

Uluslararası Siyaset ve Siber Güvenlik Dergisi (USSG)

Aralık 2026

Cilt 1, No: 1

USSG, ESUPA tarafından yayımlanan bir akademik e-dergidir.

İmtiyaz Sahibi ve Baş Editör:

Prof. Dr. Ozan ÖRMECİ

https://politikaakademisi.org/uluslararasi-siyaset-ve-siber-guvenlik-dergisi-ussg/



ULUSLARARASI SİYASET VE SİBER GÜVENLİK DERGİSİ (USSG)

ARALIK 2026

CİLT 1 SAYI: 1

E-ISSN:

İmtiyaz Sahibi/Owner:

Prof. Dr. Ozan ÖRMECİ

Baş Editör/ Editor-in-chief:

Prof. Dr. Ozan ÖRMECİ

YAYIN İDARE MERKEZİ / PUBLICATION OFFICE

Alanya, TÜRKİYE

E-posta: esupakurumsal@gmail.com

İnternet sitesi: https://politikaakademisi.org/uluslararasi-siyaset-ve-siber-guvenlik-dergisi-ussg/

YAYIN TÜRÜ / PUBLICATION TYPE

Yaygın Süreli Yayın / Periodical

SAYFA DÜZENİ / DESIGN

Prof. Dr. Ozan ÖRMECİ

BASKI / PRINTING

Alanya, TÜRKİYE

Amaç ve Kapsam

Uluslararası Siyaset ve Siber Güvenlik Dergisi (USSG), tüm sosyal bilimler akademisyenlerini, öğrencilerini ve araştırmacılarını bilimsel makalelerini yayımlanmak üzere göndermeye davet etmektedir.

Uluslararası Siyaset ve Siber Güvenlik Dergisi (*USSG*), coğrafi veya konu bazlı herhangi bir sınırlama olmaksızın, tüm sosyal bilimler çalışmalarına yer vererek geniş bir akademik kitleye hitap etmeyi amaçlamaktadır. Bununla birlikte, derginin öncelikli gündemini uluslararası siyaset ile siber güvenlik alanının kesiştiği konular ve alanlar oluşturmaktadır.

Uluslararası Siyaset ve Siber Güvenlik Dergisi (*USSG*), Türkiye merkezli bir akademik dergidir.

Uluslararası Siyaset ve Siber Güvenlik Dergisi; teorik, metodolojik ve araştırmaya dayalı makaleler, özgün görüş yazıları ve kitap incelemeleri yayımlamaktadır.

Uluslararası Siyaset ve Siber Güvenlik Dergisi'nin yayın dilleri Türkçe ve İngilizcedir.

Uluslararası Siyaset ve Siber Güvenlik Dergisi (USSG), şu anda Google Scholar ve Türkiye Kaynakçası tarafından endekslenmektedir.

Uluslararası Siyaset ve Siber Güvenlik Dergisi (*USSG*), ICMJE (Uluslararası Tıp Dergileri Editörleri Komitesi) ve COPE (Yayın Etiği Komitesi) tarafından önerilen akademik etik prosedürlerini esas alır. Bu prosedürler editörler, yazarlar ve hakemler için geçerlidir.

Uluslararası Siyaset ve Siber Güvenlik Dergisi (*USSG*), Budapeşte Açık Erişim Girişimi'nde belirtilen Açık Erişim İlkelerini benimsemekte ve bilimsel yayınların araştırmacılara ücretsiz olarak sunulmasının bilginin küresel düzeyde paylaşımını artıracağı ilkesi doğrultusunda, içeriğine anında ve ücretsiz erişim sağlamaktadır.

Uluslararası Siyaset ve Siber Güvenlik Dergisi (*USSG*), orijinal yazarın ve kaynağın belirtilmesi koşuluyla her türlü ortamda sınırsız kullanıma, dağıtıma ve çoğaltmaya izin veren standart Creative Commons Atıf 4.0 Uluslararası Lisansı'nı sunmaktadır.

Dergide yayımlanan tüm makaleler Uluslararası Politika Akademisi (UPA) web sitesinde (https://politikaakademisi.org/uluslararasi-siyaset-ve-siber-guvenlik-dergisi-ussg/) arşivlenmektedir.

Uluslararası Siyaset ve Siber Güvenlik Dergisi'ne yapılacak tüm makale başvuruları, şimdilik esupakurumsal@gmail.com e-posta adresi üzerinden yapılmaktadır.

Editörler Kurulu:

1-) Prof. Dr. Ozan ÖRMECİ (Baş Editör)



2-) Doç. Dr. Oğuzhan GÖKSEL (Editör)



3-) Doç. Dr. Eren Alper YILMAZ (Editör)



4-) Dr. Ahmet CEYLAN (Editör)



5-) Dr. Serdar ÇUKUR (Editör)



6-) Dr. Mehmet EMİR (Editör)



7-) Dr. Oğuzhan MANİOĞLU (Editör)



8-) Dr. Cansu Arısoy GEDİK (Editör)



9-) Dr. Seda Gözde TOKATLI (Editör)



10-) Dr. Sina KISACIK (Editör)



11-) Dr. Beril Hakverir KUTMAN (Editör)



12-) Ayşe ÇUKUR (Yardımcı Editör)



13-) Erol NAGAŞ (Yardımcı Editör)



14-) Sadık ARPACI (Yardımcı Editör)



Danışma Kurulu:

1-) Hasan Kerem ÜNSAL (AKSAV)



2-) Prof. Dr. Behçet Kemal YEŞİLBURSA (Bursa Uludağ Üniversitesi)



3-) Prof. Dr. Gürol BABA (Ankara Sosyal Bilimler Üniversitesi)



4-) Prof. Dr. Cenk ÖZGEN (Giresun Üniversitesi)



5-) Doç. Dr. Ali Oğuz DİRİÖZ (TOBB Ekonomi ve Teknoloji Üniversitesi)



6-) Dr. Hüsmen AKDENİZ (RUBASAM)



7-) Dr. Mesut ÖZEL (İstanbul Kent Üniversitesi)



8-) Dr. Teoman Ertuğrul TULUN (AVİM)



9-) Dr. Özker KOCADAL (Uluslararası Kıbrıs Üniversitesi)



Yayın Etik Kuralları

Uluslararası Siyaset ve Siber Güvenlik Dergisi (*USSG*), *UPA Strategic Affairs* dergisi örnek alınarak hazırlanmıştır. *USSG*, ICMJE (Uluslararası Tıp Dergileri Editörleri Komitesi) ve COPE (Yayın Etiği Komitesi) tarafından önerilen akademik etik prosedürlerine uymaktadır. Bu prosedürler editörler, yazarlar ve hakemler için geçerlidir.

Aşağıda bilimsel araştırma ve yayın etiğine aykırı eylemler listelenmiştir:

İntihal: Başkalarının orijinal fikirlerini, yöntemlerini, verilerini veya çalışmalarını, bilimsel kurallara uygun şekilde kaynak göstermeden, kısmen veya tamamen kendi çalışmasıymış gibi sunmak.

Uydurma: Gerçekte var olmayan veya tahrif edilmiş verileri bilimsel araştırmada kullanmak.

Çarpıtma: Araştırma kayıtlarını veya elde edilen verileri değiştirmek; araştırmada kullanılmayan cihaz veya malzemeleri kullanılmış gibi sunmak; araştırma sonuçlarını destek sağlayan kişi ve kuruluşların çıkarları doğrultusunda değiştirmek veya şekillendirmek.

Yeniden Yayınlama: Akademik atamalar ve terfiler için aynı yayınları ayrı yayınlar olarak sunmak.

Salam Dilimleme: Bir çalışmanın sonuçlarını, çalışmanın bütünlüğünü tehlikeye atacak şekilde uygunsuz bir biçimde parçalara ayırmak ve bunları birden fazla yayında yayınlamak, bu yayınları akademik atamalar ve terfiler için ayrı yayınlar olarak sunmak.

Haksız Yazarlık: Aktif katkıda bulunmayan kişileri yazarlar arasına dahil etmek veya katkıda bulunanları dışlamak, yazar sıralamasını haksız ve uygunsuz bir şekilde değiştirmek, aktif katkıda bulunanların isimlerini sonraki sayılardan çıkarmak veya aktif katkıda bulunmamasına rağmen nüfuzunu kullanarak yazarlar arasına adını eklemek.

Dergimiz ayrıca, Etik Kurul onayı gerektiren bilimsel alanlardaki tüm çalışmaların ilgili Etik Kurul'un kararını almış olmasını şart koşmaktadır. Bu bağlamda, yazarlar makalenin ilk veya son sayfasında Etik Kurul onayının tarihini ve numarasını belirtmelidir. 2020 yılından bu yana Ulakbim TR Dizin endeksi tarafından uygulanan düzenlemeler doğrultusunda, Etik Kurul onayı gerektirdiği hâlde buna sahip olmayan çalışmalar dergimizde yayımlanmak üzere değerlendirilmeyecektir.

Dergimizde Etik Kurul onayı gerektiren çalışmalar şunlardır:

- Anketler, görüşmeler, odak grup çalışmaları, gözlem, deneyler ve tartışma teknikleri gibi yöntemlerle katılımcılardan veri toplamayı içeren nitel veya nicel yaklaşımlar kullanılarak yürütülen tüm araştırmalar.
- İnsan ve hayvanların (materyaller veya veriler dahil) deneysel veya diğer bilimsel amaçlarla kullanıldığı çalışmalar.
- İnsanlar üzerinde yapılan klinik araştırmalar.

- Hayvanlar üzerinde yapılan bilimsel araştırmalar.
- Kişisel Verilerin Korunması Kanunu çerçevesindeki retrospektif çalışmalar.

Bu tür çalışmaların değerlendirmeye alınabilmesi için ilgili Etik Kurul onaylarının alınmış olması ve bu onayların makale metninde açıkça belirtilmesi gerekmektedir.

Son olarak, dergi politikasınca gereğince, yapay zekâ kullanımıyla ilgili bazı sınırlamalar bulunmaktadır. Yapay zekâ uygulamaları; makalelerin çevirisi, redaksiyonu, başlık belirlenmesi ve istatistiki verilerin görselleştirilmesi gibi konularda tamamen serbesttir. Buna karşın, makalelerin içeriğinde yapay zekâ kullanımı yüzde 20 ile sınırlıdır.

Makale Formatı

Uluslararası Siyaset ve Siber Güvenlik Dergisi (*USSG*), DergiPark sistemi, İntihal.net, Turnitin veya iThenticate programından en fazla yüzde 20 benzerlik puanı alan makaleleri kabul etmektedir (Dipnotlar ve Referanslar rapora dahil edilmemelidir).

Makalelerin uzunluk üst sınırı, Özet ve Dipnotlar hariç 20.000 kelimedir. Makaleler için herhangi bir sayfa sınırı yoktur. Benzer şekilde, makaleler için alt sınır 3.000 kelimedir ve herhangi bir sayfa sınırı bulunmamaktadır. Araştırma makalelerinin yanı sıra, dergi, görüş veya karşı görüş bildiren açıklayıcı yazılara, kitap özetlerine ve çeviri yazılarına da yer vermektedir.

Uluslararası Siyaset ve Siber Güvenlik Dergisi (*USSG*), yazarlarını İngiliz veya Amerikan tarzında bir yazım dili kullanmaya teşvik etmektedir. Yazarlar, makalelerinin tamamını esupakurumsal@gmail.com adresine göndermelidir. Makaleler, aşağıda belirtilen format kurallarına uygun olmalıdır. Format uygunsuzluğu durumunda makale hakkında sürecin devam ettirilip ettirilmeyeceği editörün kararına bırakılacaktır.

Makaleler, tercihen ilgili konuda uzman iki farklı akademisyen tarafından anonim olarak incelenir. *Uluslararası Siyaset ve Siber Güvenlik Dergisi*'nde yalnızca 2/2 kabul alan makaleler yayınlanır. "Revizyon" kararlarında, derginin editörlerine karar verme fırsatı tanınır. "Kapsamlı Revizyon" kararlarında ise derginin editörleri ve hakemleri ortak bir karara varmalıdır. Bir onay ve bir ret alan makaleler üçüncü bir hakeme gönderilecektir. Kitap incelemeleri ve görüş yazıları için editör onayı yeterlidir.

Katkıda bulunanlar, makalelerinin yayınlanmasından önce bir onay sözleşmesi imzalamalıdır.

FORMAT DETAYLARI

Biçim:

Kenar boşlukları: Tüm kenar boşlukları her taraftan 2,5 cm (1 inç) olmalıdır.

Ana Başlık: Ana başlık, Times New Roman yazı tipinde, 12 punto boyutunda, büyük harflerle, ortalanmış ve kalın formatta olmalıdır.

Yazar Adları: Yazar adları, akademik unvanlar olmadan, Times New Roman yazı tipinde 12 punto boyutunda, ana başlığın altına (metni sağa hizalayarak) eklenmelidir. Akademik unvanlar ve bağlı kurumlar, e-posta adresi ve tercihen bir ORCID numarasıyla birlikte ilk dipnot olarak aşağıda listelenmelidir.

Öz: Bölüme, bölümün içeriğini 100 ila 250 kelimeyle özetleyen bir Öz bölümüyle başlayın. Öz, Times New Roman 12 punto boyutunda yazılmalıdır.

Anahtar Kelimeler: Öz bölümünün ardından bu bölümde en fazla 5 anahtar kelime yazılmalıdır. Anahtar kelimeler, Times New Roman yazı tipinde, 12 punto büyüklüğünde ve italik olmalıdır.

Hizalama: Hizalama iki yana yaslı olmalıdır. İlk satırlar içten başlamamalıdır.

Yazı Tipi: Times New Roman yazı tipi, 12 punto büyüklüğünde ve 1,5 satır aralığı kullanılmalıdır. Her paragrafın başına 0 punto, sonuna ise 6 punto boşluk bırakılmalıdır.

Alt Başlıklar: Her makalenin bir Giriş ve bir Sonuç bölümü olmalıdır. Giriş ve Sonuç bölümleri numaralandırılmamalıdır. Alt başlık sayısı en fazla 20 olmalıdır. Alt başlıklar 1., 2., 3.; 1.1., 1.2., 1.3.; 1.1.1., 1.1.2., 1.1.3. vb. şeklinde numaralandırılmalıdır. Alt başlıklar 12 punto büyüklüğünde, kalın harflerle ve yalnızca ilk harfleri büyük harfle yazılmalıdır.

Çift tırnak: Vurgulanan kelimeler veya alıntılanan cümleler için çift tırnak ("….") kullanılmalıdır. Çift tırnak kullanılırken alıntıdaki metin italik yazılmalıdır.

İtalik: Dergi, kitap ve gazete adları hem metin içinde, hem de kaynakça bölümünde italik olarak yazılmalıdır. Yabancı kelimeler de metin içinde italik yazılmalıdır.

Tablolar ve Grafikler: Tablolar, grafikler ve haritalar, Roma rakamları veya normal rakamlarla, kalın yazı tipi ve 12 punto Times New Roman yazı tipi kullanılarak Tablo I, Grafik 2, Harita III vb. şeklinde numaralandırılmalıdır. Tablo, grafik ve harita numaraları üst tarafta yazılmalıdır. Grafik numaralarının ardından, 12 punto Times New Roman yazı tipiyle bir tanım verilmelidir.

Kaynak Gösterimi:

Kaynak gösterimi için Chicago stili dipnot sistemi kullanılır.

Dipnotlar, 10 punto Times New Roman yazı tipi ve "metni sola hizala" stiliyle yazılmalıdır.

Referanslar metin içinde dipnotla belirtilmeli ve sayfanın alt kısmında ayrıntılı olarak açıklanmalıdır.

Dipnotlar, ilgili cümlenin sonuna (noktadan sonra) üst simge olarak Arap rakamlarıyla yazılmalıdır.

Dipnotlar, Microsoft Word'de Referanslar sekmesindeki "Dipnot Ekle" seçeneğine tıklanarak eklenebilir.

Her dipnot nokta ile biter.

Sayfa referansları tek sayfalar için "s.", çok sayfalı kitaplar için ise "ss." şeklinde olmalıdır.

Kitaplar:

Standart Kaynakça: Yazarın soyadı, Yazarın adı (Yayın yılı), *Kitabın adı*, Yayın yeri: Yayınevi.

Standart dipnot ilk kullanım: Yazarın adı ve soyadı (Yayın yılı), *Kitabın adı,* Yayın yeri: Yayınevi, ss. 12-13.

Standart Dipnot ikinci kullanım: Yazarın adı ve soyadı (Yayın yılı), *Kitabın adı*, ss. 12-13.

Standart Dipnot ardışık kullanımı: *A.g.e.*, ss. 12-13.

Birden fazla yazarlı kaynakça: Yazarın soyadı, Yazarın adı & Yazarın soyadı, Yazarın adı (Yayın yılı), *Kitabın adı*, Yayın yeri: Yayınevi.

Birden fazla yazarlı dipnot ilk kullanım: Yazarın adı ve soyadı & Yazarın adı ve soyadı & Yazarın adı ve soyadı (Yayın yılı), *Kitabın adı*, Yayın yeri: Yayınevi, ss. 1-4.

Birden fazla yazarlı dipnot ikinci kullanım: Yazarın adı ve soyadı vd. (Yayın yılı), *Kitabın adı*, ss. 1-4.

Birden fazla yazarlı dipnot ardışık kullanımı: *A.g.e*, ss. 1-4.

Makaleler:

Standart Kaynakça: Yazarın soyadı, Yazarın adı (Yayın yılı), "Makalenin adı", *Derginin adı*, Cilt(Sayı), ss. 10-32 (tam makale).

Makale dipnotunun ilk kullanımı: Yazarın adı ve soyadı (Yayın yılı), "Makalenin adı", *Derginin adı*, Cilt(Sayı), s. 7 (yalnızca alıntı yapılan sayfa).

Makale dipnotunun ikinci kullanımı: Yazarın adı ve soyadı (Yayın yılı), "Makalenin adı", s. 7 (yalnızca alıntı yapılan sayfa).

Makale Dipnotunun ardışık kullanımı: *A.g.e.*, s. 7.

Birden fazla yazarlı makale Kaynakça: Yazarın soyadı, Yazarın adı & Yazarın soyadı, Yazarın adı & Yazarın soyadı, Yazarın adı & Yazarın soyadı, Yazarın adı (Yayın yılı), "Makalenin adı", *Derginin adı*, Cilt(Sayı), ss. 10-32 (tam makale).

