliştirici faaliyetlerin artırılmasına odaklanılmaktadır. Hibrit Mükemmeliyet Merkezi'nin NATO

[16] Durumsal farkındalık bir bireyin, organizasyonun veya devletin coğrafi ve siber uzay dâhil olmak üzere, güvenliğini etkileyebilecek olaylardan, gelişmeler ve tehditlerin farkında olabilmesidir

[17] NATO hibrit tehditlere karşı savunma stratejisini hazırlanma, caydırma ve savunma üzerine kurgulamıştır. Hazırlanma adımı kapsamında NATO birimleri hibrit aktiviteleri takip etmekte, bunula ilgili bilgileri NATO karargâhına bağlı Müşterek İstihbarat ve Güvenlik Birimine (Joint Intelligence and Security Division) aktarmaktadır. Müttefik ülkelerden gelen hibrit tehdit bilgileri NATO Hibrit Analiz Birimi tarafından analiz edilerek, karar vericilere tehdit ile ilgili bilgi sunulmaktadır (NATO, 2022).

Stratejik İletişim Mükemmeliyet Merkezi (NATO Strategic Communication Center of Excellence) ve Avrupa Birliği Dış ilişkiler Servisine bağlı Stratejik İletişim Merkezi'nin (Strategic Communication Center) iş birliğinin artırılması sağlanmıştır. Hibrit Mükemmeliyet Merkezi'nin ortak eğitimler ve yeni kavramlar geliştirme yeteneğine dayanarak ilerleme sağlanmaktadır (The European Union, 2022, s. 4).

Krize Müdahale Başlığı altında, karargâh personelleri seviyesinde düzenli toplantılara katılım sağlanarak krize hazırlığın artırılması sağlanmıştır. Hibrit Mükemmeliyet Merkezi tarafından düzenlenen üst seviye toplantılar, seminerler ve bilgilendirmelere her iki tarafın karargâh personelinin katılımı sağlanarak krize hazırlık seviyesinin yükseltilmesi amaçlanmaktadır. Bu başlık altında dikkat çeken bir diğer gelişme ise AB ve NATO'nun tatbikatlara karşılıklı katılımlarının sağlanmasıdır. Covid 19 salgınıyla birlikte artan dezenformasyona karşı koyma, lojistik desteğin sağlanması ve siber güvenliğin önemi bir kez daha öne çıkmıştır (NATO, 2021, s. 5).

Dayanıklılığı artırmak başlığı altında, devletlerin güvenlik kapasitelerinin artırılması ve var olan hassasiyetlerinin giderilmesinin önemi ortaya konulmaktadır. Bu kapsamda, gelişen teknolojilere yönelik olarak verilen, siber güvenliğin artırılması gibi eğitimlere, AB ve NATO personellerinin de katılması ve bilgi sahibi olması amaçlanmaktadır (The European Union, 2022, s. 5). Hibrit Mükemmeliyet merkezinin yapmış olduğu senaryo temelli tatbikatlarla, AB ve NATO personellerinin krizi yönetme kapasitelerinin gelişmesine katkı sağlanmaktadır. Uzay çalışmaları kuvvet çarpanı olarak ön plana çıktığından, 2020 yılında, AB'nin acil durumlara yönelik olarak uzayda iş birliği çalışmalarına NATO personeli de dâhil edilmektedir. İki örgütün de sahip olduğu savunma kabiliyetlerinin gelişmesine yönelik olarak geliştirilen planların uyumlandırılması konusunda çalışmalar yapılmaktadır. İki örgütün acil müdahale kurumlarının gerektiği takdirde müşterek bir şekilde çalışabilmesi için eğitimler, tatbikatlar ve planlar geliştirilmiştir (Latici, 2020, s. 7). Kritik altyapıların, enerji santrallerinin korunmasına yönelik çalışmalar gözden geçirilmekte ve iki örgütün de sahip olduğu sağlıkla ilgili sivil askerî yetenekler konusunda çalışmalarda bulunulmaktadır (NATO, 2019, s. 4). Ayrıca iki örgütün de yurtdışında görev yapan birlikleri arasında rolleri ve eşgüdümleri konusunda çalışmalar yapılarak aralarındaki iş birliği artırılmıştır (NATO, 2021, s. 10).

Siber güvenlik ve savunma, AB ve NATO iş birliği kapsamında öne çıkan bir diğer başlıktır. Siber savunma kabiliyetlerinin geliştirilmesi kapsamında siber tehditler konusunda kurumlar ve personeller arasında bilgi değişimleri sağlanması için bilgilendirmeler, çalıştaylar, toplantılar yapılmaktadır. İki örgütün de siber güvenlik kapsamında eğitim ihtiyacının belirlenmesine yönelik çalışmalar yapılarak, eğitimlerin ve tatbikatların icra edilmesi sağlanmaktadır. Siber güvenlik alanında araştırma, geliştirme ve yeniliğin geliştirilmesi için AB, NATO ve NATO'nun İşbirlikçi Siber Savunma Mükemmeliyet Merkezi arasında çalışmalar yapılmaktadır. Siber güvenliğin sağlanmasına yönelik olarak NATO ve AB siber güvenlik müdahale timlerinin koordinasyonuna yönelik olarak teknik düzenlemeler gerçekleştirilmiştir (NATO, 2019, s. 5).

Hibrit Savaş Bağlamında AB ve NATO İşbirliği'nin Değerlendirilmesi

Temmuz 2016'da gerçekleştirilen NATO zirvesinde yayımlanan AB ve NATO ortak bildirisinde iş birliği vurgulanmış ve bu kapsamda ilerlemeler kaydedilmiştir. Bu kapsamda yedi ilerleme raporu yayımlanmıştır.