Birden fazla yazarın yer aldığı dipnotun ilk kullanımı: Yazarın adı ve soyadı vd. (Yayın yılı), "Makalenin adı", *Derginin adı*, Cilt(Sayı), s. 7 (yalnızca alıntı yapılan sayfa).

Birden fazla yazarın yer aldığı dipnotun ikinci kullanımı: Yazarın adı ve soyadı vd. (Yayın yılı), "Makalenin adı", s. 7 (yalnızca alıntı yapılan sayfa).

Birden fazla yazarın yer aldığı dipnotun ardışık kullanımı: *A.g.e.*, s. 7.

Gazeteler:

Başyazı: *The New York Times Başyazısı* (2015), "Makalenin adı", 23.07.2010 (tam yayın tarihi), s. 5.

Başlıksız: *Los Angeles Tribune* (2012), "Makalenin/haberin adı", 23.07.2010 (tam yayın tarihi), s. 13.

Belirli bir köşe yazarı/muhabir tarafından yazılan haber (Kaynakça): Muhabirin/köşe yazarının soyadı, Muhabirin/köşe yazarının adı (Yayın yılı), "Makalenin/haberin adı", *Gazetenin adı*, 23.07.2010 (tam yayın tarihi), s. 3.

Belirli bir köşe yazarı/muhabir tarafından yazılan haber (Dipnot): Muhabirin/köşe yazarının adı ve soyadı (Yayın yılı), "Makalenin/haberin adı", *Gazetenin adı*, 23.07.2010 (tam yayın tarihi), s. 3.

Belirli bir köşe yazarı/muhabir tarafından yazılmış (Dipnot) ikinci kullanım: Muhabirin/köşe yazarının adı ve soyadı (Yayın yılı), "Makalenin/haberin adı", s. 3.

Gazetelerde dipnotun ardışık kullanımı: *A.g.e.*

İnternet arşivleri: Muhabirin/köşe yazarının/derginin tam adı (Yayın yılı), "Makalenin/haberin adı", *Gazetenin adı*, 23.07.2010 (tam yayın tarihi), Erişim Tarihi: GG.AA.YYYY, Erişim Adresi: http://www. (tam URL).

Kurumlar ve Kuruluşlar:

Kurumun adı, "Sayfa adı", 23.07.2012 (Sayfa son değiştirilme tarihi), Erişim Tarihi: GG.AA.YYYY, Erişim Adreresi: http://www. (tam URL).

Filmler: Yönetmenin tam adı (Yapım yılı), "Filmin adı".

Youtube: "Video başlığı", Erişim Tarihi: GG.AA.YYYY, Erişim Adresi: http://www (tam URL).

Endeksler

Uluslararası Siyaset ve Siber Güvenlik (USSG) Dergisi'nin dahil olduğu endeksler şunlardır:

Türkiye Kaynakçası

Google Scholar



ÖNSÖZ

2012 yılından beri, yaklaşık 15 yıldır, Türk Dış Politikası başta olmak üzere uluslararası siyasetin farklı alanlarında sürekli yayın yapan Uluslararası Politika Akademisi (UPA) akademik girişiminin Kurucu Genel Koordinatörü olarak, ekibimle birlikte, 2020 yılında kurduğumuz uluslararası akademik e-dergi *UPA Strategic Affairs*'in başarısından da cesaret alarak, 2026 yılı itibariyle Siyaset Bilimi ve Uluslararası İlişkiler'in önümüzdeki yıllarda en önemli ve stratejik alt disiplinlerinden biri olmak muhtemel siber güvenlik, bilişim teknolojileri ve yapay zekâ mücadelesi konusunda yeni bir akademik dergi kurmaya karar verdik. Kuşkusuz, bu kararı almamızda, kısa bir süre önce AKSAV ile kurduğumuz ortaklık neticesinde hayata geçirilen Elektronik Sanat ve Uluslararası Politika Enstitüsü veya kısa ismiyle ESUPA adlı düşünce kuruluşunun gelecek planlamaları da etkili oldu.

Uluslararası siyasette jeopolitik rekabetin keskinleştiği, en köklü demokrasilerin bile popülizme esir düştüğü bir çağda, kuşkusuz, siber alandaki rekabet de giderek sertleşmekte ve güvenlik riskleri artmaktadır. Ülkemiz Türkiye de, bu konuda gelişmiş ülkelerin yaptığı atılımları yakından takip etmekte ve yabancı istihbarat kuruluşları, organize suç örgütleri ve terör örgütlerinin devlet kurumları, özel kurumlar ve önemli kişilere yaptığı saldırılar karşısında aldığı güvenlik önlemlerini giderek arttırmaktadır. Bu bağlamda, özellikle 2025 yılı başlarında kurulan T.C. Cumhurbaşkanlığı'na bağlı Siber Güvenlik Başkanlığı (SBG), bu alandaki gerekli düzenlemeleri önerecek ve yapacak, ihtiyaç duyulan yasal mevzuatın oluşturulmasını sağlayacak, gelecek planlamalarını oluşturacak ve vatandaşlarımız ve kurumlarımızın güvenliği sağlayacak temel kurum olarak çalışmalarına başlamıştır. Henüz emekleme aşamasında olmasına karşın, kurum, hızla gelişmekte ve ülkemize ve insanlığa faydalı işler yapmaya çalışmaktadır.

İşte biz de, UPA ve ESUPA ekibi olarak, bu yeni kurduğumuz ve siber güvenlik başta olmak üzere uluslararası siyasetin farklı boyutlarını içerek yeni hakemli akademik e-dergimizle bu sürece katkıda bulunmak istedik. AKSAV Başkanı Hasan Kerem Ünsal'la birlikte başlattığımız ESUPA girişiminin devamı niteliğindeki bu dergi, bu anlamda Türkiye'nin siber geleceğine yön vermek için kurulmuştur. İlerleyen aylarda ve yıllarda, bu alanda Türkiye ve dünyada isim yapmış önemli uzmanlarla yapacağımız çalışmalar neticesinde, amacımız, Türkiye Cumhuriyeti'nin kurumlarına doğru politika tavsiyeleri verebilecek yüksek nitelikli işlere imza atabilmektir. Bu doğrultuda çalışma azim ve kararlılığımız tamdır.

Bu duygu ve düşüncelerle, senede iki defa (Haziran ve Aralık) yayımlanacak olan dergimizin ilk cilt ve ilk sayısını sizlere gururla takdim ediyoruz. Dileğimiz, evlatlarımızın daha temiz, güzel, iyi ve barışçıl bir dünyada yaşamasıdır. Bunun için ise, terörist zihniyetli, şiddeti ve ayrımcılığı meşru gören, başka insanlara karşı kötü emelleri olan, insan ve doğayı sevmeyen kıskanç ve kötücül insanlara karşı kendimizi koruyabilmemiz şarttır. Bu nedenle, günümüzde artık güvenliğin kaçınılmaz ve temel bir unsuru olan siber güvenlik alanında bilimsel çalışmalar yapılacak olan bu dergiye desteklerinizi beklemekteyiz.

Saygılarımızla...

O. Ormeci

Prof. Dr. Ozan ÖRMECİ

15 Kasım 2026

İÇİNDEKİLER

Önsöz…..……...1

İçindekiler……..3

Popular Movies About Cyber Security.....4

Ozan ÖRMECİ

Rusya-Ukrayna Savaşı Sonrasında Avrupa Birliği Dış Politikasının Dönüşümü: 'Normative Power Europe' Yaklaşımının Yeniden Değerlendirilmesi……..26

Oğuzhan MANİOĞLU

Avrupa Birliği Güvenlik Girişimlerinin Ukrayna-Rusya Savaşı Çerçevesinde Dönüşümü: Dost ve Düşman Algısının Belirginleşmesi (2022-2026).....55

Mehmet EMİR & İsmail Hakkı PEKİN

Türkiye'nin Siber Güvenlik Politikaları.....95

Ozan ÖRMECİ

Multidimensional Human Security Among Older Muslim Migrants in Europe: Vulnerability, Discrimination, and Protection.....123

Cemal YILMAZ

POPULAR MOVIES ABOUT CYBER SECURITY

Ozan ÖRMECİ[1]

Abstract: As cybersecurity and cyber governance gain importance among states, companies, institutions, and individuals in the 21st-century world, cultural products addressing this field are also rapidly proliferating. The United States—a leading nation in this arena alongside the People's Republic of China—holds a near-monopoly due to the power of Hollywood and serves as the source of many significant productions. However, the recent rise in the subject's importance has led to the production of similar films in other countries as well. This article presents a list of significant films covering topics such as cybersecurity, cyber governance, and cyber warfare, while providing key information about them. It will contribute to the literature and the academic community by helping to identify productions suitable for use as visual resources in courses within this field.

Keywords: *Cyber Security, Cyber Governance, Cyber Warfare, Hollywood, Cinema.*

Makale Geliş Tarihi: 23.09.2026

Makale Kabul Tarihi: 26.09.2026

DOI: 10.5281/zenodo.23233951

[1] Professor of Political Science, ESUPA President.
Email: ozanormeci@gmail.com.
Website: http://www.ozanormeci.com.
ORCID: 0000-0001-8850-6089.

SİBER GÜVENLİK HAKKINDA POPÜLER FİLMLER

Öz: 21. yüzyıl dünyasında devletler, şirketler, kurumlar ve bireyler nezdinde siber güvenlik ve siber yönetişim konuları önem kazandıkça, bu alana odaklanan kültürel ürünler de hızla çoğalmaktadır. Çin Halk Cumhuriyeti ile birlikte bu alanda önde gelen bir ülke olan Amerika Birleşik Devletleri, Hollywood'un gücü sayesinde neredeyse tekel konumundadır ve pek çok önemli yapımın kaynağını oluşturmaktadır. Bununla birlikte, söz konusu konunun son dönemde kazandığı önem, başka ülkelerde de benzer filmlerin üretilmesini beraberinde getirmiştir. Bu makale; siber güvenlik, siber yönetişim ve siber savaş gibi konuları ele alan önemli filmlerin bir listesini sunmakta ve bunlara dair temel bilgiler sağlamaktadır. Çalışma, bu alandaki derslerde görsel kaynak olarak kullanılabilecek yapımların belirlenmesine yardımcı olarak literatüre ve akademik camiaya katkı sağlayacaktır.

Anahtar Kelimeler: *Siber Güvenlik, Siber Yönetişim, Siber Savaş, Hollywood, Sinema.*

Introduction

As cybersecurity and cyber governance gain importance among states, companies, institutions, and individuals in the 21st-century world, cultural products addressing this field are also rapidly proliferating. The United States—a leading nation in this arena alongside the People's Republic of China—holds a near-monopoly due to the power of Hollywood and serves as the source of many significant productions. However, the recent rise in the subject's importance has led to the production of similar films in other countries as well.

This article presents a list of significant films covering topics such as cybersecurity, cyber governance, and cyber warfare, while providing key information about them. It will contribute to the literature and the academic community by helping to identify productions suitable for use as visual resources in courses within this field. For the research, film-related websites such as IMDb.com, Beyazperde.com, and Rotten Tomatoes will be utilized.

1. The List of Popular Movies about Cyber World

Since internet technology—and particularly the cybersecurity issues it has spawned—gained prominence in the eyes of popular culture and the general public primarily during the 2000s, most popular films in this genre were also produced in the new millennium. However, since the early adoption of internet technology in the United States (U.S.) and Western countries started in the 1980s and the 1990s, there are also some popular films from these eras that feature similar themes. It is also noteworthy that almost all such films are U.S.-based (at this point, one must undoubtedly also mention the power and allure of Hollywood), while successful productions from other countries emerge only very rarely.



The first popular film in this genre is the 1983 production "WarGames". Nominated for three Academy Awards and grossing ten times its budget, the film centers on a young college student (Matthew Broderick) who, in an attempt to impress his girlfriend, hacks into a U.S. Department of Defense program—essentially a simulation of a potential nuclear war with the Soviet Union (USSR)—and inadvertently brings the world to the brink of World War III through his actions within the system.

Starring Matthew Broderick, a popular young star of the time, this film contributed to the understanding and, to some extent, the encouragement of hacker culture in the U.S. and worldwide. It is no coincidence that a group of hackers from Milwaukee, Wisconsin, influenced by the film, used the 414s code to hack into many important public and private organizations in the U.S., showcasing the first dangerous examples of computer hacking. Following this group's actions, the "Computer Fraud and Abuse Act 18 USC 1030", the first legal regulation in the U.S., was enacted. The law focused particularly on protecting government computers, especially those related to justice, defense, and national security.[2]

[2] For details, see; Salih Bıçakçı (2013), *21. Yüzyılda Siber Güvenlik*, İstanbul Bilgi Üniversitesi Yayınları.



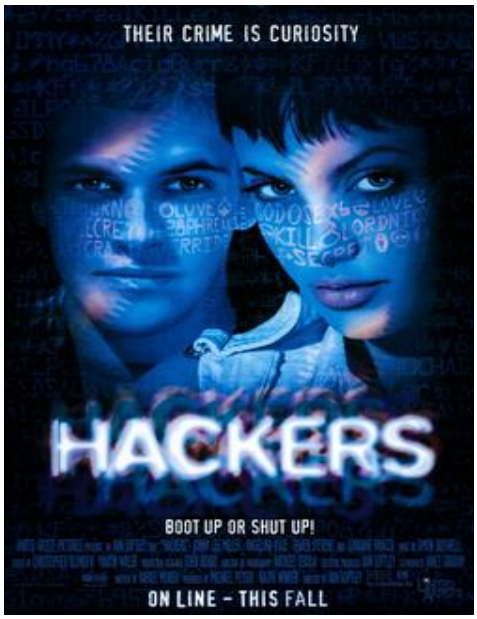
,

Another pioneering film is the 1992 production “Sneakers”. a 1992 adventure film directed by renowned filmmaker Phil Alden Robinson, “Sneakers” features a star-studded cast including Robert Redford, Dan Aykroyd, Sidney Poitier, River Phoenix, and Ben Kingsley. The film is one of the productions that most closely reflects realistic penetration logic, as it addresses social engineering, penetration testing, teamwork, and security vulnerabilities. In this respect, it stands as one of the first productions to directly tackle the theme of cybersecurity. The presence of a major star like Robert Redford in the film undoubtedly played a role in elevating the importance of the subject matter in the eyes of the general public and even governments.

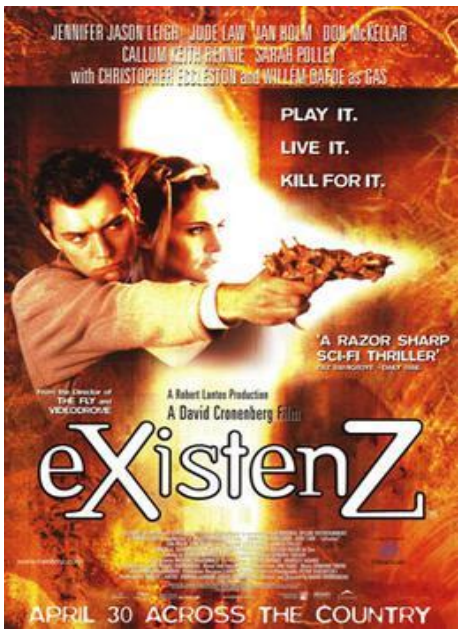
The plot of the film is briefly as follows: Martin Bishop (Robert Redford) leads a group of computer experts who test security systems. Government officials ask the team to carry out a secret operation, but when they refuse, they are blackmailed by the officials. Finding themselves caught in a dangerous game, the experts realize they have obtained a program capable of cracking every encryption code on Earth.



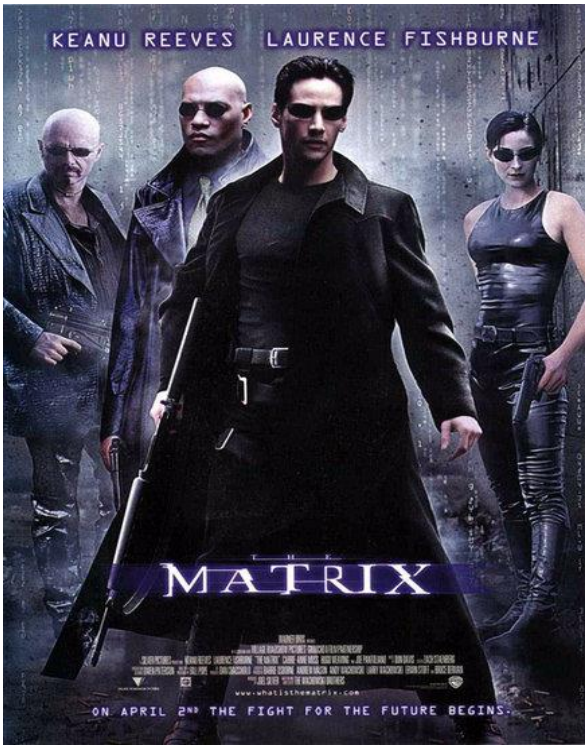
Another significant production is the 1995 film "The Net". The film was directed by Irwin Winkler, with a screenplay by John Brancato and Michael Ferris. Famous actress Sandra Bullock stars in the lead role. The film centers on a software analyst (Sandra Bullock) who works from home and conducts her entire life online; she unwittingly finds herself at the center of a massive cyber-conspiracy and sees her identity digitally erased. "The Net" arrived just two months before "Hackers*"* (1995) and helped introduce the general public to concepts like cyberattacks, online ordering, and digital footprints.



Another production that marked a turning point in this genre—released almost concurrently with the film "The Net"—is "Hackers" (1995). Written by Rafael Moreu and directed by Iain Softley, the film stars Jonny Lee Miller, Angelina Jolie, and Jesse Bradford. The appearance of Jolie—who would go on to become a major star—played a significant role in drawing attention to the film. The movie tells the story of Dade Murphy (Jonny Lee Miller), a child prodigy who was banned from using computers and telephones until the age of 18 after causing a massive system crash on Wall Street at age 11. Years later, after starting at a new high school in New York, Dade meets Kate (Angelina Jolie) and a group of other talented young hackers. As events unfold, one of the group members hacks into the mainframe of a major oil company. Implicated in the resulting incident, the youths find themselves forced to evade the FBI and prove their innocence.