Birinci ilerleme raporunda hibrit tehditlerle mücadelenin her zamankinden daha fazla önem kazandığı, NATO'nun Kuzey Atlantik Konseyi ve AB'nin Siyasi ve Güvenlik Komitesi

arasında karşılıklı bilgilendirmeler icra edildiği, iki örgütün de Hibrit Mükemmeliyet Merkezi'nin kurulmasına katkı sağlayacağı ve katılacağı, Birlik ve NATO'nun ilk defa hibrit temelli senaryo tatbikat icra ettiği ifade edilmiştir (2017, s. 3-4).

İkinci ilerleme raporunda bir taraftan iş birliğini geliştirme konusunda kısa vadede somut sonuçlar almak üzerine odaklanılırken, diğer yandan da uzun vadede iş birliğini geliştirecek izleyen adımların atılmasına odaklanıldığı belirtilmiştir. Ortak istihbarat analiz çalışmalarının ilkinin tasnif dışı gizlilik derecesiyle tamamlandığı, izleyen analiz çalışmasının ise planlandığı ifade edilmiştir (NATO, 2017, s. 2).

Üçüncü ilerleme raporunda istihbarat birimleri arasında eşgüdümün sağlandığı ve böylelikle ortak durumsal resmin oluşturulabileceği bildirilmiştir. Aynı ilerleme raporunda Avrupa Birliği Hibrit Birleştirme Hücresi, NATO Hibrit Analiz Birimi ve Hibrit Mükemmeliyet Merkezi arasında bilgi alışverişinde bulunulduğu bildirilmiştir (2018, s. 2).

Dördüncü ilerleme raporuna göre hibrit tehditlere yönelik olarak gerçekleştirilen tatbikatlar esnasında AB ve NATO irtibat subaylarının birbirlerinin karargâhlarına iştirak ettiği bildirilmiştir (NATO, 2019, s. 2).

Beşinci ilerleme raporunda iki örgüt arasında stratejik iletişim kapsamında iş birliğinde bulunulmuştur. Ayrıca 2020 yılı başlarından itibaren Covid 19'la mücadelede iş birliğinde bulunulduğu belirtilmektedir. Covid 19'la mücadele kapsamında yardımların ulaştırılması, dezenformasyonla mücadele ve kara propagandaya karşı koyma, siber güvenlik ve krizin etkilerinin izleyen harekât alanlarına etkileri konularında iş birliğinde bulunulduğu belirtilmiştir (NATO, 2020, s. 2).

Altıncı ilerleme raporunda Covid 19 salgının tüm dünyayı etkilediği, NATO ve AB yetkililerinin bu ortamda dezenformasyonla mücadele, siber tehditlere karşı koyma konularında istişarelerde bulunduğu belirtilmiştir. İki örgütün yetkilerinin bu konuda salgın ortamında hibrit tehditlerle mücadele konusunda görüşmelerde bulunmuşlardır (NATO, 2021, s. 2).

Yedinci ilerleme raporunda Rusya'nın Ukrayna müdahalesi ertesinde, hibrit tehditlere karşı siyasi diyaloğun sürdürüldüğü ve geliştirildiği, AB'nin Siyasi ve Güvenlik Komitesi'yle NATO'nun Kuzey Atlantik Konseyi arasında iş birliğinin artırıldığı belirtilmiştir (The European Council, 2022, s. 12). Ayrıca aynı raporda iki örgütün iş birliğinin hibrit tehditlere karşı istenen kapsamda gelişmesi ve istenilen seviyede koordineli ve tutarlı çalışmaların gerçekleştirilmesi için uzun ve devam edilmesi gereken bir süreç bulunduğu da ifade edilmiştir (The European Council, 2022, s. 13).

Rusya'nın Gürcistan ve Ukrayna'ya müdahaleleri, Birlik ordusuna karşı çıkan İngiltere'nin Brexit kararı alması gibi, Avrupa kıtasındaki yaşanan siyasi ve askerî gelişme ve çekişmeler, Avrupa kıtasında güvenlik algılarının sorgulanmasına yol açmıştır (Nuhut, 2022, s. 114; Çelik, 2022, s. 205). Bu süreçte NATO'nun varlığının sorgulanması, önceden de süregelen bağımsız AB ordusu kurulması tartışmaları, AB'ye üye ülkeler arasında bazı çekincelerin doğmasına neden olmuştur.

AB ve NATO'nun karar alma mekanizması incelendiğinde, NATO ve AB üyesi ülkelerin veto hakları bulunmaktadır. Bu nedenle iki örgütte de üye ülkeler arasında ikili ve çok taraflı ilişkiler karar alınmasını etkilemektedir. İki örgüte de üye ülkeler açısından kendi politik hedeflerine her iki örgüt nezdinde ulaşma imkânı daha kolayken, tek örgüte üye ABD, Finlandiya, Güney Kıbrıs Rum Kesimi, İsveç ve Türkiye açısından her iki örgütün önemli

kararlarına etki etmeleri daha zor olmaktadır. Tek örgüte üye ülkeler açısından örgütler arası faaliyetlere katılım, diğer örgütteki değişimlerden haberdar olması daha yavaş olmakta, iş birliğini etkilemektedir (Ewers-Peters vd. 2023, s. 30).