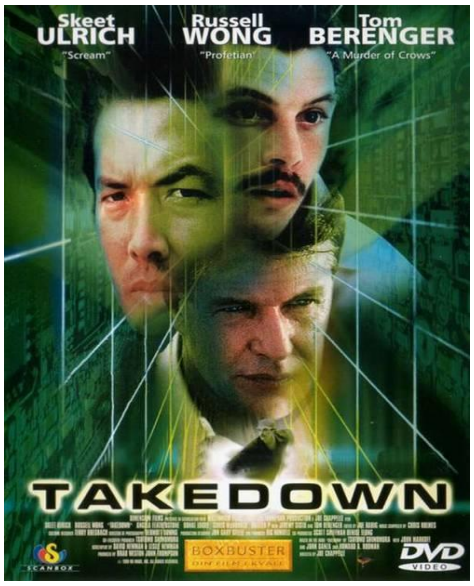


"eXistenZ" is a 1999 science fiction-horror film written, produced, and directed by the renowned filmmaker David Cronenberg. Although it was overshadowed by the famous "The Matrix"—which was released the same year—it has since evolved into a cult classic thanks to its prophetic vision and philosophical depth. The film, which centers around virtual reality, features fictional technological inventions such as organic consoles and bio-ports and also incorporates concepts that foreshadowed the advent of artificial intelligence.



A true cinematic legend, the 1999 film "The Matrix" is a groundbreaking masterpiece that radically transformed film history and popular culture, prompting questions about the nature of reality and the anxieties of the digital age. Evoking dread with the concept that humanity lives within a simulation created by machines, the film was directed by the Wachowski Brothers and starred Keanu Reeves, Laurence Fishburne, and Carrie-Anne Moss.

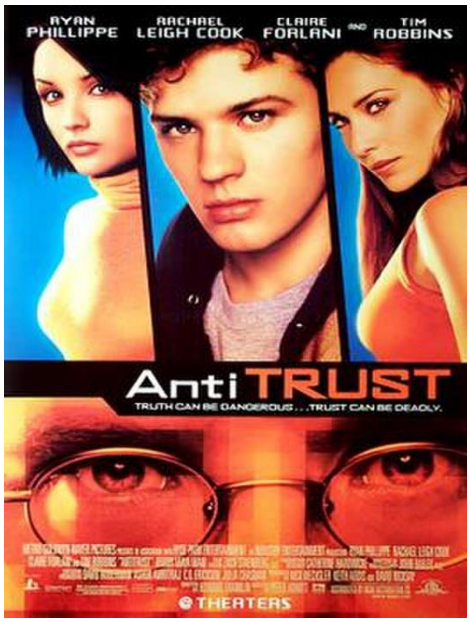
The film draws directly from Jean Baudrillard's "Simulacra and Simulation". By prompting the viewer to ask, "What if the world we inhabit is merely a mental prison?", it transposes Plato's "Allegory of the Cave" into the modern cyber world. The choice between the "red pill and the blue pill" has evolved into a universal metaphor—used in fields ranging from sociology to politics—to illustrate the dilemma of either shedding illusions to confront painful truths (awakening) or maintaining a comfortable lie. Released in 1999—on the threshold of a new millennium—the film struck a chord with societal anxieties at a time when the internet was newly entering our lives and there was intense debate over whether artificial intelligence and computers might one day take over humanity (amidst fears such as the Y2K bug).



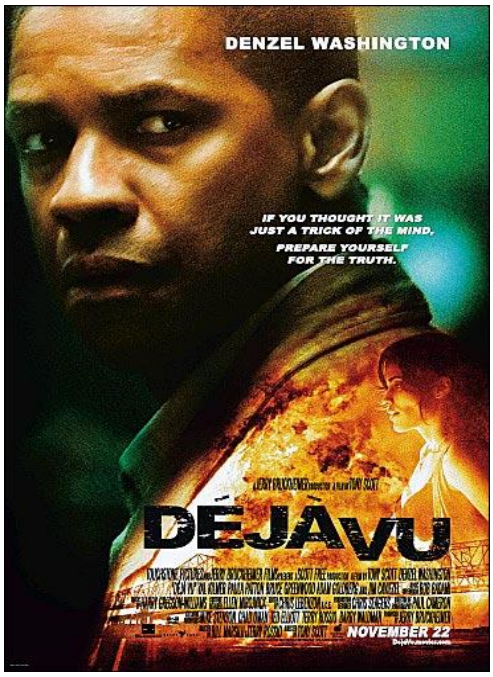
Another important yet little-known film is the 2000 production "Takedown". This film is based on the story of the capture of computer hacker Kevin Mitnick. The film, adapted from a book about Mitnick, is directed by Joe Chappelle and stars Skeet Ulrich and Russell Wong. Kevin Mitnick (Skeet Ulrich) is one of the world's most skilled and most wanted computer hackers. He is constantly pursuing ever larger and more challenging cyber targets. One day, he attempts to breach the computer system of security expert and former hacker Tsutomu Shimomura (Russell Wong). This move pits Mitnick against a worthy adversary, sparking a digital game of cat and mouse between the two. Tsutomu Shimomura collaborated with the FBI to conduct a major operation aimed at capturing Mitnick.



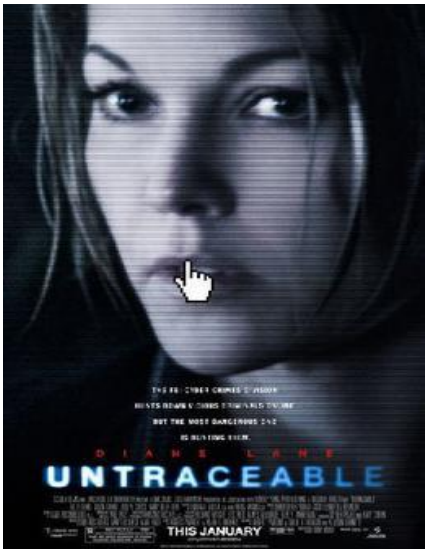
The 2001 film "Swordfish" is another significant production that left its mark on the genre. Written by Skip Woods and directed by Dominic Sena, the film drew a large audience thanks to its star-studded cast, which included John Travolta, Hugh Jackman, Halle Berry, Don Cheadle, Vinnie Jones, and Sam Shepard. The plot centers on Gabriel Shear (John Travolta)—the charismatic and dangerous leader of a covert counter-terrorism unit known as "Black Cell"—and his team as they join forces with Stanley Jobson (Hugh Jackman), an ex-convict and one of the world's best hackers, to recover funds generated from an off-the-books operation.



The 2001 film "Antitrust" is another significant film that stands out for addressing companies and the legal aspects of this field. Written by Howard Franklin and directed by Peter Howitt, the film stars Ryan Phillippe, Tim Robbins, and Rachael Leigh Cook. It centers on young, idealistic programmers and a major corporation (NURV) that offers talented young people substantial salaries, an informal work environment, and creative opportunities. Although NURV's charismatic CEO appears well-intentioned, new employee Milo Hoffman (Ryan Phillippe) begins to uncover a terrifying, hidden truth about the company's operations. Hoffman discovers that the company's true objective—and the secret agenda behind its global communication system—is a sinister, illegal cyber-theft network designed to destroy competitors. Featuring clear allusions to Microsoft and Bill Gates, the film attracted attention for its young, popular cast and sparked discussion regarding various aspects of cybersecurity.

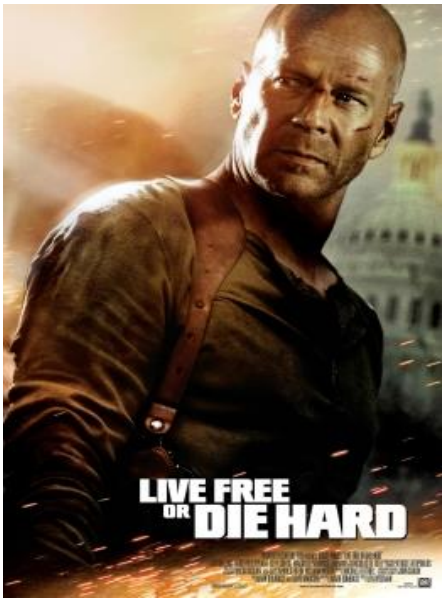


The 2006 film "Déjà Vu" is a significant science fiction action movie directed by Tony Scott and starring Denzel Washington, which uniquely blends the concepts of time travel and memory. By combining the sensation of having experienced something before—known as "déjà vu"—with advanced surveillance and time-folding technology used to alter the past, the film creates an incredibly thrilling story. With this futuristic aspect, the film has garnered significant attention and acclaim.



The 2008 film "Untraceable" tells the story of an FBI agent attempting to catch a cyber serial killer who tortures victims online, broadcasts the acts live, and accelerates the rate of death as the number

of clicks on the website increases. Directed by Gregory Hoblit, the film stars Diane Lane in the lead role. The film, which leans heavily towards the horror genre, is significant for demonstrating how the internet can be used for dangerous purposes.



The 2008 film "Live Free or Die Hard" follows the efforts of aging detective John McClane (Bruce Willis)—who has left the police department to work in a cybersecurity unit—to stop a massive cyber-terrorist attack aimed at crippling America's computer infrastructure. Directed by Len Wiseman, the film attracted significant attention as a new installment in the popular Bruce Willis franchise and boosted interest in the field of cybersecurity.



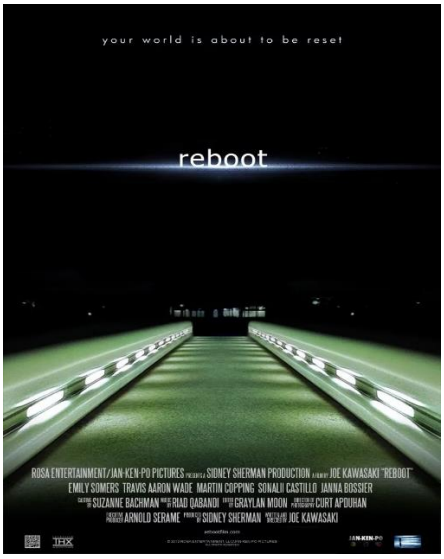
"Eagle Eye", a 2008 American action-thriller directed by DJ Caruso and written by John Glenn, Travis Adam Wright, Hillary Seitz, and Dan McDermott, is a significant yet lesser-known film centered on information and communication technologies. The cast includes Shia LaBeouf, Michelle Monaghan, Rosario Dawson, Michael Chiklis, Anthony Mackie, and Billy Bob Thornton. The plot follows two strangers forced to go on the run together after receiving a phone call from a mysterious woman who uses information and communication technology to track their every move. The film, which achieved unexpectedly high box-office success, also marked a significant turning point by demonstrating the steadily growing interest in this subject.



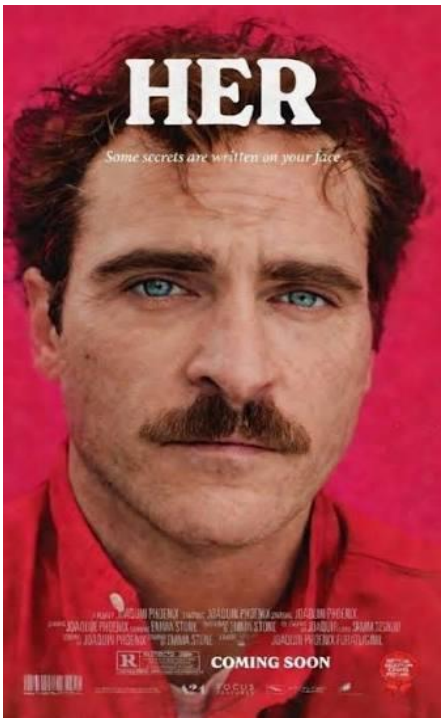
The 2010 film "The Social Network" holds great significance as a cult classic that captures the transformation of the digital age and the human ambitions involved in the founding of Facebook. The film examines how social media has transformed individual lives—and by extension, humanity as a whole—while focusing on the inception and evolution of Facebook, a pivotal milestone in this realm. Directed by the acclaimed David Fincher, the film stars Jesse Eisenberg (in the role of Facebook founder Mark Zuckerberg). The film has secured a top spot on lists of the best movies of the 21st century, becoming the primary cinematic reference point for modern digital culture.



The 2011 film "Source Code" holds a unique place in cinema for creating an ingenious narrative loop through the masterful use of a limited timeframe (eight minutes) and a single setting (a train), as well as for successfully blending the philosophies of consciousness, parallel universes, and destiny. Directed by Duncan Jones and starring Jake Gyllenhaal, the film centers on a physically disabled soldier attempting to uncover a terrorist plot through a government-controlled program or simulation.

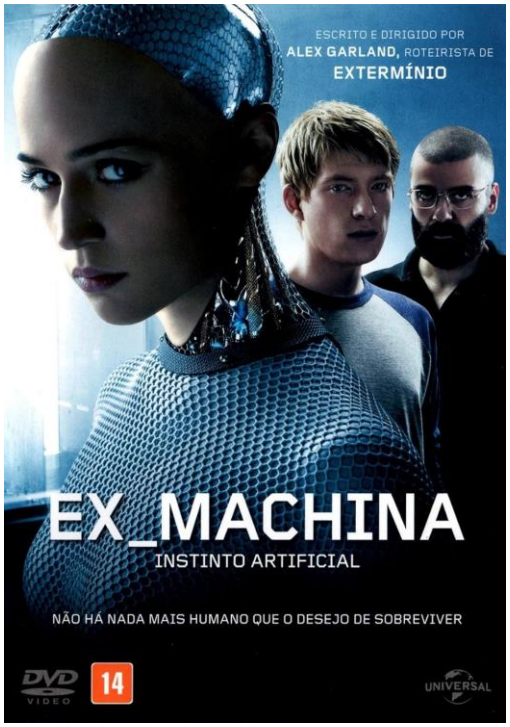


The 2012 film "Reboot" centers on a young female hacker who, following a traumatic event, wakes up to find an iPhone fused to her hand and a countdown ticking down to zero, and attempts to solve the mystery. Directed by Joe Kawasaki, the film stars Emily Somers in the lead role. The film has drawn attention as a dystopian cyber-thriller that explores the place of the internet and technology in our lives, the bond between humans and the virtual world, and the dangers arising from this connection.



Written and directed by Spike Jonze, "Her" (2013) is regarded as both a timeless masterpiece and a prophetic film in the contexts of cinema history and modern sociology. Starring Joaquin Phoenix, the film predicted—with uncanny accuracy—the advent of large language models (LLMs), advanced voice assistants, and human-like relationships with artificial intelligence. Today, the emotional bonds people form with AI through platforms like ChatGPT (particularly its voice mode) and Character.ai serve as a testament to the film's visionary nature. Set in a near-future Los Angeles, the film follows Theodore (Joaquin Phoenix), a lonely man who embarks on an extraordinary virtual romance with an AI operating system. Through this narrative, the film transcends the genre of ordinary science fiction to offer a social critique regarding the profound isolation humans can experience in a world where technology has reached its zenith. Theodore's

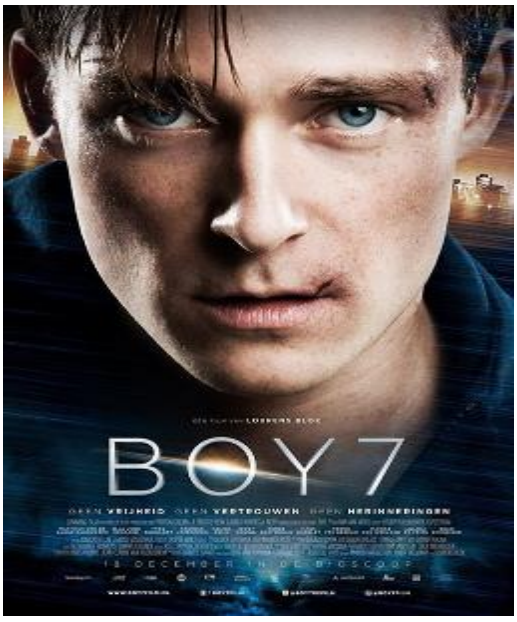
existence amidst the crowded streets of Los Angeles—connected only by the earpiece in his ear—perfectly mirrors the reality of contemporary metropolitan life and digital isolation.



Directed by Alex Garland, the 2014 film "Ex Machina" centers on a programmer who is summoned by a mysterious CEO to a remote mountain home to conduct a Turing test on an artificially intelligent humanoid robot. Caleb (Domhnall Gleeson), a 24-year-old programmer, is winning a competition organized by the major tech company where he works. As his prize, he travels to the secluded home of the company's brilliant and reclusive CEO, Nathan (Oscar Isaac), located deep in nature. Nathan asks Caleb to administer a Turing test to Ava (Alicia Vikander), a newly developed humanoid AI. As the test progresses, Caleb begins to develop feelings for Ava. Meanwhile, Ava devises an escape plan by employing human emotions, manipulation, and a desire for survival. By the end of the film, Ava manages to outsmart her creator and escape to the outside world, leaving Caleb locked inside the mountain home. The film is a groundbreaking production that provokes deep reflection on the future of robotics technology.



The 2014 German film "Who Am I" (originally titled "Kein System ist Sicher") centers on Benjamin (Tom Schilling), a young computer genius who feels like a "loser" and goes largely unnoticed in everyday life, as he struggles to find an identity and a sense of belonging within the hacker community. An introverted hacker, Benjamin meets Max (Elyas M'Barek)—a fellow hacker—and his friends, eventually joining their underground hacking group, CL3X (or FRI3NDS). Having dreamed of becoming a superhero since childhood, Benjamin attempts to use the group as a vehicle to become a world-renowned hacker. The team makes a name for itself through various cyber operations; however, their massive, high-profile hacks attract the attention of both German Intelligence (BND) and Russian gangsters, dragging them into a dangerous game. This remarkable production—one of the rare films not made in the U.S.—has been highly acclaimed by audiences.



The 2015 Dutch film "Boy 7" centers on a young man who wakes up on a crowded subway with no memory of his past, and his fight for justice within dystopian police state that prioritizes security over freedom. Adapted from Mirjam Mous' novel of the same name, the film stands out as a rare European entry in this genre—a type of production seldom seen outside the U.S.—and was directed by Lourens Blok.



"Blackhat" (2015) centers on a talented, imprisoned hacker who collaborates with the government to stop a global cyber-terrorist network. In the film, Nicholas Hathaway—a brilliant hacker portrayed by Chris Hemsworth—is recruited for the mission on the condition of his release while serving a prison sentence for cybercrimes. Alongside an international team of American and Chinese agents, Hathaway joins a global pursuit stretching from Chicago to Los Angeles and from Hong Kong to Jakarta. Their objective is to uncover the identity of the cyber-terrorist wreaking havoc on a global scale and to thwart his plans.