İkinci çekince Birlik içerisinde ABD ile savunma alanında yakın ilişkiler geliştiren üye ülkelerin varlığıdır (İnat, 2022) . Başta Fransa ve Almanya olmak üzere, AB üyesi ülkeler ABD'den bağımsız savunma politikası gütmek isterken, İsveç, Finlandiya, Orta ve Doğu Avrupa ülkeleri ulusal çıkarlarından dolayı AB ve NATO nezdinde savunma iş birliği politikalarını desteklemektedir (Ewers-Peters vd. 2022, s. 34).

Üçüncü çekince otuz NATO ülkesinin yirmi birinin AB üyesi olması nedeniyle mali kaynak gerektiren ordu kapasitelerinin farklı iki örgüte tahsis edilememesidir (Papaioannou, 2022). Bu hassasiyete yönelik olarak akıllı savunma[18] (Smart Defence) kavramı geliştirilmiştir. Akıllı savunma harcamalarıyla üye ülkeler geliştirecekleri müşterek projeler ile daha az mali kaynak harcayarak daha fazla, savunma yeteneği geliştirmeyi hedeflemişlerdir. Avrupa Savunma Eylem Planı (European Defence Action Plan) uyarınca üye ülkeler Avrupa Savunma Fonu'na (European Defence Fund) müşterek savunma projelerinde araştırma ve geliştirmede kullanılmak üzere fon aktarmayı kabul etmektedir (Raik vd. 2017, s. 19).

Dördüncü çekince ise NATO ve AB nezdinde Güney Kıbrıs Rum Kesimi ve Türkiye gibi üye ülkelerin birbiri arasında tarihten gelen anlaşmazlıklarının bulunmasıdır. AB üyesi ancak NATO üyesi olmayan Güney Kıbrıs Rum Yönetimi, NATO üyesi ve AB üyesi olmayan Türkiye arasındaki Kıbrıs sorunu ve buna bağlı yaşanan gerginlikler, iki örgütün tam kapasitede bilgi paylaşımında bulunmasında, ortak tatbikatların icra edilmesinde ve savunmada iş birliğinin oluşturulmasına engel teşkil edebilmektedir (Tardy & Lindstrom vd. 2019, s. 11).

Sonuç

Soğuk savaşın ertesinde küreselleşmenin ve teknolojinin etkisiyle, öncelikle devletlerin güvenlik aktörü olarak görev aldıkları güvenlik ortamı yerini, çok aktörlü (askerî birlikler, terörist unsurlar, yabancı savaşçılar, organize suç örgütleri vb.), daha az maliyetli ve istenen sonuca daha kısa sürede ulaşmayı amaçlayan, sınırları, cephesi ve muharebe sahası belli olmayan, sivil ve asker ayrımının olmadığı, hibrit savaş ortamına bırakmıştır.

AB'nin hibrit tehditlere yanıtı yeni bir olgu olmamakla beraber, özellikle Rusya'nın Kırım'ı ilhakı, Suriye İç Savaşı'ndan kaynaklanan düzensiz göçmen krizi ve yabancı terörist savaşçıların Birlik içerisinde yapmış olduğu eylemlerin artmasıyla hız kazanmıştır. AB Komisyonu'nun 6 Nisan 2016'da yayınlamış olduğu "Hibrit Tehditler Karşı Koyma Ortak Çerçevesi-Avrupa Birliği Yanıtı" ortak iletişim belgesinde dünyada tehdit ortamının değiştiğine vurgu yapılmıştır. Adı geçen belge, günümüz hibrit ortamının AB tarafından nasıl algılandığını anlamak ve Birliğin tehditlere nasıl önlemler aldığını görmek açısından önemlidir. Belgede Balkanlar'da ve Avrupa'nın güneyinde yaşanan gelişmelerin Avrupa kıtasının güvenliğini nasıl etkilediği belirtilmiştir. Üye ülkelerce hibrit tehditlere karşı alınacak tedbirler ve NATO iş birliğine işaret edilmiştir. Üye ülkelerden tehditlerin

[18] Akıllı Savunma: Ülkelerin aynı konularda ayrı olarak harcama yapmalarının önüne geçilmesi ve müşterek hareket etmelerinin sağlanmasıdır. Böylece savunma ihtiyaçlarına daha az kaynak ayırarak daha fazla savunma yeteneği geliştirilmesinin sağlanmasını amaçlamaktadır (Grand, 2012, s. 45)

tanımlanması, farkındalığın artırılması, dayanıklılığı inşası, önleme, krize cevap verme ve yenilenme adımlarını içerecek faaliyetlerin uygulanması istenmiştir.

Temmuz 2016'da gerçekleştirilen NATO zirvesinde yayımlanan AB ve NATO ortak bildirisinde hibrit tehditlere karşı koyma, operasyonel işbirliğini genişletme ve uygulama, siber güvenlik ve savunma alanında koordinasyonu artırma, bütünleyici, tutarlı ve tamamlayıcı savunma kabiliyetleri oluşturma, daha güçlü savunma sanayi oluşturma, tatbikatlarda koordinasyonun artırılması, savunma ve güvenlik kapasitelerinin oluşturulması, ortak ülkelerin dayanımını artırma olmak üzere yedi alanda işbirliğine gidileceği bildirilmiştir.

Temmuz 2016 da gerçekleştirilen NATO zirvesinde yayımlanan AB NATO ortak bildirisindeki iş birliği alanları, özellikle Rusya'nın Kırımı işgali sonrasında gelişen ve değişen güvenlik ortamında iki örgütün iş birliğinin nasıl geliştirebileceğine yönelik olarak stratejik yol haritası niteliğindedir. Nitekim bu yol haritası kapsamında hibrit tehditlere karşı iş birliğine yönelik olarak 2016 ve 2017 de bazı başlıklar öne çıkmaktadır. Bunlar;

- Durumsal farkındalık,
- Stratejik iletişim,
- Krize müdahale ve dayanımın arttırılması,
- Siber güvenlik ve savunmadır.

Bu başlıklar kapsamında faaliyetlerin gerçekleştirilmesiyle AB ve NATO kurumlarıyla üye ülkeleri arasındaki iş birliğinin geliştirilmesi hedeflenmiştir. Bugüne kadar NATO ve AB iş birliğinin geliştirilmesi yönelik olarak 7 ilerleme raporu yayınlanmıştır

Avrupa Birliği ve NATO'nun hibrit tehditlere karşı iş birliğine kararı verdiği zirveden günümüze yayımlanan yedi ilerleme raporu değerlendirildiğinde, bugün gelinen noktada kaydedilen ilerlemelerin iki örgüt temsilcilerinin temas düzeyinin geliştiği ayrıca ortak tatbikatlara katılım, siyasi temaslar ve bilgi değişimi konusunda ilerleme kaydedildiği görülmektedir. Özellikle iki tarafında katılabildiği, Helsinki de kurulan Hibrit Mükemmeliyet Merkezinin hayata geçmesiyle AB ve NATO arasında iş birliğinin arttığı, bilgi değişimleri, elde edilen tecrübelerin ve araştırmaların paylaşımı konusunun ivme kazandığı değerlendirilmektedir. Ayrıca Dünyayı etki altına alan Covid 19 salgının iki örgütün iş birliğine ivme kazandırdığı, özellikle dezenformasyonla mücadele, stratejik iletişim, kara propagandaya karşı koyma, siber tehditlerle mücadele konularında iş birliğine gidildiği gözlemlenmektedir. Öte yönden örgütlerin stratejik düzeyde iş birliğinin gelişmesi için siyasi irade desteğinin üye ülkelerin ulusal çıkarlarından, tehdit algılamalarının farklılıklarından ve bilgi değişimi konusundaki çekincelerinden ötürü yetersiz kaldığı değerlendirilmektedir. Yedinci İlerleme raporunda da belirtildiği üzere iki örgütün iş birliğinin hibrit tehditlere karşı istenen kapsamda gelişmesi için tamamıyla koordineli ve tutarlı çalışmaların gerçekleştirilmesi temelinde uzun ve devam edilmesi gereken bir süreç bulunmaktadır.

Hibrit tehditlerle değişen güvenlik çevresi, güvenliğin sürekli sorgulanmasına yol açmaktadır. Son döneme kadar, Avrupa Birliği'nin güvenlik politikası daha çok AB komşuluk politikasıyla etrafındaki hassas bölgeleri kuvvetlendirmesine ve yumuşak gücüne dayanırken, NATO'nun güvenlik politikası ise daha çok gelecek bir silahlı tehdide karşılık bireysel ve kolektif müttefik ülkelerin kapasitelerin geliştirilmesine yani sert gücüne bağlanmıştır. Savaşın yasal olabilmesi NATO antlaşmasının 5. Maddesinin işletilmesine bağlanmıştır. Savaş ortamının değişmesi hibrit tehditlere karşı yalnızca yumuşak veya sert gücün yeterli

gelmemesi nedeniyle, AB ve NATO'da hibrit tehditlere hazır olup olmadığının sorgulanmasına yol açmıştır. Bu kapsamda NATO'nun 2014'te gerçekleşen Galler Zirve'sinde siber saldırılara karşı, 5. Madde kapsamında harekete geçilebileceği bildirilmiştir. NATO'nun 2021'de gerçekleşen Brüksel Zirve'sinde ise hibrit savaş kapsamında üye devletlere bir saldırı oluştuğunda 5. Madde kapsamında karşı harekete geçileceği bildirilmiştir. Görülmektedir ki, var olan tehditlerdeki değişmeler, örgütlerin de canlılar gibi varlıklarını devam ettirmeleri için çevreye uyum sağlamalarına yol açmakta, tehditlerden korunmak için tedbir almaya yöneltmektedir.

Sonuç olarak, hibrit savaşın beraberinde getirmiş olduğu değişim her iki organizasyonun güçlü ve zayıf taraflarını ortaya çıkarmıştır ve iş birliğini hızlandırmıştır. Hali hazırda NATO'nun 30 üyesinden hemen hemen üçte ikisinin AB üyesi ülkeler olduğu düşünüldüğünde, NATO ve AB birbirinin alternatifi değil, aksine tamamlayıcısıdır. NATO tehditlere karşı kullanabileceği sert gücü ile ön plana çıkarken, AB ise daha çok yumuşak gücü ile ön plana çıkmaktadır. Bu sebeple birbiriyle örtüşen iki örgüt arasında planlamaların uyumlanmasına ve iş birliğine ihtiyaç duyulmaktadır. İki örgütün iş birliğinin artırılması konusunda;

- Ortak hibrit tehditlerin açıkça ortaya konması ve bu tehditlerin stratejik seviyede ele alınarak, daha tutarlı politikalar geliştirilmesi,
- İki örgütün güç kapasitelerinin ortaya konularak, hangi tehdide, nasıl müşterek cevap verilebileceğine yönelik tedbirler geliştirilmesi,
- Tehdit tanımları arasındaki farklılıkların giderilerek, çözüm yollarının görüşme, dostça girişim, arabuluculuk vb. siyasi temaslarla aranması, böylelikle bilgi değişimi konusunda çekincelerin ortadan kaldırılması,
- Geleceğe yönelik senaryoların oluşturularak, ortak tatbikatlarda denenmesi ve krize cevap verme konusunda hassasiyetlerini giderilmesi,
- Siber tehditlerle mücadele boyutunda iki örgütün kurumları arasında iş birliğinin geliştirilerek gerektiği takdirde ortak merkezde birleştirilmesi gibi konulara daha fazla odaklanılması gerekmektedir.