The controversial 2016 film "Snowden" tells the true story of Edward Snowden, the former NSA agent who exposed the U.S. government's covert, global digital surveillance and data collection activities. Directed by renowned filmmaker Oliver Stone, the film features actor Joseph Gordon-Levitt in the role of Snowden. It closely examines the Snowden affair—an event that sparked a global conversation about the secret systems enabling the U.S. (a democracy that nonetheless pursues hegemonic policies) to closely monitor its own citizens and those of other nations, and which subsequently drove the development of indigenous technologies in countries around the world.



The 2016 documentary "Zero Days" explores the true background of the world of cyber warfare and the destructive Stuxnet cyber weapon, developed by the U.S. and Israel to sabotage Iran's nuclear program. The film chronicles the emergence of Stuxnet, the world's first malware capable of inflicting physical damage on industrial systems. It recounts how the virus initially targeted only the centrifuges at Iran's Natanz nuclear facility but spiraled out of control, spreading to other systems globally. The film details the covert operation—codenamed "Operation Olympic Games"—jointly conducted by U.S. (NSA) and Israeli intelligence agencies. In doing so, it demonstrates how such cyber weapons can cripple a nation's infrastructure without the need for traditional military intervention. Furthermore, the film discusses the dangers posed by "zero-day" vulnerabilities in the digital realm and addresses the security crisis resulting from the global cyber arms race, as well as potential future scenarios of cyber warfare.



The 2019 film "The Great Hack" is a Netflix documentary that reveals the inside story of the Cambridge Analytica data scandal and how the personal data of millions of Facebook users was harvested without consent and used for political manipulation. Social media likes, searches, and browsing habits can effectively transform into massive commercial and political weapons. The film also covers Cambridge Analytica's use of data to interfere in political processes during the 2016 U.S. elections and the UK's Brexit campaign. In this regard, it explores—through real events and firsthand accounts—how the digital footprints left in the online world threaten individual and societal freedoms.

Conclusion

In conclusion, as the impact of internet-based technologies on world politics and the global economy grows, state regulations and security measures in this domain are intensifying, and the subject is becoming increasingly strategic. Consequently, cultural elements related to this field are also on the rise. In this context, this study aims to list significant films produced in the Western world that deal with cybersecurity and related technologies. Although this is not a conventional academic article, it is significant as pioneering work in a new field and for offering a selection of films suitable for use in academic studies.

The review has also demonstrated that the U.S. wields significant power and influence in this field, driven by the "Hollywood effect". Indeed, virtually all popular films produced in this sector are of U.S. origin. This highlights the importance of the "soft power" concept formulated by American political scientist Joseph S. Nye years ago. Through this means, the U.S. fosters the adoption of its culture and lifestyle by other societies while keeping its economy vibrant. Undoubtedly, however, other nations will eventually make breakthroughs in information technology, cybersecurity, and cinema as their own sectors develop. What matters to us, on the other hand, undoubtedly, is the development and growing importance of the subject and culture of cybersecurity.

BIBLIOGRAPHY

- Beyazperde.com, https://www.beyazperde.com/.
- Bıçakçı, Salih (2013), *21. Yüzyılda Siber Güvenlik*, İstanbul Bilgi Üniversitesi Yayınları.
- Imdb.com, https://www.imdb.com/.
- Rotten Tomatoes, https://www.rottentomatoes.com/.

RUSYA–UKRAYNA SAVAŞI SONRASINDA AVRUPA BİRLİĞİ DIŞ POLİTİKASININ DÖNÜŞÜMÜ: 'NORMATIVE POWER EUROPE' YAKLAŞIMININ YENİDEN DEĞERLENDİRİLMESİ

Oğuzhan MANİOĞLU[1]

Öz: Rusya Federasyonu'nun 24 Şubat 2022'de Ukrayna'ya karşı başlattığı geniş çaplı işgal, Avrupa Birliği'nin (AB) dış politika araçlarını, güvenlik anlayışını ve Rusya ile kurduğu karşılıklı bağımlılık ilişkisini önemli ölçüde değiştirmiştir. Bununla birlikte, bu değişimin, AB'nin normatif kimliğinden bütünüyle bir kopuş mu, yoksa daha önce başlayan jeopolitikleşme eğilimlerinin hızlanması mı olduğu tartışmalıdır. Bu çalışma, AB dış politikasındaki dönüşümü "Normatif Güç Avrupa" yaklaşımı çerçevesinde ve 1994–23 Temmuz 2026 dönemini kapsayan karşılaştırmalı bir doküman analiziyle incelemektedir. Araştırma korpusu, amaçlı ölçüt örneklemesiyle seçilen 25 AB ve AB–NATO belgesi ile Türkçe ve İngilizce 32 akademik çalışmadan oluşmaktadır. Belgeler; normatif gerekçelendirme, politika araçlarının normlarla uyumu ve uygulamadaki tutarlılık olmak üzere üç analitik ölçüte göre kodlanmıştır. Bulgular, 2022'nin mutlak bir başlangıçtan çok 2014 sonrasında gelişen yaptırım, enerji çeşitlendirmesi ve güvenlik kapasitesi eğilimlerini hızlandıran kritik bir eşik olduğunu; buna karşılık Avrupa Barış Fonu aracılığıyla ölümcül askerî yardımın finansmanı ile Rus enerjisinden planlı çıkışın araç setinde niteliksel kırılmalar yarattığını göstermektedir. AB'nin egemenlik, toprak bütünlüğü ve uluslararası hukuk vurgusu süreklilik sergilese de, yaptırım muafiyetleri, üye devletler arasındaki farklılıklar, alternatif enerji tedarikçileriyle ilişkiler ve NATO'ya devam eden bağımlılık normatif söylem ile uygulama arasında seçici bir uyuma işaret etmektedir. Çalışma, "Normatif Güç Avrupa" yaklaşımının AB'nin politika gerekçelerini açıklamayı sürdürdüğünü; ancak politika tasarımı ve uygulamasının, normlar ile güvenlik çıkarlarının koşullu biçimde bütünleştiği jeostratejik bir normatif güç modeliyle daha isabetli açıklanabileceğini savunmaktadır.

Anahtar Kelimeler: *Avrupa Birliği, Normatif Güç Avrupa, Rusya–Ukrayna Savaşı, Stratejik Özerklik, Enerji Güvenliği.*

Makale Geliş Tarihi: 03.09.2026

Makale Kabul Tarihi: 26.09.2026

[1] Arş. Gör. Dr., İstanbul Kent Üniversitesi İktisadi, İdari ve Sosyal Bilimler Fakültesi Siyaset Bilimi ve Kamu Yönetimi Bölümü, İstanbul, Türkiye.
E-posta: oguzhan.manioglu@kent.edu.tr.
ORCID: 0000-0001-9475-2307.

THE TRANSFORMATION OF THE EUROPEAN UNION'S FOREIGN POLICY AFTER THE RUSSIA–UKRAINE WAR: A REASSESSMENT OF THE 'NORMATIVE POWER EUROPE' APPROACH

Abstract: Russia's full-scale invasion of Ukraine on 24 February 2022 significantly altered the European Union's (EU) foreign-policy instruments, security outlook, and interdependence with Russia. It remains contested, however, whether this change represents a departure from the EU's normative identity or an acceleration of geopolitical trends already under way. This article reassesses the transformation of EU foreign policy through the "Normative Power Europe" framework by conducting a comparative document analysis covering the period from 1994 to 23 July 2026. The purposively selected corpus consists of 25 EU and EU–NATO documents and 32 academic studies published in Turkish and English. The documents were coded according to three analytical criteria: normative justification, congruence between policy instruments and declared norms, and consistency in implementation. The findings show that 2022 was not an absolute beginning but a critical juncture that accelerated sanctions, energy diversification, and security-capacity trends that had developed since 2014. At the same time, the financing of lethal military assistance through the European Peace Facility and the planned phase-out of Russian energy produced qualitative changes in the EU's policy toolbox. Although the Union has consistently invoked sovereignty, territorial integrity, and international law, sanctions exemptions, differences among member states, relations with alternative energy suppliers, and continued dependence on NATO reveal selective congruence between normative discourse and implementation. The article argues that "Normative Power Europe" continues to explain the justificatory dimension of EU policy, whereas policy design and implementation are better understood as a geostrategic form of normative power in which norms and security interests are conditionally integrated.

Keywords: *European Union, Normative Power Europe, Russia–Ukraine War, Strategic Autonomy, Energy Security.*

DOI: 10.5281/zenodo.23233997

Giriş

Avrupa Birliği'nin (AB) uluslararası rolü, uzun süre askerî güçten çok hukuk, ekonomik bütünleşme, diplomasi ve norm yayma kapasitesi üzerinden tanımlanmıştır. Maastricht Antlaşması sonrasında Ortak Dış ve Güvenlik Politikası'nın kurumsallaşması, AB'yi klasik bir devlete dönüştürmemiş; fakat demokrasi, insan hakları, hukukun üstünlüğü ve çok taraflılık gibi ilkeleri dış ilişkilerinin meşruiyet kaynağı hâline getirmiştir. Bu özgün aktörlük biçimi, önce "*sivil güç*", daha sonra "*yumuşak güç*" ve "*Normatif Güç Avrupa*" kavramlarıyla açıklanmıştır.[2]

Rusya'nın 2014'te Kırım'ı ilhakı ve Ukrayna'nın doğusundaki çatışma, AB'nin normatif iddiaları ile güvenlik ihtiyaçları arasındaki gerilimi belirginleştirmiştir. Buna rağmen, enerji karşılıklı bağımlılığı, üye devletlerin Rusya'ya ilişkin farklı tehdit algıları ve oybirliğine dayalı karar alma, 2014–2021 dönemindeki tepkinin sınırlarını çizmiştir. 24 Şubat 2022'de başlayan geniş çaplı işgal ise yaptırımların kapsamının genişletilmesi, Avrupa Barış Fonu (*European Peace Facility* – EPF) üzerinden askerî yardımın finansmanı, enerji ilişkilerinin yeniden düzenlenmesi, Ukrayna'ya aday ülke statüsü verilmesi ve AB–NATO koordinasyonunun güçlendirilmesi gibi daha ileri adımları mümkün kılmıştır.[3]

Bu değişim, literatürde iki karşıt yorumu öne çıkarmıştır. İlk yorum, savaşın AB'yi normatif ve sivil güç kalıplarından uzaklaştırarak jeopolitik bir aktöre dönüştürdüğünü savunmaktadır. İkinci yorum ise, egemenlik, toprak bütünlüğü ve uluslararası hukuk ilkelerinin AB'nin sertleşen politikasını mümkün kılan ortak gerekçeler olduğunu, dolayısıyla normların etkisini kaybetmediğini ileri sürmektedir.[4] Her iki yorumun da açıklayıcı yönleri bulunmakla birlikte, yalnızca kurumsal söyleme veya kullanılan araçların "*sert*" niteliğine odaklanmak, norm ile çıkar arasındaki ilişkinin uygulamada nasıl kurulduğunu göstermemektedir.

---

[2] François Duchêne (1972), "Europe's Role in World Peace", içinde (editör: Richard Mayne) *Europe Tomorrow: Sixteen Europeans Look Ahead*, Londra: Fontana, ss. 32–47; Joseph S. Nye, Jr. (2004), *Soft Power*, New York: PublicAffairs, ss. 5–11; Charlotte Bretherton & John Vogler (2006), *The European Union as a Global Actor*, 2. Baskı, Londra: Routledge.

[3] European Council (2022), "European Council Conclusions on Russia's Unprovoked and Unjustified Military Aggression against Ukraine", 24.02.2022, Erişim Tarihi: 20.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2022/02/24/european-council-conclusions-24-february-2022/; Tom Casier (2023), "The EU and Russia: The War That Changed Everything", *Journal of Common Market Studies*, 61(S1), ss. 31–44; Heidi Maurer & Richard G. Whitman & Nicholas Wright (2023), "The EU and the Invasion of Ukraine", *International Affairs*, 99(1), ss. 219–238.

[4] Giselle Bosse (2024), "The EU's Response to the Russian Invasion of Ukraine", *Journal of Common Market Studies*, 62(5), ss. 1222–1238; Elisabeth Johansson-Nogués & Francesca Leso (2025), "Geopolitical EU?", *Journal of Common Market Studies*, 63(1), ss. 127–142.

Bu çalışma, şu soruya cevap aramaktadır: Rusya'nın 2022'deki geniş çaplı işgali, AB dış politikasında yeni bir yönelim mi başlatmış, yoksa 2014 sonrasında gelişen eğilimleri mi hızlandırmıştır ve bu süreç Normatif Güç Avrupa yaklaşımının açıklayıcılığını nasıl etkilemiştir? Çalışmanın temel argümanı iki bölümden oluşmaktadır. Birincisi, 2022 mutlak bir başlangıç değil, 2014 sonrasında gelişen jeopolitikleşme, yaptırım ve enerji çeşitlendirmesi eğilimlerini hızlandıran kritik bir eşiktir. Buna karşılık, EPF aracılığıyla ölümcül askerî yardımın ortak biçimde finansmanı ile Rus enerjisinden planlı çıkış, araçların kapsamı ve maliyeti bakımından niteliksel değişim yaratmıştır. İkincisi, normatif ilkeler AB politikasının gerekçelendirilmesinde merkezi konumunu korurken, yaptırım muafiyetleri, karar alma tıkanmaları, alternatif enerji ortaklarının insan hakları sicili ve NATO'ya bağımlılık, normatif söylem ile uygulama arasında tam değil seçici bir uyum olduğunu göstermektedir.

Çalışmanın literatüre katkısı, "*normatif AB*" ile "*jeopolitik AB*"yi birbirini dışlayan kategoriler olarak ele almamasıdır. Bunun yerine, söylem, araç tasarımı ve uygulama düzeylerini birbirinden ayıran üç aşamalı bir değerlendirme kullanılmaktadır. Böylece, bir politikanın normatif bir dille gerekçelendirilmesi ile aynı politikanın tasarım ve sonuçlarının normatif ölçütlerle uyumlu olması arasındaki fark görünür hâle getirilmektedir. Makalenin devamında ise, önce kuramsal ve analitik çerçeve açıklanmakta, ardından araştırma tasarımı sunulmaktadır. Üçüncü bölüm, 1990'lardan 2022'ye AB–Rusya–Ukrayna ilişkilerini ve enerji transitinin jeopolitik rolünü incelemekte; dördüncü bölüm de savaş sonrasındaki yaptırım, askerî destek, güvenlik, enerji ve AB–NATO politikalarını karşılaştırmalı olarak değerlendirmektedir. Tartışma bölümünde ise alternatif açıklamalar ve karşı örnekler ele alınmaktadır.

1. Kuramsal ve Analitik Çerçeve

1.1. Sivil Güçten Normatif Güç Avrupa'ya

Duchêne'nin "*Sivil Güç Avrupa*" yaklaşımı, Avrupa bütünleşmesinin uluslararası etkisini askerî kapasiteden çok ekonomik ilişkiler, diplomasi ve kurumsal iş birliğine dayandırmıştır. Nye'ın yumuşak güç kavramı ise, tercihleri zorlama yerine çekicilik yoluyla şekillendirme kapasitesine dikkat çekmiştir. Bu iki yaklaşım, AB'nin geleneksel araçlarını açıklamakla

birlikte, Birliğin kendi kurumsal yapısından kaynaklanan norm üretme ve yayma kapasitesini tam olarak kavramsallaştırmamaktadır.[5]

Manners'ın geliştirdiği "*Normatif Güç Avrupa*" yaklaşımı bu boşluğu doldurmayı amaçlamıştır. Yaklaşıma göre, AB'nin uluslararası etkisi yalnızca sahip olduğu maddi kaynaklardan değil, uluslararası ilişkilerde "*normal*" ve meşru kabul edilen ilkelerin içeriğini belirleme kapasitesinden doğmaktadır. Barış, özgürlük, demokrasi, hukukun üstünlüğü, insan hakları ve dayanışma bu normatif kimliğin merkezindedir. Normlar; genişleme koşulluluğu, ticaret anlaşmaları, diplomatik açıklamalar, teknik yardım, yaptırımlar ve kurumsal örnek oluşturma gibi farklı kanallarla yayılabilir.[6]

Normatif Güç Avrupa yaklaşımı, AB'nin ne söylediğini ve politikalarını hangi ilkelerle meşrulaştırdığını açıklamada güçlüdür; ancak aktörün öz tanımı ile davranışının normatif sonucunu eşitleme riski taşımaktadır. Hyde-Price, AB'nin büyük güçlerin güvenlik çıkarlarından bağımsız olmadığını ve normatif söylemin maddi çıkarları örtebileceğini savunur. Toje, iddialar ile ortak eylem kapasitesi arasındaki boşluğa dikkat çeker. Smith ise, dış politikanın değerler ve çıkarlar arasında değişen uzlaşmalarla şekillendiğini gösterir.[7] Bu eleştiriler, normatifliğin yalnızca söylem üzerinden değil, seçilen araçların tasarımı ve uygulamadaki tutarlılığı üzerinden de sınanmasını gerektirir.

Rusya–Ukrayna Savaşı sonrasındaki literatür de ikili bir tablo sunmaktadır. Bosse, 2022'deki ortak tepkinin yalnızca tehdit algısıyla açıklanamayacağını, 2014 sonrasında yerleşen egemenlik ve uluslararası hukuk gerekçelerinin daha sert tedbirleri mümkün kıldığını belirtmektedir. Maurer, Whitman ve Wright, uzun süreli dış politika iş birliğinin üye devletlerde "*ortak Avrupa sorumluluğu*" normu ürettiğini savunmaktadır. Buna karşılık, Casier ile Johansson-Nogués ve Leso, söylemde belirgin bir jeopolitikleşme görülse de, ortak kapasite ve sonuç düzeyinde daha karmaşık bir tablo bulunduğunu göstermektedir.[8]

---

[5] François Duchêne (1972), "Europe's Role in World Peace", ss. 32–47; Joseph S. Nye, Jr. (2004), *Soft Power*, ss. 5–11.

[6] Ian Manners (2002), "Normative Power Europe: A Contradiction in Terms?", *Journal of Common Market Studies*, 40(2), ss. 235–258.

[7] Adrian Hyde-Price (2006), "Normative Power Europe: A Realist Critique", *Journal of European Public Policy*, 13(2), ss. 217–234; Asle Toje (2008), "The Consensus–Expectations Gap", *Security Dialogue*, 39(1), ss. 121–141; Karen E. Smith (2014), *European Union Foreign Policy in a Changing World*, 3. Baskı, Cambridge: Polity Press.