KAYNAKÇA

ARQUILA, J. (2005). "Netwar Revisited: The Fight for Future Continues". *Network Terrorism and Global Insurgency.* (ed. R. Bunker). New York: Routledge Group: 8-19

GÜRCAN, M. (2012). "Savaşın Evrimi ve Teorik Yaklaşımlar". *Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri.* (ed. A. Sandıklı). Ankara: Bilgesam Yayınları: 69-129.

HOFFMAN, F. (2006). *Lessons Form*. Lebanon: Hezbollah and Hybrid Wars.

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

HORN, C. B. (2016). *On Hybrid Warfare.* Ottawa: Minister of National Defence.

HUBER, T. M. (2002). "Compound Warfare: A Conceptual Framework". *Compound Warfare: That Fatal Knot. Fort Leavenworth.* (ed. T. M. Huber). Kansas: U.S. Army Command and General Staff College Press: 1-9.

JACOBS, A. - G. LASCONJARIAS (2015). "NATO's Hibrid Flanks Handling Unconventional Unconventional Warfare in South and East". *Research Paper No. 112*. Roma: Research Division-Nato Defense College: 1-12.

BOOT, M. - M. DORAN (2013). "Political Warfare- Policy Innovation Memorandum N. 33". *Council on Foreign Relations*: 1-4.

BOWERS, C. O. (2012). "Identifying Emerging Hybrid Adversaries". *Parameters*: 39-50.

BUZAN, B. (2008). "Askerî Güvenliğin Değişen Gündemi". *Uluslararası İlişkiler.* V/18: 107-123.

CLAUSEWITZ, C. V. (2019). *Savaş Üzerine.* İstanbul: Alfa Yayınları.

CREVELD, M. V. (1991). *The Transformation of War.* New York: The Free Press.

CREVELD, M. V. (1999). *The Rise and Decline of the State.* Cambridge: Cambridge University Press.

ÇALKIVİK, A. (2014). "Soğuk Savaş ve Sonrası Güvenlik Siyaseti". *Küresel Siyasete Giriş: Uluslar Arası İlişkilerde Kavramlar, Teoriler Süreçle*. (ed. E. Balta). İstanbul: İletişim Yayınları: 281-299.

DEDEOĞLU, B. (2014). *Uluslararası Güvenlik ve Strateji.* İstanbul: Yeni Yüzyıl Yayınları.

EKER, S. (2015). "Savaş Olgusunun Dönüşümü: Yeni Savaşlar ve Suriye Krizi Örneği". *Türkiye Ortadoğu Çalışmaları Dergisi*. II/1: 33-66.

EROL, M. S. - Ş. OĞUZ (2018). "Karma Savaş Teorisi ve Rusya-Ukrayna Savaşı". *Türk Dünyası İncelemeleri Dergisi.* XVIII/2: 399-415.

GÖK, A. (2019). *Hibrit Savaşlar: Rusya'nın Afganistan (1979) ve Ukrayna (2014) Askerî Müdahaleleri ile İsrail-Lübnan Savaşları (1982, 2006) Örnek Olayları Işığında Tarihsel-Mukayeseli Bir İnceleme.* Ankara: Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü. (Yayımlanmamış Doktora Tezi).

KÄİHKÖ, I. (2021). "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession". *The US Army War College Quarterly: Parameters.* LI/3: 115-127.

KALDOR, M. (2003). *Global Civil Society: An Answer to War.* Cambridge Polity.

KALDOR, M. (2012). *New and Old Wars.* Cambridge: Polity Press.

KALDOR, M. (2013). *Defence of New Wars.* Stability. II/1: 1-16.

KARAOSMANOĞLU, A. L. (2015). "Savunma Planlaması ve Stratejik Belirsizlik". *Bilge Strateji.* VII/12: 23-45.

KINROSS, S. (2004). "Clausewitz and Low-Intensity Conflict". *Journal of Strategic Studies.* XXVII/1: 35-58.

KOFMAN, M. - M. ROJANSKY (2015). "A Closer Look at Russia's "Hybrid War"". *Kennan Cable*: 1-8.

LIANG, Q. - W. XIANGSUI (1999). *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House.

LIND, W. (2004). "Understanding Fourth Generation Warfare". *Military Review*: 13-14.

LIND, W. S. vd. (1989). "The Changing Face of War: Into the Fourth Generation". *Marine Corps Gazette*: 22-26

MANSOOR, P. R. (2012). "Hybrid Warfare in History". *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present.* (ed. W. Murray-P. R. Mansoor). New York: Cambridge University Press: 1-17.

McFATE, M. - A. V. JACKSON (2006). "The Object Beyond War: Counterinsurgency and the Four Tools of Political Competition". *Military Review* (January-February).

MÜNKLER, H. (2010). *Yeni Savaşlar - Die neuen Kriege.* 1. Baskı. (çev. Z. A. Yılmazer). İstanbul: İletişim Yayınları.

NATO (2016). "Social Media as A Tool of Hybrid Warfare". *NATO Strategic Communications Centre of Excellence*: 10.

NATO (2016). *Social Media as A Tool of Hybrid Warfare.* Riga: NATO Strategic Communications Centre of Excellence.

NEMETH, W. J. (2002). "Future War and Chechnya: A Case for Hybrid Warfare". *Master of Arts in National Security Affairs from the Naval Postgraduate School*. California: Naval Postgraduate School.