[8] Giselle Bosse (2024), "The EU's Response to the Russian Invasion of Ukraine", ss. 1222–1238; Heidi Maurer & Richard G. Whitman & Nicholas Wright (2023), "The EU and the Invasion of Ukraine", ss. 219–238; Tom Casier (2023), "The EU and Russia: The War That Changed Everything", ss. 31–44; Elisabeth Johansson-Nogués & Francesca Leso (2025), "Geopolitical EU?", ss. 127–142.

Bu çalışma, normatif güç ile jeopolitik aktörlük arasındaki ilişkiyi sıfır toplamlı bir karşıtlık olarak ele almamaktadır. Güvenlik ve jeoekonomik araçların kullanılması tek başına normatif kimliğin terk edildiğini göstermez.[9] Yaptırımlar, askerî destek veya enerji politikası egemenlik ve uluslararası hukuku koruyabilir; ancak aynı araçlar orantısız maliyet, seçici uygulama veya farklı alanlardaki norm ihlallerinin görmezden gelinmesi sonucunu da doğurabilir. Bu nedenle, değerlendirme, aracın "*yumuşak*" veya "*sert*" olmasından çok normla ilişkisinin nasıl kurulduğuna odaklanmalıdır.

1.2. Normatif Söylem ile Politikanın Normatif Niteliğini Ayırmak

Çalışmada normatiflik üç analitik düzeyde incelenmektedir. İlk düzey "*normatif gerekçelendirme*"dir. AB kurumlarının bir politikayı egemenlik, toprak bütünlüğü, demokrasi, insan hakları, hukukun üstünlüğü veya çok taraflılıkla açıkça ilişkilendirip ilişkilendirmediği değerlendirilir. Bu düzey, kurumsal söylemi gösterir; politikanın sonuçlarının normatif olduğunu tek başına kanıtlamaz.

İkinci düzey "*araç–norm uyumu*"dur. Seçilen politika aracının ilan edilen normu korumaya elverişli, hukuken temellendirilmiş ve hedefle orantılı olup olmadığı incelenir. Örneğin, hedefli yaptırımların doğrudan karar alıcıları ve savaş kapasitesini sınırlamaya yönelmesi araç–norm uyumunu güçlendirirken, kapsamı belirsiz muafiyetler veya sivil nüfusa ölçüsüz zarar riski uyumu zayıflatabilir.

Üçüncü düzey "*uygulama tutarlılığı*"dır. Üye devletlerin ortak kararlara fiilen uyumu, yük paylaşımı, istisnalar, veto ve gecikmeler ile politikanın başka alanlardaki normatif taahhütlerle çelişip çelişmediği değerlendirilir. Alternatif enerji tedarikçileriyle insan hakları koşulu aranmaksızın kurulan ilişkiler veya ortak askerî hedeflerin ulusal öncelikler nedeniyle bloke edilmesi, normatif gerekçe sürse bile uygulama tutarlılığını düşürür.

[9] Robert D. Blackwill & Jennifer M. Harris (2016), *War by Other Means: Geoeconomics and Statecraft*, Cambridge, MA: Harvard University Press.

Tablo 1. Normatiflik Değerlendirme Ölçütleri

Analiz düzeyi	**Temel soru**	**Güçlü uyum göstergesi**	**Gerilim göstergesi**
Normatif gerekçelendirme	Politika hangi ilke veya hukuk kuralıyla meşrulaştırılıyor	Egemenlik, toprak bütünlüğü ve uluslararası hukuka açık ve sürekli atıf	Değer söyleminin belirsiz veya yalnızca araçsal kullanımı
Araç–norm uyumu	Seçilen araç ilan edilen normu korumaya elverişli mi	Hukuki dayanak, hedeflilik, orantılılık ve denetim	Geniş istisnalar, dolanma kanalları veya normla çelişen araç tasarımı
Uygulama tutarlılığı	Politika üye devletler ve alanlar arasında tutarlı uygulanıyor mu	Süreklilik, yük paylaşımı ve kurumsal uygulama	Veto, gecikme, seçicilik ve başka normatif taahhütlerle çelişki

Normlar ile stratejik çıkarlar, bir politika egemenlik ve uluslararası hukuk gibi ilkeleri korurken, AB'nin güvenliğini ve kapasitesini de güçlendiriyorsa tamamlayıcıdır. Buna karşılık, güvenlik veya ekonomik çıkarlar, ilan edilen ilkelerin seçici uygulanmasına, benzer ihlallerin farklı değerlendirilmesine ya da kurumsal yükümlülüklerin aşındırılmasına yol açıyorsa norm–çıkar çatışması ortaya çıkar. Bu ayrım, AB'nin söylemde normatif kalırken uygulamada neden karma bir profil sergileyebildiğini açıklamaya imkân verir.

2. Araştırma Tasarımı ve Yöntem

2.1. Kapsam ve Belge Seçimi

Araştırma, yapılandırılmış ve karşılaştırmalı doküman analizine dayalı nitel bir vaka çalışmasıdır. Doküman analizi, kurumsal kararların zaman içindeki süreklilik ve değişimini izlemeye, resmî gerekçeler ile uygulamaya ilişkin göstergeleri aynı analitik çerçevede

karşılaştırmaya elverişlidir.[10] Vaka, AB'nin Rusya'nın Ukrayna'ya yönelik politikalarına verdiği kurumsal tepki olarak tanımlanmıştır. Zaman aralığı, AB–Rusya Ortaklık ve İşbirliği Anlaşması'nın imzalandığı 1994'ten AB'nin Rusya'ya karşı 21. yaptırım paketini kabul ettiği 23 Temmuz 2026'ya kadar uzanmaktadır.[11]

Belge korpusu, amaçlı ölçüt örneklemesiyle oluşturulmuştur. Birincil kaynaklar için üç dâhil etme ölçütü kullanılmıştır: belgenin (i) AB–Rusya veya AB–Ukrayna ilişkilerinin kurumsal çerçevesini belirlemesi; (ii) yaptırımlar, askerî destek, güvenlik ve savunma, enerji veya AB–NATO iş birliği alanlarından en az birinde politika yönelimi ya da uygulama kararı içermesi; (iii) AB kurumları veya AB–NATO tarafından yayımlanmış resmî metin olması. Haber özetleri, imzasız yorumlar, aynı kararın mükerrer dil sürümleri ve yalnızca teknik düzeltme içeren belgeler dışlanmıştır. Akademik kaynaklarda hakemli yayın, konuya doğrudan katkı ve kuramsal ya da ampirik özgünlük ölçütleri aranmış; görüş yazıları ile kaynağı belirsiz çevrim içi içerikler korpusa alınmamıştır.

Bu ölçütlerle 25 birincil kurumsal belge ve Türkçe ile İngilizce yayımlanmış 32 akademik çalışma incelenmiştir. Birincil korpus; ortaklık anlaşmaları, Avrupa Komşuluk Politikası ve Doğu Ortaklığı belgeleri, 2014 sonrası yaptırım kararları, 2016 AB Küresel Stratejisi, EPF kararları, 2022 Stratejik Pusula ve "*REPowerEU*", 2023 AB–NATO Ortak Bildirisi, 2024 Ukrayna Yardım Fonu, 2025 enerji yol haritası ve Hızlı Konuşlanma Kapasitesi belgeleri ile 2026 yaptırım ve askerî destek güncellemelerinden oluşmaktadır. Akademik korpus; Normatif Güç Avrupa'nın kurucu ve eleştirel metinleri, AB–Rusya–Ukrayna ilişkileri, enerji karşılıklı bağımlılığı, yaptırımlar, EPF, stratejik özerklik ve savaş sonrası AB aktörlüğü üzerine çalışmaları kapsamaktadır. Türkçe literatür, özellikle enerji arz güvenliği, asimetrik bağımlılık, yaptırımların maliyeti ve alternatif tedarik politikalarına ilişkin ampirik tartışmayı yerel yazınla karşılaştırmak amacıyla korpusa dâhil edilmiştir.

[10] Glenn A. Bowen (2009), "Document Analysis as a Qualitative Research Method", *Qualitative Research Journal*, 9(2), ss. 27–40.
[11] Council of the European Union (2026/a), "Russia's War against Ukraine: EU Sanctions", 23.07.2026, Erişim Tarihi: 21.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/sanctions-against-russia/.

Tablo 2. Araştırma korpusunun kapsamı

Kaynak grubu	Dönem	Belge sayısı	Seçim amacı
AB–Rusya ve AB–Ukrayna kurucu ilişki belgeleri	1994–2017	6	2022 öncesi kurumsal ve normatif tabanı belirlemek
Yaptırım, güvenlik, savunma ve enerji belgeleri	2014–2026	16	Araçların kapsam, yoğunluk ve uygulama değişimini izlemek
AB–NATO ortak belgeleri	2016–2023	3	Stratejik özerklik ile ittifak bağımlılığı ilişkisini değerlendirmek
Türkçe ve İngilizce hakemli akademik çalışmalar ile temel kitaplar	1972–2025	32	Kuramsal ölçütleri kurmak ve resmî belgeleri eleştirel literatürle karşılaştırmak
Toplam		**57**	

2.2. Kodlama, Tema Seçimi ve Sınırlılıklar

Belgeler, iki aşamada analiz edilmiştir. İlk aşamada kronolojik kodlama yapılarak 2022 öncesi ve sonrası dönemlerdeki süreklilikler, hızlanmalar ve niteliksel kırılmalar belirlenmiştir. İkinci aşamada, metinler, 5 politika teması altında kodlanmıştır: ekonomik yaptırımlar, EPF ve askerî destek, Stratejik Pusula ve savunma kapasitesi, enerji güvenliği ve "*REPowerEU*", AB–NATO iş birliği. Temalar, yalnızca savaş sonrasında öne çıktıkları için değil, normlar ile stratejik çıkarların farklı araç türlerinde sınanmasına imkân verdikleri için seçilmiştir. Yaptırımlar jeoekonomik baskıyı; EPF askerî yardımın normatif sınırlarını; Stratejik Pusula ortak kapasiteyi; *REPowerEU* karşılıklı bağımlılık ve tedarikçi seçimini; AB–NATO ilişkisi ise stratejik özerklik ile ittifak bağımlılığını temsil etmektedir.

Her tema **Tablo 1**'deki üç ölçüte göre değerlendirilmiştir. Bulgular, resmî hedef beyanlarının tekrarıyla sınırlı tutulmamış; muafiyetler, uygulama gecikmeleri, üye devlet farklılıkları ve temel argümanla çelişen örnekler özellikle aranmıştır. Kurumsal belgelerdeki iddialar, akademik çalışmalardaki bulgular ve mevcut olduğunda uygulamaya ilişkin resmî verilerle karşılaştırılmıştır. Bu yöntem, nedensel etkiyi nicel olarak ölçmez; belgelerin politika yönelimini nasıl kurduğunu ve karar tasarımının bu yönelimle ne ölçüde uyumlu olduğunu değerlendirir.

Araştırmanın 3 sınırlılığı vardır. Birincisi, kamuoyuna açık belgelere dayanılması, Konsey içi pazarlıkların ve gizli askerî kararların tümünü gözlemlemeyi engeller. İkincisi, savaş devam ettiği için uzun dönemli politika sonuçları kesinleşmemiştir. Üçüncüsü, 5 tema AB dış politikasının tamamını değil, dönüşüm iddiasını sınamak için seçilen başlıca alanları kapsamaktadır. Bu sınırlılıklar nedeniyle, çalışma, AB'nin "*normatif*" ya da "*jeopolitik*" olduğuna ilişkin kesin ve değişmez bir sınıflandırma yapmamakta; farklı politika aşamalarındaki uyum ve gerilimleri karşılaştırmaktadır.

3. 2022 Öncesinde AB–Rusya–Ukrayna Üçgeni ve Enerji Jeopolitiği

3.1. Ortaklık Siyasetinden Rekabetçi Komşuluğa

Soğuk Savaş sonrasında AB, Rusya ve Ukrayna ile ilişkilerini ortaklık, ekonomik entegrasyon ve siyasal dönüşüm beklentisi üzerinden kurdu. Rusya ile 1994'te imzalanıp 1997'de yürürlüğe giren Ortaklık ve İşbirliği Anlaşması, siyasi diyalog, ticaret ve yatırımın geliştirilmesini hedefliyordu. Ukrayna ile imzalanan benzer anlaşma 1998'de yürürlüğe girdi. Bununla birlikte iki ilişki aynı siyasal mantığa dayanmıyordu. Rusya, AB tarafından stratejik ortak ve Avrupa güvenlik düzeninin büyük bir bileşeni olarak görülürken Ukrayna uzun süre bağımsız bir jeopolitik özne olmaktan çok istikrar ve reform politikalarının hedefi olarak ele alındı.[12]

2004 genişlemesi, AB'nin sınırlarını Karadeniz ve Doğu Avrupa'ya taşıdı. Aynı yıl başlatılan Avrupa Komşuluk Politikası, komşu ülkelerde AB normlarına yakınlaşmayı üyelik vaadi olmaksızın teşvik etti. 2009'da kurulan Doğu Ortaklığı ise; Ukrayna, Moldova, Gürcistan,

[12] European Union (1997), "Agreement on Partnership and Cooperation between the European Communities and the Russian Federation", *Official Journal of the European Communities*, L 327, 28.11.1997, Erişim Tarihi: 21.08.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:21997A1128(01); European Union (1998), "Partnership and Cooperation Agreement between the European Communities and Ukraine", 01.03.1998, Erişim Tarihi: 21.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/documents-publications/treaties-agreements/agreement/?id=1994019; Elisabeth Johansson-Nogués & Francesca Leso (2025), "Geopolitical EU?", ss. 127–142.

Ermenistan, Azerbaycan ve Belarus ile siyasal ortaklık ve ekonomik bütünleşmeyi derinleştirdi. AB, bu politikaları teknik ve normatif dönüşüm programı olarak sundu; Rusya ise ortak komşuluk alanında nüfuz rekabeti olarak algıladı. Bu farklı okuma, Ukrayna'nın Avrupa yönelimi ile Rusya'nın bölgesel düzen iddiasını giderek karşı karşıya getirdi.[13]

2013 Vilnius Zirvesi öncesinde Ukrayna Devlet Başkanı Viktor Yanukoviç'in AB Ortaklık Anlaşması'nı imzalamaktan vazgeçmesi, Euromaidan protestolarını ve ardından iktidar değişimini tetikledi. Rusya'nın 2014'te Kırım'ı ilhakı ve Donbas'taki ayrılıkçı güçleri desteklemesi üzerine, AB, diplomatik kısıtlamalar, kişi ve kuruluşlara yönelik varlık dondurma kararları ile finans, savunma ve enerji alanlarında sektörel yaptırımlar uyguladı. AB–Ukrayna Ortaklık Anlaşması'nın siyasi bölümleri 2014'te, Derin ve Kapsamlı Serbest Ticaret Alanı ise 2016'da uygulanmaya başladı; anlaşma 2017'de tamamen yürürlüğe girdi.[14]

Bu dönem, normatif söylem ile stratejik ihtiyatın birlikte işlediğini gösterir. AB, Ukrayna'nın egemenliği ve toprak bütünlüğünü savundu ve yaptırımların sürdürülmesini Minsk Anlaşmaları'nın uygulanmasına bağladı. Buna karşılık, yaptırımların hedefli ve kademeli tasarlanması, enerji ilişkilerinin büyük ölçüde korunması ve Ukrayna'ya askerî destek konusunda ortak bir AB aracının kullanılmaması, üye devletlerin Rusya ile ekonomik bağlarını ve tırmanma kaygılarını yansıttı. Dolayısıyla, 2014 bir kopuş yaratmış, fakat karşılıklı bağımlılığın temel yapısını ortadan kaldırmamıştır. Sjursen ve Rosén'in gösterdiği üzere, ortak yaptırımlar normatif gerekçeler üzerinden kurulmuş; yine de maliyet ve risk dağılımı, politikanın kapsamını sınırlamıştır.[15]

3.2. Gaz Krizleri, Transit Ülke Konumu ve Boru Hattı Siyaseti

Enerji, AB–Rusya–Ukrayna üçgeninin ekonomik olduğu kadar stratejik niteliğe sahip en önemli alanıdır. Rusya başlıca üretici ve ihracatçı, AB büyük ithalat pazarı, Ukrayna ise Sovyet döneminden kalan geniş boru hattı sistemiyle temel transit ülke konumundaydı. Bu

---

[13] European Commission (2004), "European Neighbourhood Policy Strategy Paper", COM(2004) 373 final, 12.05.2004, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0373; Council of the European Union (2009), "Joint Declaration of the Prague Eastern Partnership Summit", 07.05.2009, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://www.consilium.europa.eu/media/31797/2009_eap_declaration.pdf; Kristi Raik & Steven Blockmans & Anna Osypchuk & Anton Suslov (2024), "EU Policy towards Ukraine: Entering Geopolitical Competition over European Order", *The International Spectator*, 59(1), ss. 39–58.

[14] European Union (2014), "Association Agreement between the European Union and Ukraine", *Official Journal of the European Union*, L 161, 29.05.2014, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/agree_internation/2014/295/oj/eng; Council of the European Union (2026/a), "Russia's War against Ukraine: EU Sanctions".

[15] Helene Sjursen & Guri Rosén (2017), "Arguing Sanctions: On the EU's Response to the Crisis in Ukraine", *Journal of Common Market Studies*, 55(1), ss. 20–36.

yapı karşılıklı bağımlılık yarattı; ancak tarafların bağımlılığı aynı düzeyde değildi. AB arz güvenliğine, Rusya ihracat gelirlerine, Ukrayna ise transit gelirleri ile gaz tedarikine ihtiyaç duyuyordu. Fiyat, borç ve transit tarifesi anlaşmazlıkları bu yapıyı tekrarlayan krizlere açık hâle getirdi.[16]

Ocak 2006'daki Rusya–Ukrayna gaz anlaşmazlığı sırasında Ukrayna'ya yönelik kesinti bazı Avrupa ülkelerine ulaşan akışları da düşürdü. Ocak 2009'daki ikinci kriz daha ağır sonuç doğurdu; Rus gazının Ukrayna üzerinden Avrupa'ya sevki yaklaşık iki hafta kesildi ve özellikle Orta ve Güneydoğu Avrupa ülkeleri ciddi arz açığı yaşadı. Bu krizler, ticari bir fiyat uyuşmazlığının transit altyapısı üzerinden Avrupa çapında güvenlik sorununa dönüşebildiğini gösterdi. AB'nin 2010 tarihli gaz arz güvenliği düzenlemesi, ters akış kapasitesi, depolama ve bölgesel dayanışma mekanizmalarını güçlendirmeye yönelik bir kurumsal cevap oldu.[17]

Rusya ve AB içindeki farklı aktörler, transit riskini aynı araçlarla yönetmedi. Rusya, Ukrayna'yı çevreleyen doğrudan güzergâhlara yöneldi. Baltık Denizi üzerinden Almanya'ya ulaşan Nord Stream 1, 2011–2012'de faaliyete geçti. 2015'te gündeme gelen Nord Stream 2, aynı hattın kapasitesini arttırmayı hedefledi. Karadeniz üzerinden tasarlanan South Stream projesi 2014'te iptal edildi; daha sonra Türkiye üzerinden TürkAkım geliştirildi. Bu projeler, Rusya açısından transit riskini ve Ukrayna'ya bağımlılığı azaltma aracıydı. Ukrayna açısından ise, transit gelirlerinin ve stratejik öneminin aşınması anlamına geliyordu.[18]

AB içinde boru hatlarına ilişkin ortak tutum oluşmadı. Almanya ve bazı Batı Avrupa şirketleri Nord Stream projelerini ticari arz güvenliği ve doğrudan bağlantı olarak savunurken, Polonya, Baltık ülkeleri ve Ukrayna projeleri jeopolitik risk olarak değerlendirdi. Avrupa Komisyonu, Üçüncü Enerji Paketi hükümleri ve rekabet kuralları yoluyla boru hatlarını iç pazar hukukuna bağlamaya çalıştı. Bununla birlikte, Nord Stream 2 tartışması, üye devlet çıkarları ile Enerji Birliği'nin dayanışma iddiası arasındaki ayrışmayı görünür kıldı. Siddi'nin belirttiği gibi,

[16] Eric Pardo Sauvageot (2020), "Between Russia as Producer and Ukraine as a Transit Country: EU Dilemma of Interdependence and Energy Security", *Energy Policy*, 145, 111699.
[17] Laura Rodríguez-Fernández & Ana Belén Fernández Carvajal & Luis Manuel Ruiz-Gómez (2020), "Evolution of European Union's Energy Security in Gas Supply during Russia–Ukraine Gas Crises 2006–2009", *Energy Strategy Reviews*, 30, 100518.
[18] Eric Pardo Sauvageot (2020), "Between Russia as Producer and Ukraine as a Transit Country: EU Dilemma of Interdependence and Energy Security"; Marco Siddi (2020), "Theorising Conflict and Cooperation in EU–Russia Energy Relations: Ideas, Identities and Material Factors in the Nord Stream 2 Debate", *East European Politics*, 36(4), ss. 544–563.

enerji ilişkisinde piyasa, kimlik ve jeopolitik aynı anda etkiliydi; yalnızca ticari veya yalnızca güvenlikçi bir açıklama yetersizdi.[19]

AB'nin diğer cevabı tedarik ve güzergâh çeşitlendirmesiydi. Güney Gaz Koridoru, Azerbaycan gazını Gürcistan ve Türkiye üzerinden Avrupa'ya taşımayı hedefledi; Trans Anadolu Doğalgaz Boru Hattı ve Trans Adriyatik Boru Hattı bunun temel parçaları oldu. LNG terminalleri, enterkonektörler ve depolama kapasitesi de geliştirildi. Buna rağmen, düşük maliyetli Rus gazı, mevcut altyapı ve üye devletlerin farklı enerji bileşimleri nedeniyle 2022'ye kadar Rusya'nın ağırlığı devam etti. Türkçe literatürde Gündoğdu ve Çakır Gündoğdu, 2022 krizini Soğuk Savaş sonrası enerji kırılganlıklarının devamı içinde konumlandırırken; Dinçer, asimetrik karşılıklı bağımlılığın savaş sonrasında tedarikçi ve güzergâh çeşitlendirmesini hızlandırdığını göstermektedir.[20] Böylece, 2006 ve 2009 krizlerinin ardından dayanıklılık araçları güçlenmiş olsa da, bağımlılığın siyasi sonuçları ortadan kalkmamıştır.

3.3. 2014–2021 Döneminde Kademeli Jeopolitikleşme

2014 sonrasında AB dış politikasında 2022'de görünür hâle gelecek 3 eğilim gelişti. Birincisi, ekonomik yaptırımlar dış politikanın kalıcı bir aracı oldu. Yaptırımlar 6 ayda bir yenilendi ve belirli kişi, kuruluş ve sektörlere genişletildi. İkincisi, enerji güvenliği iç pazar politikasının ötesine geçerek, dış politika ve dayanıklılık gündemiyle birleşti. Üçüncüsü, 2016 AB Küresel Stratejisi "*ilkeli pragmatizm*", dayanıklılık ve stratejik özerklik kavramlarını öne çıkararak değerler ile çıkarların birlikte yönetilmesi gerektiğini kabul etti.[21]

Bu eğilimler, 2022'deki dönüşümün kurumsal ve düşünsel öncüllerini oluşturdu. AB'nin Ukrayna'daki demokratik normları ve güvenlik sektörü reformunu destekleyen savaş öncesi politikaları da normatif etkinin güvenlik kapasitesiyle birlikte geliştiğini göstermektedir.[22] Savaş, yaptırım mantığını, enerji çeşitlendirmesini veya savunma iş birliğini ilk kez üretmedi.

---

[19] *A.g.e.*

[20] Emre Gündoğdu & Burçin Çakır Gündoğdu (2023), "Avrupa Birliği Enerji Güvenliğinin 2022 Ukrayna Krizi Bağlamında Analizi", *Marmara Üniversitesi Avrupa Araştırmaları Enstitüsü Avrupa Araştırmaları Dergisi*, 31(2), ss. 133–159; Melih Dinçer (2023), "Asimetrik Karşılıklı Bağımlılık Çerçevesinde Avrupa Birliği-Rusya Enerji İlişkilerinin Analizi: Ukrayna–Rusya Savaşı'nın AB Enerji Politikası Üzerindeki Etkisi", *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 13(2), ss. 394–433.

[21] European External Action Service (2016), *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy*, Brüksel, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf; Nathalie Tocci (2017), *Framing the EU Global Strategy: A Stronger Europe in a Fragile World*, Londra: Palgrave Macmillan.

[22] Gergana Noutcheva & Kateryna Zarembo (2025), "Normative Power at Its Unlikeliest: EU Democratic Norms and Security Service Reform in Ukraine", *Cooperation and Conflict*, 60(3), ss. 504–523.

Buna karşılık, daha önce sınırlı ve kademeli ilerleyen araçların ölçeğini büyüttü, karar hızını arttırdı ve askerî yardım ile enerji bağlarının kesilmesi gibi önceki dönemde ortak politika hâline gelemeyen seçenekleri mümkün kıldı. Bu nedenle, 2022, hem yol bağımlılığının, hem de kriz kaynaklı yeniliğin birlikte incelenmesini gerektirir.

4. Bulgular

4.1. Ekonomik Yaptırımların Kapsamı ve Sınırları

AB, 2014'te başlattığı yaptırım rejimini 2022 sonrasında kapsam, sektör ve uygulama mekanizması bakımından önemli ölçüde genişletti. Finansal kısıtlamalar, Rusya Merkez Bankası'nın rezervlerine erişimin sınırlandırılması, belirli bankaların SWIFT sisteminden çıkarılması, çift kullanımlı ve ileri teknoloji ürünlerinin ihracat kontrolü, petrol ve kömür ithalatına yönelik yasaklar ile çok sayıda kişi ve kuruluşa uygulanan tedbirler bu genişlemenin başlıca unsurlarıdır. 23 Temmuz 2026'da kabul edilen 21. paket, enerji, finansal hizmetler, kripto varlıklar ve yaptırımların dolanılmasına ilişkin tedbirleri daha da sıkılaştırmıştır.[23]

Normatif gerekçelendirme düzeyinde yaptırımlar güçlü bir süreklilik göstermektedir. Konsey belgeleri, tedbirleri, Ukrayna'nın egemenliği ve toprak bütünlüğünün korunması, saldırı savaşının maliyetinin arttırılması ve uluslararası hukukun savunulmasıyla ilişkilendirmektedir. 2014'te geliştirilen gerekçeler 2022'de terk edilmemiş; daha ağır ve maliyetli araçları meşrulaştıracak biçimde genişlemiştir. Bosse'nin bulguları, 2014 sonrasında yerleşen anlam ve gerekçelerin 2022'de üye devletler arasındaki hızlı uzlaşmayı kolaylaştırdığını desteklemektedir.[24]

Araç tasarımı ise 2014'e göre niteliksel değişim göstermiştir. Meissner ve Graziani'nin karşılaştırmalı veri seti, 2014'te hedefli ve sınırlı olan tedbirlerin 2022'de kapsamlı sektör yaptırımlarına dönüştüğünü göstermektedir. Bu değişim, AB'nin ekonomik ağırlığını güvenlik amacıyla kullanan jeoekonomik bir aktör hâline geldiğine işaret eder.[25] Yaptırımların karar alıcıları, savaş finansmanını ve askerî-teknolojik kapasiteyi hedeflemesi araç–norm uyumunu güçlendirmektedir. Düzenli gözden geçirme, insani istisnalar ve hukuki denetim de yaptırım tasarımının normatif yönünü destekler.

[23] Council of the European Union (2026/a), "Russia's War against Ukraine: EU Sanctions".
[24] Giselle Bosse (2024), "The EU's Response to the Russian Invasion of Ukraine", ss. 1222–1238.
[25] Katharina Meissner & Chiara Graziani (2023), "The Transformation and Design of EU Restrictive Measures against Russia", *Journal of European Integration*, 45(3), ss. 377–394.

Bununla birlikte, uygulama tutarlılığı sınırlıdır. Altıncı yaptırım paketinde deniz yoluyla taşınan Rus petrolü yasaklanırken, boru hattı petrolüne geçici istisna tanınması, Macaristan, Slovakya ve Çekya gibi kara ile çevrili ülkelerin enerji bağımlılıklarını yansıtmıştır. Bu istisnalar ortak kararın alınmasını sağlamış, fakat maliyetlerin üye devletler arasında eşit dağılmadığını göstermiştir.[26] Yaptırımların üçüncü ülkeler üzerinden dolanılması, Rus LNG'sinin bir süre kapsam dışında kalması ve bazı üye devletlerin uygulamadaki isteksizliği de etkinliği azaltmıştır. Battır ve Yiğittepe'nin karşılıklı ekonomik bağımlılık yaklaşımıyla ulaştığı sonuçlar da yaptırımların kısa vadeli etkisinin doğalgaz bağımlılığı ve yeni altyapının yüksek maliyeti nedeniyle sınırlandığını vurgulamaktadır.[27] Burada norm ile çıkar tamamen karşıt değildir; istisnalar koalisyonun korunması için gerekli bir uzlaşma olarak görülebilir. Ancak uzlaşma kalıcılaştığında, evrensel ilke iddiası seçici uygulamaya dönüşmektedir.

Sonuç olarak, yaptırımlar, AB'nin normatif gerekçeleri jeoekonomik kapasiteye dönüştürebildiği en güçlü alandır; fakat yaptırım birliği, homojen ulusal tercihlerden değil, farklı maliyetlerin muafiyet ve geçiş süreleriyle yönetilmesinden doğmuştur. Bu bulgu, normların ortak eylemi kolaylaştırdığını, çıkar dağılımının ise eylemin tasarımını belirlediğini göstermektedir.

4.2. Avrupa Barış Fonu ve Barış Normu ile Askerî Yardım Arasındaki Gerilim

EPF, 2021'de AB bütçesi dışında kurulan ve askerî ya da savunma etkisi olan Ortak Dış ve Güvenlik Politikası eylemlerini finanse eden bir araçtır. Rusya'nın işgalinden dört gün sonra Konsey, Ukrayna Silahlı Kuvvetlerine ölümcül ve ölümcül olmayan teçhizat sağlanmasını finanse eden yardım tedbirlerini kabul etti. AB böylece tarihinde ilk kez devam eden yüksek yoğunluklu bir savaşta üçüncü bir ülkeye ortak fon aracılığıyla ölümcül askerî teçhizat sağladı. 2022–2025 döneminde EPF üzerinden Ukrayna'nın askerî ve savunma ihtiyaçları için 6,4 milyar avro harekete geçirilmiş; 2024'te ayrıca 5 milyar avroluk Ukrayna Yardım Fonu kurulmuştur.[28]

---

[26] Council of the European Union (2026/c), "EU Sanctions against Russia: Questions and Answers", Erişim Tarihi: 22.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/; Council of the European Union (2026/d), "Timeline – EU Sanctions against Russia", Erişim Tarihi: 22.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-sanctions-against-russia/.

[27] Orhan Battır & Levent Yiğittepe (2023), "Rusya-Ukrayna Savaşında Yaptırımlar ve Enerji Güvenliği; Karşılıklı Ekonomik Bağımlılıklar Perspektifinden Bir Değerlendirme", *Yönetim ve Ekonomi Dergisi*, 30(3), ss. 549–573.

[28] Council of the European Union (2021), "Council Decision (CFSP) 2021/509 Establishing a European Peace Facility", 22.03.2021, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2021/509/oj; Council of the European Union (2022/b), "Council Decision (CFSP) 2022/338 on an Assistance Measure under

Bu adım, AB'nin sivil ve normatif güç kimliği açısından açık bir gerilim yaratmaktadır. "Barış" amacı taşıyan bir fonun silah tedarikini finanse etmesi ilk bakışta kavramsal çelişki olarak görülebilir. AB bu gerilimi, Birleşmiş Milletler Şartı'nın 51'inci maddesinde tanınan meşru müdafaa hakkı, saldırıya uğrayan devletin egemenliği ve Avrupa barış düzeninin korunması üzerinden çözmektedir. Askerî yardım bu çerçevede savaşı teşvik eden değil, saldırganlığın başarıya ulaşmasını engelleyen ve adil barışın koşullarını koruyan araç olarak sunulmaktadır.

Araç–norm uyumu bakımından bu gerekçe savunulabilir; ancak otomatik değildir. Askerî yardımın normatif niteliği, son kullanım denetimi, uluslararası insancıl hukuk, sivil kayıpların azaltılması ve siyasi çözüm arayışının sürdürülmesi gibi koşullara bağlıdır. Ayrıca EPF'nin bütçe dışı niteliği Avrupa Parlamentosunun denetimini sınırlamakta ve hesap verebilirlik tartışması yaratmaktadır. Fabbrini, EPF'nin ortak mali kapasiteyi genişlettiğini, fakat yönetişim ve mali dayanışma bakımından yapısal sınırlılıkların sürdüğünü göstermektedir.[29]

Üye devlet farklılıkları uygulama düzeyinde daha belirgindir. Askerî yardımın miktarı, türü ve zamanlaması ulusal tercihlere göre değişmiştir. Macaristan'ın bazı EPF geri ödemelerini ve Ukrayna'ya ilişkin ortak sonuçları bloke etmesi, oybirliği kuralının bir üye devlete kolektif politikayı geciktirme imkânı verdiğini göstermiştir. Buna karşılık 2024/1471 sayılı karar, Rusya'ya yönelik kısıtlayıcı tedbirler sonucunda doğan olağanüstü gelirlerden alınan mali katkıların EPF üzerinden Ukrayna'ya askerî destek için tahsisini düzenleyerek yeni bir finansman kanalı oluşturmuştur. Tarafsızlık politikası izleyen üyeler ise çekimser kalma ve belirli askerî harcamalara katkıda bulunmama düzeneklerinden yararlanmıştır.[30] Bu durum, EPF'nin AB düzeyinde önemli bir yenilik olmasına rağmen askerî desteğin büyük bölümünün ulusal kararlar ve NATO koordinasyonu üzerinden yürüdüğünü ortaya koymaktadır.

---

the European Peace Facility for the Supply to the Ukrainian Armed Forces of Military Equipment", 28.02.2022, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2022/338/oj; Council of the European Union (2024/a), "Ukraine Assistance Fund: Council Allocates €5 Billion under the European Peace Facility", 18.03.2024, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2024/03/18/ukraine-assistance-fund-council-allocates-5-billion-under-the-european-peace-facility-to-support-ukraine-militarily/; Council of the European Union (2026/b), "EU Military Support for Ukraine", Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/military-support-ukraine/.

[29] Federico Fabbrini (2023), "Funding the War in Ukraine", *Politics and Governance,* 11(4), ss. 52–61.

[30] Council of the European Union (2024/b), "Council Decision (CFSP) 2024/1471 on the Allocation of the Amounts of the Financial Contribution Paid to the European Peace Facility pursuant to Decision (CFSP) 2024/1470", 21.05.2024, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2024/1471/oj/eng; European Parliamentary Research Service (2025), *European Peace Facility – For Ukraine, but Not Only*, Brüksel: European Parliament, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772833/EPRS_BRI%282025%29772833_EN.pdf.

EPF, 2022'nin niteliksel kırılma yarattığı en açık alandır. Yine de kırılma, AB'nin barış normunu terk etmesinden çok barışı korumak için meşru zor kullanma kapasitesinin desteklenebileceği yönündeki yeniden yorumdan kaynaklanmaktadır. Normatif uyum, yardımın hukukiliği ve savunma amacıyla güçlenmekte; denetim eksikliği, ulusal vetolar ve yük paylaşımı sorunlarıyla zayıflamaktadır.