NUHUT, Ö. (2022). "AB Ordusu Kurma Çabaları Nereye Evrildi ve NATO'yla Birlikte Nereye Evrilebilir? *Cappadocia Journal of Area Studies.* 4/1: 112-130.

PATREUS, D. (2010). "What we Learned in Iraq". *Global Policy*. I/1: 116-117.

EWERS-PETERS, N. M. (2023). "Positioning Member States in EU-NATO Security Cooperation: Towards a Typology. *European Security*. 23/1: 22-41.

RAIK, K., - P. JÄRVENPÄÄ (2017). *A New Era of EU-NATO Cooperation How to Make the Best of a Marriage of Necessity.* Tallinn: International Centre for Defence and Security.

LATİCİ, T. (2020). *Understanding EU-NATO Cooperation Theory and Practice, European Parlaiment Briefing.* European Parlaimentary Research Service.

TARDY, T. - G. LINDSTROM (2019). "The Scope of EU-NATO Cooperation". *NATO and the EU-The Essential Partners*. Luxembourg: European Union Institute for Security Studies (EUISS): 5-12.

TOFFLER, A. (1993). *War and Anti-War: Survival at the Dawn of the 21st Century.* Boston: Little Brown Company.

TÜRKGENCI, Y. - H. SAYAT (2018). "Komuta ve Kontrol". *Savaşın Değişen Modeli: Hibrit Savaş*. İstanbul: Milli Savunma Üniversitesi: 63-70.

VARLIK, A. B. (2013). "Savaşı Tanımlamak: Terminolojik Bir Yaklaşım". *Avrasya Terim Dergisi.* I/2: 114-129.

WHEATLY, G. F. (1996). "Information Warfare and Deterrence". *NDU Press Book*: 1-8.

WIJK, R. D. (2012). "Hybrid Conflict and the Changing Nature of Actors". *The Oxford Handbook of War*. (ed. Y. Boyer- J. Lindley French). Oxford: Oxford University Press: 358-373.

Zİ, S. (2020). *Savaş Sanatı.* İstanbul: Türkiye İş Bankası Kültür Yayınları.

İnternet Kaynakları

AKEKER, F. A. (2019). "Haklı Savaş". *Güvenlik Portalı*. Erişim Tarihi: 18.10.2019.

https://trguvenlikportali.com/wpcontent/uploads/2019/10/HakliSavas_FulyaAksuEreker_v.1.pdf

ARMITAGE, R. L. - J. NYE (2022, 11 17). "CSIS COMMISSION On Smart Power: A Smarter More Secure America". *Carnegie Endownmentt*. Erişim Tarihi: 17.11.2022.

https://carnegieendowment.org/files/csissmartpowerreport.pdf

BIÇAKÇI, S. (2019). *Hibrit Savaş.* 26.09.2022 tarihinde Güvenlik Portalı. Erişim Tarihi: 18.11.2019.

https://trguvenlikportali.com/wpcontent/uploads/2019/11/HibritSavas_SalihBicakci_v.1.pdf

CEBROWSKI, A. K. - J. H. GARSTKA (2022). "Network-Centric Warfare - Its Origin and Future". *U.S. Naval Institute*. Erişim Tarihi: 18.10.2022.

https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future

CERT-EU (2022). *The Computer Emergency Response Team for the EU Institutions*. Erişim Tarihi: 27.08.2022.

https://cert.europa.eu/about-us

CORBEIL, A. (2022). "Russia is Learning About Hezbollah". *Carniege Edwment for International Peace*. Erişim Tarihi: 15.05.2022.

https://carnegieendowment.org/sada/67651

Council of the European Union (2014). *On the Arrangements for the Implementation by the Union of the Solidarity Clause (2014/415/EU) Article5.* Erişim Tarihi: 27.08.2022.

https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A32014D0415

Council of The European Union (2020). "Joint Staff Working Document". *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*. Erişim Tarihi: 31.07.2020.

https://www.eumonitor.nl/9353000/1/j4nvgs5kjg27kof_j9vvik7m1c3gyxp/vlau7deud1z5/f=/10047_20.pdf

ÇELİK, Ü. (2022). *AB'nin Küresel Stratejisi ve AB Ordusu Tartışması.* Erişim Tarihi: 17.11.2022.

https://dergipark.org.tr/en/download/article-file/700843

ENISA (2022). "About ENISA". *The European Union Agency For Cyber Security*. Erişim Tarihi: 17.11.2022.

https://www.enisa.europa.eu/about-enisa

ERKMEN, S. (2019). "Silahlı Güçler; Ordular, Para-Militer Yapılar, Özel Askerî Şirketler". *Güvenlik Portalı*. Erişim Tarihi: 01.11.2019.

https://trguvenlikportali.com/wpcontent/uploads/2019/11/SilahliGucler_SerhatErkmen_v.1.pdf

European Commission (2015). "Review of the European Neighbourhood Policy". E*uropean Commission*. Erişim Tarihi: 18.10.2015.

https://neighbourhoodenlargement.ec.europa.eu/system/files/201812/jointcommunication_review-of-the-enp.pdf

European Commission (2016). "FAQ: Joint Framework on Countering Hybrid Threats". *European Commission - Fact Sheet*. Brussels: European Commission. Erişim Tarihi: 06.04.2016.

https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250

European Commission (2016). "Joint Framework on Countering Hybrid Threats: A European Union Response Preventing, Responding to Crisis and Recovering"*. EUR-LEX*. Erişim Tarihi: 06.04.2016.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