4.3. Stratejik Pusula ve Kapasite–Uygulama Açığı

Stratejik Pusula 21 Mart 2022'de, işgalden kısa süre sonra kabul edilmiş olsa da, hazırlıkları 2020'de başlamıştır. Bu zamanlama, belgenin savaşın doğrudan ürünü olmadığını; savaşın mevcut taslağın tehdit değerlendirmesini ve siyasi önemini değiştirdiğini göstermektedir. Belge, 5.000 personele kadar AB Hızlı Konuşlanma Kapasitesi, askerî hareketlilik, siber savunma, hibrit tehditlerle mücadele, ortak tatbikat ve savunma yatırımlarının güçlendirilmesi gibi hedefler belirlemiştir.[31]

Normatif gerekçelendirme belgenin merkezindedir. Stratejik Pusula, AB'nin güvenliğini demokrasi, insan hakları ve kurallara dayalı uluslararası düzenle ilişkilendirir. Bu yönüyle, kapasite artışı, salt güç maksimizasyonu değil, normatif düzeni koruma aracı olarak sunulmaktadır. 2025'te Hızlı Konuşlanma Kapasitesinin operasyonel hâle gelmesi, uzun süre uygulamaya geçirilemeyen Muharebe Gruplarına kıyasla kurumsal ilerleme anlamına gelmektedir.[32]

Bununla birlikte, operasyonel olma, bağımsız ve sürekli harekât kapasitesinin kanıtı değildir. Kuvvet üretimi, ortak finansman, siyasi yetkilendirme, stratejik ulaştırma ve istihbarat alanlarında üyelerin ve NATO'nun imkânlarına bağımlılık devam etmektedir. Helwig, savaşın AB'nin ortak karar alma kapasitesini arttırdığını; fakat ABD'nin güvenlik garantisi, istihbaratı ve askerî imkânları karşısındaki bağımlılığı da görünür kıldığını belirtmektedir.[33] Riddervold ve Rieker de, AB'nin daha olgun bir dış ve güvenlik aktörü hâline geldiğini kabul ederken, karar alma, uygulama ve kaynaklarda kalıcı boşluklar bulunduğunu göstermektedir.

---

[31] Council of the European Union (2022/a), "A Strategic Compass for Security and Defence", 21.03.2022, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf, ss. 14–25.

[32] Council of the European Union (2025), "A Strategic Compass for Security and Defence", Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/strategic-compass/.

[33] Niklas Helwig (2023), "EU Strategic Autonomy after the Russian Invasion of Ukraine", *Journal of Common Market Studies*, 61(S1), ss. 57–67; Marianne Riddervold & Pernille Rieker (2024), "Finally Coming of Age?", *European Security*, 33(3), ss. 497–516.

Bu nedenle, Stratejik Pusula'nın dönüşüm değeri, bütünleşik bir Avrupa Ordusu yaratmasından değil, güvenlik ve savunmayı AB'nin kalıcı politika gündemine yerleştirmesinden kaynaklanmaktadır. Belge, 2022 öncesi stratejik özerklik arayışını hızlandırmış; fakat egemenlik hassasiyetleri ve ulusal kapasite farklılıklarını ortadan kaldırmamıştır.

4.4. Enerji Güvenliği, Transit Güzergâhlar ve REPowerEU

Rusya'nın enerji ihracatını siyasi baskı aracı olarak kullanması ve savaşın arz fiyatları üzerindeki etkisi, 2006, 2009 ve 2014 krizlerinde görünür olan kırılganlığı 2022'de sistemik bir güvenlik sorununa dönüştürdü. Komisyonun Mayıs 2022'de açıkladığı "*REPowerEU Planı*"; enerji tasarrufu, tedarik çeşitlendirmesi, yenilenebilir enerjinin hızlandırılması ve Rus fosil yakıtlarından çıkış hedeflerini bir araya getirdi. 2025 itibarıyla Rus gazının AB ithalatındaki payı yaklaşık yüzde 12'ye gerilemiş; Rus petrolünün payı yüzde 2 düzeyine düşmüştür. Buna rağmen, AB, 2025'te 36 milyar metreküp Rus gazı ithal etmeyi sürdürmüştür. Bu durum, hızlı çeşitlendirmeye rağmen bağımlılığın tamamen sona ermediğini göstermektedir.[34]

2022 sonrası politika, önceki dönemle hem süreklilik, hem kırılma taşır. LNG altyapısı, enterkonektörler, depolama, Güney Gaz Koridoru ve yenilenebilir enerji yatırımları 2006 ve 2009 krizlerinden sonra başlamıştı. REPowerEU, bu araçları yeni bir ölçekte birleştirmiş, enerji politikasını açık biçimde Rusya'ya karşı ekonomik güvenlik stratejisine dönüştürmüş ve 2025–2026 düzenlemeleriyle Rus gazından aşamalı çıkışı hukuki takvime bağlamıştır. Kesici, savaşın ilk aylarında enerji arz güvenliğinin AB politikasındaki belirleyici ağırlığını; Adatepe ve Göçoğlu ise savaşın kurumsal enerji politikasını hızlandırırken Türkiye üzerinden yeni bir politika alternatifi ürettiğini göstermektedir.[35] Dolayısıyla, yeni olan çeşitlendirme fikri değil, karşılıklı bağımlılığı azaltmaya yönelik siyasi kararlılığın kapsamı ve bağlayıcılığıdır.

---

[34] European Commission (2022/a), "REPowerEU Plan", COM(2022) 230 final, 18.05.2022, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:230:FIN; European Commission (2025), "Roadmap towards Ending Russian Energy Imports", COM(2025) 440 final, 06.05.2025, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0440; European Commission (2026), "REPowerEU Four Years On", Erişim Tarihi: 23.08.2026, Erişim Adresi: https://energy.ec.europa.eu/strategy/repowereu-phase-out-russian-energy-imports/repowereu-4-years_en.

[35] Gülnaz Ece Kesici (2022), "Rusya–Ukrayna Savaşı'nın AB'nin Enerji Politikalarına Yansıması", *EURO Politika*, 15, ss. 46–54; Merve Adatepe & Volkan Göçoğlu (2025), "Rusya-Ukrayna Savaşında Avrupa Birliğinin Enerji Politikası ve Türkiye", *TESAM Akademi Dergisi*, 12(1), ss. 243–276.

Normatif ve stratejik hedefler bu alanda kısmen tamamlayıcıdır. Rus fosil yakıtlarından çıkış, savaş gelirlerini azaltma, AB'nin dış baskıya açıklığını düşürme ve yeşil dönüşümü hızlandırma potansiyeli taşır. Buna karşılık, kısa vadeli arz güvenliği için LNG ve alternatif boru hattı gazına yönelmek, iklim hedefleri ve insan hakları politikasıyla gerilim yaratmaktadır. AB ile Azerbaycan arasında Temmuz 2022'de imzalanan enerji mutabakatı, Güney Gaz Koridoru'nun kapasitesini 2027'ye kadar yıllık en az 20 milyar metreküpe çıkarmayı hedeflemiştir.[36] Azerbaycan'ın AB açısından güvenilir enerji ortağı olarak tanımlanması, demokrasi ve insan hakları koşullarının enerji güvenliği karşısındaki ağırlığına ilişkin eleştirileri güçlendirmiştir.

Vezzoni, REPowerEU'nun yeşil dönüşüm, piyasa düzeni ve jeopolitik çeşitlendirme hedefleri arasında dağılımsal ve normatif çelişkiler taşıdığını belirtmektedir. Yeni LNG terminallerinin fosil yakıt bağımlılığını kilitleme riski, yüksek enerji fiyatlarının toplumsal maliyeti ve tedarikçi değişiminin yeni bağımlılıklar üretmesi bu çelişkilerin başlıca örnekleridir.[37] Öte yandan, yenilenebilir enerji, enerji verimliliği ve ortak depolama kuralları uzun vadede hem iklim normlarını hem stratejik dayanıklılığı desteklemektedir.

Enerji politikası bu nedenle jeostratejik normatif gücün en koşullu alanıdır. Rusya'ya bağımlılığın azaltılması, Ukrayna ile dayanışma ve Avrupa güvenliğiyle uyumludur; ancak alternatif ortaklıkların seçimi ve fosil altyapı yatırımları normatif tutarlılığı sınamaktadır. AB'nin başarısı yalnızca Rus ithalatının azalmasıyla değil, yeni bağımlılıkların demokrasi, iklim ve dayanışma hedefleriyle nasıl yönetildiğiyle ölçülmelidir.

4.5. AB–NATO İş Birliği ve Stratejik Özerkliğin Yeniden Tanımlanması

AB–NATO ilişkileri, 2003 Berlin Plus düzenlemelerinden bu yana kurumsal bir çerçeveye sahipti. 2016 ve 2018 ortak bildirileri hibrit tehditler, siber güvenlik, tatbikatlar ve askerî hareketlilik alanlarında iş birliğini geliştirdi. 10 Ocak 2023 tarihli üçüncü Ortak Bildiri, Rusya'nın savaşını Avrupa-Atlantik güvenliğine yönelik en ciddi tehdit olarak tanımlamış;

[36] European Commission (2022/b), "EU and Azerbaijan Enhance Bilateral Relations, Including Energy Cooperation", 18.07.2022, Erişim Tarihi: 24.08.2026, Erişim Adresi: https://enlargement.ec.europa.eu/news/eu-and-azerbaijan-enhance-bilateral-relations-including-energy-cooperation-2022-07-18_en.

[37] Rubén Vezzoni (2023), "Green Growth for Whom, How and Why?", *Energy Research & Social Science*, 101, 103134.

kritik altyapı, yeni teknolojiler, uzay, iklim ve dış müdahale gibi alanları iş birliği gündemine eklemiştir.[38]

Savaş, iki örgüt arasında işlevsel bir görev paylaşımını güçlendirmiştir. NATO kolektif savunma, caydırıcılık ve yüksek yoğunluklu askerî planlamanın merkezi olmaya devam ederken, AB de yaptırımlar, enerji, finansman, düzenleme, askerî hareketlilik ve savunma sanayii araçlarını kullanmıştır. Bu tamamlayıcılık, AB'nin sahip olduğu farklı politika yetkilerini ortak güvenlik amacıyla seferber etmesine imkân vermiştir. Maurer, Whitman ve Wright'ın "*ortak Avrupa sorumluluğu*" yaklaşımı, AB'nin NATO'nun yerine geçmeden kolektif eylem üretebilmesini açıklamaktadır.[39]

Ancak tamamlayıcılık, stratejik özerkliğin gerçekleştiği anlamına gelmemektedir. Ukrayna'ya sağlanan ileri askerî sistemler, istihbarat, stratejik nakliye ve caydırıcılık büyük ölçüde ABD ve NATO imkânlarına dayanmaktadır. Finlandiya ve İsveç'in NATO'ya katılması, Avrupa güvenliğinde İttifakın merkezi rolünü daha da pekiştirmiştir. Stratejik özerklik, bu ortamda NATO'dan ayrışma değil, Avrupa'nın ittifak içindeki kapasitesini arttırma ve gerektiğinde kendi tercihlerine göre hareket edebilme yeteneği olarak yeniden tanımlanmıştır.[40]

Bu yeniden tanımlama, norm–çıkar ilişkisini de değiştirir. NATO ile koordinasyon, Ukrayna'nın savunulması ve uluslararası hukuk düzeninin korunması bakımından normatif hedefleri desteklemektedir. Buna karşılık, karar ve kapasite bağımlılığı, AB'nin ABD'nin tercihleri değiştiğinde aynı hedefleri sürdürüp sürdüremeyeceği sorusunu açık bırakmaktadır. Dolayısıyla, AB–NATO iş birliği kısa vadede etkililiği arttırırken, uzun vadede özerklik iddiasının maddi sınırlarını görünür kılmaktadır.

[38] NATO & European Union (2016), "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO", 08.07.2016, Erişim Tarihi: 24.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/meetings/international-summit/2016/07/08-09/; NATO & European Union (2018), "Joint Declaration on EU–NATO Cooperation", 10.07.2018, Erişim Tarihi: 24.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/; NATO & European Union (2023), "Joint Declaration on EU–NATO Cooperation", 10.01.2023, Erişim Tarihi: 24.08.2026, Erişim Adresi: https://www.nato.int/cps/en/natohq/official_texts_210549.htm.

[39] Heidi Maurer & Richard G. Whitman & Nicholas Wright (2023), "The EU and the Invasion of Ukraine", ss. 219–238.

[40] Niklas Helwig (2023), "EU Strategic Autonomy after the Russian Invasion of Ukraine", ss. 57–67.

4.6. 2022 Öncesi ve Sonrası Dönüşümün Karşılaştırılması

Tablo 3. AB dış politikasında süreklilik, hızlanma ve niteliksel değişim

Politika alanı	**2022 öncesi eğilim**	**2022 sonrası değişim**	**Analitik değerlendirme**
Yaptırımlar	2014'ten itibaren hedefli, kademeli ve sektörel tedbirler	Kapsamlı finans, teknoloji, enerji ve dolanmayı önleme rejimi	Ölçek ve maliyette niteliksel artış; muafiyetler uygulama tutarlılığını sınırlıyor
Askerî destek	Ortak AB düzeyinde sınırlı; yardım ağırlıkla ulusal ve ölümcül olmayan nitelikte	EPF üzerinden ölümcül teçhizat ve ortak finansman	Araç setinde niteliksel kırılma; barış normu savunma ve meşru müdafaa üzerinden yeniden yorumlanıyor
Savunma kapasitesi	Muharebe Grupları, 2016 Küresel Strateji ve stratejik özerklik tartışması	Stratejik Pusula, Hızlı Konuşlanma Kapasitesi ve savunma hazırlığı	Önceki eğilimin hızlanması; kapasite–uygulama açığı sürüyor
Enerji	2006 ve 2009 sonrası çeşitlendirme, depolama ve piyasa entegrasyonu; Rus gazının yüksek payı	*REPowerEU*, Rus fosil yakıtlarından aşamalı çıkış ve yeni tedarik ortaklıkları	Siyasi amaç ve bağlayıcılıkta kırılma; yeni bağımlılık ve normatif seçicilik riski
AB–NATO	2016 ve 2018 bildirileriyle artan iş birliği	2023 bildirisi ve belirgin görev paylaşımı	Tamamlayıcılık güçleniyor; ABD ve NATO'ya maddi bağımlılık sürüyor

Tablo 3, savaş sonrasındaki dönüşümün tek biçimli olmadığını göstermektedir. Yaptırımlar, enerji çeşitlendirmesi, savunma iş birliği ve AB–NATO koordinasyonu 2022'den önce başlamış eğilimlerdir. Savaş, bunların hızını, kapsamını ve siyasi önceliğini arttırmıştır.

EPF'nin Ukrayna'ya ölümcül askerî yardım için kullanılması ve Rus enerjisinden çıkışın takvime bağlanması ise araç setinde niteliksel değişim oluşturmuştur. Bu nedenle, "*dönüşüm*", bütün geçmiş politikaların terk edilmesi değil, mevcut kurumsal yolların kriz koşullarında genişletilmesi ve bazı politika tabularının aşılmasıdır.

5. Tartışma

Bulgular, Normatif Güç Avrupa yaklaşımının tamamen geçersizleştiği tezini desteklememektedir. Egemenlik, toprak bütünlüğü, meşru müdafaa ve uluslararası hukuk, AB'nin yaptırım, askerî yardım ve diplomatik desteğini gerekçelendiren ortak çerçeveyi oluşturmuştur. Üye devletlerin Rusya ile farklı ekonomik bağlara ve tehdit algılarına sahip olmalarına rağmen yüksek maliyetli tedbirlerde uzlaşabilmesi, normların yalnızca süsleyici söylem olmadığını göstermektedir. Bosse ile Sjursen ve Rosén'in çalışmalarında vurgulanan normatif uzlaşma, 2014'te oluşan gerekçelerin 2022'de daha sert araçlara taşınmasını açıklamaktadır.[41]

Bununla birlikte, söylemsel süreklilik, politikanın bütün aşamalarında normatif tutarlılık bulunduğu anlamına gelmez. Yaptırımlardaki boru hattı istisnaları, EPF kararlarının bloke edilmesi, Rus gazından çıkarken insan hakları sicili tartışmalı tedarikçilerle ilişkilerin genişletilmesi ve NATO kapasitesine bağımlılık, uygulamanın stratejik ve ulusal çıkarlarla biçimlendiğini göstermektedir. Normatif Güç Avrupa yaklaşımı, bu farklılıkları tek başına açıklamakta yetersiz kalmaktadır.

Realist açıklama, Rusya'nın yarattığı ortak tehdidin üye devletleri daha maliyetli eyleme yönelttiğini ve askerî kapasitenin önemini artırdığını doğru biçimde saptar. Ancak 2022'nin ilk aylarında Fransa ve Almanya gibi büyük üyelerin ulusal tercihlerini yeniden tanımlamakta zorlanması, ortak tepkinin yalnızca en güçlü devletlerin çıkarlarıyla açıklanamayacağını gösterir. Ayrıca, Ukrayna'ya destek, kısa vadeli ekonomik maliyetlere rağmen sürdürülmüş ve uluslararası hukuk gerekçesi ortak kararların merkezinde kalmıştır.[42]

Kurumsalcı açıklama da önemli bir tamamlayıcıdır. 2014 sonrasında oluşan yaptırım prosedürleri, EPF'nin 2021'de kurulmuş olması, Komisyon'un enerji ve ticaret yetkileri ile NATO ile daha önce geliştirilen iş birliği kanalları, 2022'de hızlı eylemin kurumsal

[41] Giselle Bosse (2024), "The EU's Response to the Russian Invasion of Ukraine", ss. 1222–1238; Helene Sjursen & Guri Rosén (2017), "Arguing Sanctions: On the EU's Response to the Crisis in Ukraine", ss. 20–36.
[42] Giselle Bosse (2024), "The EU's Response to the Russian Invasion of Ukraine", ss. 1222–1238; Giselle Bosse (2022), "Values, Rights, and Changing Interests", ", *Contemporary Security Policy*, 43(3), ss. 531–546.

altyapısını sağlamıştır. Başka bir ifadeyle, kriz, boşlukta politika üretmemiş; önceden var olan kurumları yeni amaçlarla genişletmiştir. Bu durum, 2022'yi hem yol bağımlı, hem dönüştürücü kılar.

Çalışmanın bulguları, "*jeostratejik normatif güç*" olarak adlandırılabilecek koşullu bir modele işaret etmektedir. Bu modelde, normlar, AB'nin hangi ihlali sorun olarak tanımladığını ve ortak politikanın meşruiyetini belirler. Stratejik çıkarlar ve maddi kapasite ise, hangi aracın, ne hızla ve hangi istisnalarla uygulanacağını şekillendirir. İki unsur, 3 koşulda tamamlayıcıdır: stratejik araç ilan edilen normun korunmasına doğrudan hizmet ettiğinde, aracın hukuki ve demokratik denetimi bulunduğunda ve maliyetler üyeler arasında kabul edilebilir biçimde paylaşıldığında. Bu koşullar zayıfladığında, stratejik çıkarlar normların seçici uygulanmasına yol açar.