European Commission (2016). "Joint Framework on Countering Hybrid Threats: A European Union Response, Increasing Cooperation with NATO"*. European Commission*. Erişim Tarihi: 06.04.2016.

https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52016JC0018

European Commission (2022). *European Emergency Response Coordination Centre*. Erişim Tarihi: 27.08.2022.

https://civilprotectionhumanitarianaid.ec.europa.eu/what/civilprotection/emergency-response-coordination-centre-ercc_en

European Commission (2022). "Radicalisation Awareness Network"*. European Commission Website*. Erişim Tarihi: 27.08.2022.

https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran_en

European Council (2016). *Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization* (Warsaw: 8 July 2016). European Council. Erişim Tarihi: 27.05.2016.

https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

European Union (2007). "Treaty on the Functioning of the European Union Solidarity Clause"*. European Union Website*. Erişim Tarihi: 27.12.2007.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:solidarity_clause

European Union External Action Service (2018). "A Europe That Protects: Countering Hybrid Threats". *European Union External Action Service*. Erişim Tarihi: 27.12.2018.

https://www.eeas.europa.eu/sites/default/files/hybrid_threats_en_final.pdf

EXCELLENCE, C. O. (2022). "Financial Intelligence Units". *Centre of Excellence*. Erişim Tarihi: 27.08.2022.

https://www.coe.int/en/web/moneyval/implementation/fiu#:~:text=The%20global%20efforts%20to%20establish,the%20structures%20enforcing%20criminal%20legislation

GERASIMOV, V. (2013, 5 15). "The Value of Science in the Foresight". *Military Review*: 23-29. Erişim Tarihi: 17.05.2013.

https://www.timeturk.com/gerasimov-doktrini-hibrit-savas-nedir/haber-1370717

GRAND, C. (2012). "Smart Defense". *Smart Defense and The Future of NATO*. Chicago: Chicago Council on Global Affairs: 45. Erişim Tarihi: 30.03.2012.

https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/Conference_Report.pdf

HOFFMAN, F. (2014). "On Not So New Warfare: Political Warfare Vs Hybrid Threats". *Texas Nation Security Review*. Erişim Tarihi: 28.06.2014.

https://waron therocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/

HOFFMAN, F. G. (2022). "On Not So New Warfare: Political Warfare Vs Hybrid Threats". *Armed Sources Journal*. Erişim Tarihi: 28.05.2022.

https://waron therocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/

HOFFMAN, F. - A. ORNER (2021). *The Return of Great Power Proxy Wars*. Texas National Secutiy Review. Erişim Tarihi: 02.09.2021.

https://warontherocks.com/2021/09/the-return-of-great-power-proxy-wars/

Hybrid Coe (2022). *Hybrid Center of Excellence*. Erişim Tarihi: 27.12.2022.

https://www.hybridcoe.fi/who-what-and-how/

İNAT, K. (2022). "PESCO ve NATO: Hangisi Daha İleri İş Birliği*"*. *SETAV*. Erişim Tarihi: 27.05.2022.

https://www.setav.org/pesco-ve-nato-hangisi-daha-ileri-is-birligi/

MATTIS, J. N. - F. HOFFMAN (2005). "Future Warfare: The Rise of Hybrid Wars Remember General Krulak's Three Block War? Are You Ready for the Four Block War? You Better Be, Says General James Mattis"*. US Naval Institude.* Erişim Tarihi: 12.09.2022.

https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars

MAXWELL, D. (2014). "Taking a Spoon to a Gunfight: The West Dealing with Russian Unconventional and Political Warfare in Former Soviet States". *Texas National Securit Review*. Erişim Tarihi: 27.12.2014.

https://warontherocks.com/2014/04/taking-a-spoon-to-a-gunfight/

MCCONOLY, R. (2022). *Newtwork Centric Warfare*. Naval Post. Erişim Tarihi: 18.11.2022.

https://navalpost.com/what-is-network-centric-warfare/

NATO (2017). "First Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016". *NATO*. Erişim Tarihi: 14.06.2017.

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170619_170614-Joint-progress-report-EU-NATO-EN.pdf

NATO (2017). "Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016". *NATO*. Erişim Tarihi: 29.11.2017.

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_11/171129-2nd-Joint-progress-report-EU-NATO-eng.pdf

NATO (2018). "Third Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017". *NATO*. Erişim Tarihi: 27.12.2018.

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_1

NATO (2019). "Fourth Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017". *NATO*. Erişim Tarihi: 27.08.2022.

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th

NATO (2020). "Fifth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017". *NATO*. Erişim Tarihi: 16.06.2020.

https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf

NATO (2021). "Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017". *NATO*. Erişim Tarihi: 16.12.2021.

https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-N

NATO (2022). *Comprehensive Approach*. Erişim Tarihi: 15.09.2022.

https://www.nato.int/cps/en/natolive/topics_51633.htm

NATO (2022). "NATO's Response to Hybrid Threats". *NATO*. Erişim Tarihi: 15.05.2022.

https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en

ÖZDAL, H. (2021). "Putin Döneminde Rusya'nın Güvenlik Doktrinleri". *Güvenlik Portalı*. Erişim Tarihi: 26.09.2022.

https://trguvenlikportali.com/wpcontent/uploads/2021/02/PutinRusyasiGuvenlikDoktrinleri_HabibeOzdal_v.1.pdf

PAPAIOANNOU, A. (2022). "Güçlenen AB NATO İşbirliği". *NATO*. Erişim Tarihi: 27.05.2022.

https://www.nato.int/docu/review/tr/articles/2019/07/16/gueclenenabnatoiliskileri/index.html

PERRY, B. (2015). "Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations". *Small Wars Journal*. Erişim Tarihi: 09.09.2022.

https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera

RAY, C. (2022). "Eu Intcen"*. State Watch*. Erişim Tarihi: 18.11.2022.

https://www.statewatch.org/media/documents/news/2016/may/euintcenfactsheet.pdf

SOKULLU, E. C. (2019, 10 22). "Savaş Türleri". *Güvenlik Portalı*. Erişim Tarihi: 22.10.2019.

https://trguvenlikportali.com/wpcontent/uploads/2019/11/SavasTurleri_EbruCananSokullu_v.1.pdf

TDK (2022). "Savaş". *Güncel Türkçe Sözlük*. Erişim Tarihi: 14.09.2022.

https://sozluk.gov.tr/

The Computer Emergency Response Team for the EU Institutions (2022). Erişim Tarihi: 27.08.2022.

https://www.enisa.europa.eu/about-enisa

The European Council (2022). "Seventh Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO". *The European Council.* Erişim Tarihi: 20.06.2022.

https://www.consilium.europa.eu/media/57184/eu-nato-progress-report.pdf

The European Union (2022). "Seventh Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017"*. The European Union Website*. Erişim Tarihi: 09.12.2022.

https://www.consilium.europa.eu/media/57184/eu-nato-progress-rep

The European Union External Action Service (2016). "The EU Global Strategy". *The European Union External Action Service*. Erişim Tarihi: 09.12.2016.

https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

ZANDEE D. vd. (2021). "Countering Hybrid Threats Steps for Improving EU-NATO Cooperation"*. Netherlands Instıtute of International Relations*. Erişim Tarihi: 09.12.2021.

https://www.clingendael.org/pub/2021/countering-hybrid-threats/

EXTENDED ABSTRACT

Since the Cold War, the security environment, in which nations act as main security actors, has been replaced by a multi-actor system (e.g. military units, terrorist elements, foreign fighters, organized crime groups), as it is less expensive and can achieve the desired result in a shorter time. In a hybrid war environment, boundaries, fronts, and battlefields are not apparent, and there is no distinction between civilian and combatants.

Although the EU's response to hybrid threats is not a recent development, it has been more robust – particularly considering Russia's annexation of Crimea, the irregular migration problem brought on by the Syrian Civil War, and the rise in foreign terrorist fighters' activities inside the Union. The threat environment in the globe had led the EU to revise its major "Joint Framework on countering hybrid threats a European Union response" on April 6, 2016. This document is crucial to comprehending how the EU views the hybrid environment of today and how they respond to threats. It also explains how the security of Europe is impacted by the changes in the Balkans and southern Europe, and emphasizing the need for NATO collaboration and the precautions that member states must take against hybrid threats. Member states requested the implementation of various initiatives: threat identification, improving awareness, building resilience, preventing, responding to crisis, and recovering from crisis.

In July 2016, NATO and EU published a joint statement that addressed countering hybrid threats, enhancing operational cooperation, enhancing collaboration in the realm of cyber security and defence, creating complementary, coherent, defence capabilities, strengthening the defence industry, and enhancing coordination in exercises.

The areas of cooperation outlined in the joint statement serve as a strategic road map for how the two organizations can strengthen their collaboration – particularly considering the evolving and changing security landscape following Russia's invasion of Crimea. In reality, some topics related to cooperation against hybrid threats stood out in 2016 and 2017 within the context of this roadmap. Situational awareness, strategic communication, crisis intervention, building resilience, and cyber security and defence are just a few of them.

By carrying out operations under the range of these titles, the overall intention is to strengthen collaboration between EU and NATO and their member nations. Seven progress reports towards that goal have been released to date.

The above said, progress has been made in terms of participation in joint exercises, political contacts, and information sharing, as well as the contact level of the two organizations' representatives. Cooperation between the EU and NATO has improved through information exchanges and experience sharing – namely with the launch of the Helsinki-based Hybrid Center of Excellence, in which both sides can take part. In addition, following the Covid 19 outbreak, the two organizations' are cooperating more than ever, particularly in terms of battling disinformation, creating strategic communication, thwarting black propaganda, and fending off cyber threats. On the other hand, political support for cooperation growth between the two at the strategic level is insufficient because of the national interests of member states, largely due to variations in threat perceptions, and concerns over information sharing. Therefore, the aforementioned the suggestions outlined in Seventh Progress Report need to implemented if this going to work.

The constantly evolving security landscape with hybrid threats causes us to doubt security. The European Union's neighbourhood policy and soft power were the main pillars of its security strategy up until recently. Meanwhile, NATO's security strategy was more dependent on the growth of the capacities of the individual and collective allied countries, specifically hard power, in response to an armed threat. The implementation of Article 5 of the NATO Treaty determines whether war is legal. Since only soft or hard power is insufficient to defeat hybrid threats, the changing nature of warfare has caused some to doubt whether the EU and NATO are even prepared.

In this regard, NATO Wales Summit in 2014 collectively declared that Article 5 action could be taken against cyber attacks. At another NATO summit in Brussels in 2021, it was agreed that Article 5 would be invoked in the event of a hybrid attack on one of the alliance's members. As risks evolve, organizations must adapt to their surroundings to survive – just like all living things. Moreover, they must take precautions to safeguard themselves.

In turn, hybrid war's transformation has shown us both organizations' advantages and disadvantages, and has sped up communication between the two. NATO and the EU are complementary to one another, not alternatives – as nearly two-thirds of NATO's 30 countries are also EU members. The EU takes the lead with its soft power, while NATO stands out with its physical might that it can employ against counter threats. Hence, coordination of planning and collaboration between the two groups is necessary.