Nissen ve Dreyer'in "*şüpheci liberalizm*" yaklaşımı, AB'nin liberal hedeflerini korurken, güç, dayanıklılık ve bağımlılık yönetimine daha fazla önem vermesini açıklamaktadır. Helwig'in stratejik özerklik değerlendirmesi de, özerkliğin mutlak bağımsızlık değil, karşılıklı bağımlılık içinde ortak eylem kapasitesi olarak okunması gerektiğini göstermektedir.[43] Bu çalışmalarla uyumlu olarak, makalenin bulguları, savaşın AB'yi normatif olmaktan jeopolitik olmaya taşıyan doğrusal bir geçiş yaratmadığını; normatif hedeflerin daha maliyetli güvenlik ve jeoekonomik araçlarla izlenmesini hızlandırdığını ortaya koymaktadır.

Yine de, bu bütünleşmenin kalıcılığı kesin değildir. Kararlar büyük ölçüde kriz koşullarında alınmıştır; oybirliği kuralı, ulusal seçimler, bütçe baskısı ve savaş yorgunluğu ortak politikanın geri döndürülebilirliğini arttırmaktadır. Hızlı Konuşlanma Kapasitesinin operasyonel ilan edilmesi ile fiilen kullanılabilir olması, Rus enerji payının azalması ile yeni tedarik bağımlılıklarının sürdürülebilir biçimde yönetilmesi ve yaptırım paketlerinin kabulü ile etkin uygulanması arasında önemli farklar vardır. Dolayısıyla, dönüşümün ölçütü yalnızca yeni belge ve araçların kabulü değil, bunların zaman içinde uygulanmasıdır.

Sonuç

Bu çalışma, Rusya'nın 2022'de Ukrayna'ya karşı başlattığı geniş çaplı işgalin AB dış politikasında hem süreklilik, hem de değişim ürettiğini göstermektedir. 2006 ve 2009 gaz krizleri enerji dayanıklılığı gündemini, 2014'teki Kırım'ın ilhakı yaptırım rejimini, 2016

[43] Christine Nissen & Jakob Dreyer (2024), "From Optimist to Sceptical Liberalism", *International Affairs*, 100(2), ss. 675–690; Niklas Helwig (2023), "EU Strategic Autonomy after the Russian Invasion of Ukraine", ss. 57–67.

Küresel Stratejisi stratejik özerklik tartışmasını, 2016 ve 2018 AB–NATO bildirileri ise güvenlik iş birliğini savaş öncesinde başlatmıştı. Bu nedenle, 2022, AB'nin jeopolitikleşmesinin başlangıç noktası değildir.

Bununla birlikte, savaş, daha önce kademeli ilerleyen eğilimleri hızlandırmış ve iki alanda niteliksel kırılma yaratmıştır. Birincisi, EPF'nin devam eden bir savaşta ölümcül askerî teçhizatı finanse etmek için kullanılmasıdır. İkincisi, Rus fosil yakıtlarıyla karşılıklı bağımlılığın yönetilmesi yerine bu bağımlılığı sona erdirmeye yönelik ortak ve giderek bağlayıcı bir politika benimsenmesidir. Yaptırımların kapsamı, savunma hazırlığı ve AB–NATO görev paylaşımı da önceki döneme göre belirgin biçimde genişlemiştir.

Normatif Güç Avrupa yaklaşımı, AB'nin neden egemenlik, toprak bütünlüğü ve uluslararası hukuku ortak eylemin meşruiyet temeli yaptığını açıklamaya devam etmektedir. Ancak yaklaşım, normatif söylem ile araç tasarımı ve uygulama arasındaki fark gözetilmeden kullanıldığında AB politikasındaki istisnaları ve güç ilişkilerini görünmez kılmaktadır. Yaptırım muafiyetleri, EPF'deki karar alma tıkanmaları, alternatif enerji tedarikçileriyle değer–çıkar gerilimleri ve NATO'ya devam eden bağımlılık, normatif uyumun seçici ve alana göre değişen bir niteliğe sahip olduğunu göstermektedir.

Bu nedenle, savaş sonrasındaki AB dış politikası, normatif gücün terk edilmesi olarak değil, normların güvenlik ve jeoekonomik kapasiteyle koşullu biçimde bütünleştiği jeostratejik bir normatif güç modeli olarak değerlendirilmelidir. Bu model, normları dış politikanın yönünü belirleyen fakat uygulamanın bütün sonuçlarını tek başına açıklamayan unsurlar olarak ele almaktadır. Çalışmanın kuramsal katkısı, normatiflik değerlendirmesini söylem, araç ve uygulama düzeylerine ayırarak AB'nin aynı anda hem normatif süreklilik, hem stratejik uyarlama gösterebilmesini açıklamasıdır.

Araştırma, kamuya açık belgelerle ve 5 politika alanıyla sınırlıdır. Gelecek çalışmalar, Konsey içi müzakereleri, ulusal parlamento tartışmalarını, yaptırımların sektör ve toplum düzeyindeki etkilerini ve alternatif enerji ortaklıklarının insan hakları koşullarını karşılaştırmalı vaka çalışmalarıyla inceleyebilir. Savaşın seyri ve transatlantik ilişkilerdeki değişim de AB'nin kriz sırasında geliştirdiği araçların kalıcı kurumsal kapasiteye dönüşüp dönüşmediğini belirleyecektir.

KAYNAKÇA

- Adatepe, Merve & Göçoğlu, Volkan (2025), "Rusya-Ukrayna Savaşında Avrupa Birliğinin Enerji Politikası ve Türkiye: Kamu Politikası Süreci Çerçevesinde Bir Analiz", *TESAM Akademi Dergisi*, 12(1), ss. 243–276.
- Battır, Orhan & Yiğittepe, Levent (2023), "Rusya-Ukrayna Savaşında Yaptırımlar ve Enerji Güvenliği; Karşılıklı Ekonomik Bağımlılıklar Perspektifinden Bir Değerlendirme", *Yönetim ve Ekonomi Dergisi*, 30(3), ss. 549–573.
- Blackwill, Robert D. & Harris, Jennifer M. (2016), *War by Other Means: Geoeconomics and Statecraft*, Cambridge, MA: Harvard University Press.
- Bosse, Giselle (2022), "Values, Rights, and Changing Interests: The EU's Response to the War against Ukraine and the Responsibility to Protect Europeans", *Contemporary Security Policy*, 43(3), ss. 531–546.
- Bosse, Giselle (2024), "The EU's Response to the Russian Invasion of Ukraine: Invoking Norms and Values in Times of Fundamental Rupture", *Journal of Common Market Studies*, 62(5), ss. 1222–1238.
- Bowen, Glenn A. (2009), "Document Analysis as a Qualitative Research Method", *Qualitative Research Journal*, 9(2), ss. 27–40.
- Bretherton, Charlotte & Vogler, John (2006), *The European Union as a Global Actor*, 2. Baskı, Londra: Routledge.
- Casier, Tom (2023), "The EU and Russia: The War That Changed Everything", *Journal of Common Market Studies*, 61(S1), ss. 31–44.
- Council of the European Union (2009), "Joint Declaration of the Prague Eastern Partnership Summit", 07.05.2009, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://www.consilium.europa.eu/media/31797/2009_eap_declaration.pdf.
- Council of the European Union (2021), "Council Decision (CFSP) 2021/509 Establishing a European Peace Facility", 22.03.2021, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2021/509/oj.
- Council of the European Union (2022/a), "A Strategic Compass for Security and Defence", 21.03.2022, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.
- Council of the European Union (2022/b), "Council Decision (CFSP) 2022/338 on an Assistance Measure under the European Peace Facility for the Supply to the Ukrainian Armed Forces of Military Equipment", 28.02.2022, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2022/338/oj.
- Council of the European Union (2024/a), "Ukraine Assistance Fund: Council Allocates €5 Billion under the European Peace Facility", 18.03.2024, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2024/03/18/ukraine-assistance-fund-council-allocates-5-billion-under-the-european-peace-facility-to-support-ukraine-militarily/.
- Council of the European Union (2024/b), "Council Decision (CFSP) 2024/1471 on the Allocation of the Amounts of the Financial Contribution Paid to the European Peace Facility pursuant to Decision (CFSP) 2024/1470", 21.05.2024, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2024/1471/oj/eng.

- Council of the European Union (2025), "A Strategic Compass for Security and Defence", Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/strategic-compass/.
- Council of the European Union (2026/a), "Russia's War against Ukraine: EU Sanctions", 23.07.2026, Erişim Tarihi: 21.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/sanctions-against-russia/.
- Council of the European Union (2026/b), "EU Military Support for Ukraine", Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/military-support-ukraine/.
- Council of the European Union (2026/c), "EU Sanctions against Russia: Questions and Answers", Erişim Tarihi: 22.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/.
- Council of the European Union (2026/d), "Timeline – EU Sanctions against Russia", Erişim Tarihi: 22.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-sanctions-against-russia/.
- Dinçer, Melih (2023), "Asimetrik Karşılıklı Bağımlılık Çerçevesinde Avrupa Birliği-Rusya Enerji İlişkilerinin Analizi: Ukrayna–Rusya Savaşı'nın AB Enerji Politikası Üzerindeki Etkisi", *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 13(2), ss. 394–433.
- Duchêne, François (1972), "Europe's Role in World Peace", içinde (editör: Richard Mayne) *Europe Tomorrow: Sixteen Europeans Look Ahead*, Londra: Fontana, ss. 32–47.
- European Commission (2004), "European Neighbourhood Policy Strategy Paper", COM(2004) 373 final, 12.05.2004, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0373.
- European Commission (2022/a), "REPowerEU Plan", COM(2022) 230 final, 18.05.2022, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:230:FIN.
- European Commission (2022/b), "EU and Azerbaijan Enhance Bilateral Relations, Including Energy Cooperation", 18.07.2022, Erişim Tarihi: 24.08.2026, Erişim Adresi: https://enlargement.ec.europa.eu/news/eu-and-azerbaijan-enhance-bilateral-relations-including-energy-cooperation-2022-07-18_en.
- European Commission (2025), "Roadmap towards Ending Russian Energy Imports", COM(2025) 440 final, 06.05.2025, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0440.
- European Commission (2026), "REPowerEU Four Years On", Erişim Tarihi: 23.08.2026, Erişim Adresi: https://energy.ec.europa.eu/strategy/repowereu-phase-out-russian-energy-imports/repowereu-4-years_en.
- European Council (2022), "European Council Conclusions on Russia's Unprovoked and Unjustified Military Aggression against Ukraine", 24.02.2022, Erişim Tarihi: 20.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2022/02/24/european-council-conclusions-24-february-2022/.

- European External Action Service (2016), *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy*, Brüksel, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.
- European Parliamentary Research Service (2025), *European Peace Facility – For Ukraine, but Not Only*, Brüksel: European Parliament, Erişim Tarihi: 23.08.2026, Erişim Adresi: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772833/EPRS_BRI%282025%29772833_EN.pdf.
- European Union (1997), "Agreement on Partnership and Cooperation between the European Communities and the Russian Federation", *Official Journal of the European Communities*, L 327, 28.11.1997, Erişim Tarihi: 21.08.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:21997A1128(01).
- European Union (1998), "Partnership and Cooperation Agreement between the European Communities and Ukraine", 01.03.1998, Erişim Tarihi: 21.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/documents-publications/treaties-agreements/agreement/?id=1994019.
- European Union (2014), "Association Agreement between the European Union and Ukraine", *Official Journal of the European Union*, L 161, 29.05.2014, Erişim Tarihi: 22.08.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/agree_internation/2014/295/oj/eng.
- Fabbrini, Federico (2023), "Funding the War in Ukraine: The European Peace Facility, the Macro-Financial Assistance Instrument, and the Slow Rise of an EU Fiscal Capacity", *Politics and Governance*, 11(4), ss. 52–61.
- Gündoğdu, Emre & Gündoğdu, Burçin Çakır (2023), "Avrupa Birliği Enerji Güvenliğinin 2022 Ukrayna Krizi Bağlamında Analizi", *Marmara Üniversitesi Avrupa Araştırmaları Enstitüsü Avrupa Araştırmaları Dergisi*, 31(2), ss. 133–159.
- Helwig, Niklas (2023), "EU Strategic Autonomy after the Russian Invasion of Ukraine: Europe's Capacity to Act in Times of War", *Journal of Common Market Studies*, 61(S1), ss. 57–67.
- Hyde-Price, Adrian (2006), "Normative Power Europe: A Realist Critique", *Journal of European Public Policy*, 13(2), ss. 217–234.
- Johansson-Nogués, Elisabeth & Leso, Francesca (2025), "Geopolitical EU? The EU's Wartime Assistance to Ukraine", *Journal of Common Market Studies*, 63(1), ss. 127–142.
- Kesici, Gülnaz Ece (2022), "Rusya–Ukrayna Savaşı'nın AB'nin Enerji Politikalarına Yansıması", *EURO Politika*, 15, ss. 46–54.
- Manners, Ian (2002), "Normative Power Europe: A Contradiction in Terms?", *Journal of Common Market Studies*, 40(2), ss. 235–258.
- Maurer, Heidi & Whitman, Richard G. & Wright, Nicholas (2023), "The EU and the Invasion of Ukraine: A Collective Responsibility to Act?", *International Affairs*, 99(1), ss. 219–238.

- Meissner, Katharina & Graziani, Chiara (2023), "The Transformation and Design of EU Restrictive Measures against Russia", *Journal of European Integration*, 45(3), ss. 377–394.
- NATO & European Union (2016), "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of NATO", 08.07.2016, Erişim Tarihi: 24.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/meetings/international-summit/2016/07/08-09/.
- NATO & European Union (2018), "Joint Declaration on EU–NATO Cooperation", 10.07.2018, Erişim Tarihi: 24.08.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/.
- NATO & European Union (2023), "Joint Declaration on EU–NATO Cooperation", 10.01.2023, Erişim Tarihi: 24.08.2026, Erişim Adresi: https://www.nato.int/cps/en/natohq/official_texts_210549.htm.
- Nissen, Christine & Dreyer, Jakob (2024), "From Optimist to Sceptical Liberalism: Reforging European Union Foreign Policy amid Crises", *International Affairs*, 100(2), ss. 675–690.
- Noutcheva, Gergana & Zarembo, Kateryna (2025), "Normative Power at Its Unlikeliest: EU Democratic Norms and Security Service Reform in Ukraine", *Cooperation and Conflict*, 60(3), ss. 504–523.
- Nye, Joseph S., Jr. (2004), *Soft Power: The Means to Success in World Politics*, New York: PublicAffairs.
- Pardo Sauvageot, Eric (2020), "Between Russia as Producer and Ukraine as a Transit Country: EU Dilemma of Interdependence and Energy Security", *Energy Policy*, 145, 111699.
- Raik, Kristi & Blockmans, Steven & Osypchuk, Anna & Suslov, Anton (2024), "EU Policy towards Ukraine: Entering Geopolitical Competition over European Order", *The International Spectator*, 59(1), ss. 39–58.
- Riddervold, Marianne & Rieker, Pernille (2024), "Finally Coming of Age? EU Foreign and Security Policy after Ukraine", *European Security*, 33(3), ss. 497–516.
- Rodríguez-Fernández, Laura & Fernández Carvajal, Ana Belén & Ruiz-Gómez, Luis Manuel (2020), "Evolution of European Union's Energy Security in Gas Supply during Russia–Ukraine Gas Crises 2006–2009", *Energy Strategy Reviews*, 30, 100518.
- Siddi, Marco (2020), "Theorising Conflict and Cooperation in EU–Russia Energy Relations: Ideas, Identities and Material Factors in the Nord Stream 2 Debate", *East European Politics*, 36(4), ss. 544–563.
- Sjursen, Helene & Rosén, Guri (2017), "Arguing Sanctions: On the EU's Response to the Crisis in Ukraine", *Journal of Common Market Studies*, 55(1), ss. 20–36.
- Smith, Karen E. (2014), *European Union Foreign Policy in a Changing World*, 3. Baskı, Cambridge: Polity Press.
- Tocci, Nathalie (2017), *Framing the EU Global Strategy: A Stronger Europe in a Fragile World*, Londra: Palgrave Macmillan.

- Toje, Asle (2008), "The Consensus–Expectations Gap: Explaining Europe's Ineffective Foreign Policy", *Security Dialogue,* 39(1), ss. 121–141.
- Vezzoni, Rubén (2023), "Green Growth for Whom, How and Why? The REPowerEU Plan and the Inconsistencies of European Union Energy Policy", *Energy Research & Social Science,* 101, 103134.

AVRUPA BİRLİĞİ GÜVENLİK GİRİŞİMLERİNİN UKRAYNA-RUSYA SAVAŞI ÇERÇEVESİNDE DÖNÜŞÜMÜ: DOST VE DÜŞMAN ALGISININ BELİRGİNLEŞMESİ (2022-2026)

Mehmet EMİR[1]

İsmail Hakkı PEKİN[2]

Öz: Ukrayna ve Rusya arasında 2022 yılı başında başlayan savaş, Avrupa Birliği'nin Soğuk Savaş sonrasından itibaren kural koyan ve sivil güç kimliği odağında kurduğu güvenlik yaklaşımını temelden değiştirmiştir. Bu çalışmada, devam eden savaşın Avrupa Birliği'nin güvenlik girişimlerine etkileri; savaş öncesi, savaş süreci ve 2024-2026 yılları arasındaki kurumsallaşma boyutuyla ele alınmaktadır. Ayrıca, siber güvenlik ile dost ve düşman algısındaki dönüşümler de analiz edilmiştir. Araştırmada, ontolojik güvenlik, kolektif güvenlikleştirme ve kriz anlarında kurumsal inşa yaklaşımını bütünlük içinde ele alan nitel bir süreç izleme tasarımı izlenmiştir. Avrupa Birliği'nin dönüşümü, Ortak Güvenlik ve Savunma Politikası'ndan ziyade, piyasa, bütçe, sanayi ve düzenleme yetkileri üzerinden gerçekleşmiştir. Dolayısıyla, bu dönüşüm, piyasa aracılığıyla güvenlik olarak kavramsallaşmıştır. Siber güvenlik yönüyle, Avrupa Birliği, tarafsız bir düzenleyici anlayıştan, tedarik zincirlerinde dost ve düşman tanımlamasını hukuki bir temele dayandıran jeopolitik odağında siber egemenlik yaklaşımına yönelmiştir. Algısal düzeyde devam eden savaş çerçevesinde Rusya düşmanlaştırılırken, ABD ise güvenilir bir müttefik konumundan şüphe uyandıran bir aktöre dönüşmüştür. Avrupa Birliği, bu durum karşısında askeri bağımlılık ile tek başına bırakılma korkusu arasında büyük bir çıkmaza sürüklenmiştir. Araştırma sonucuna göre, Avrupa Birliği'nin güvenlik dönüşümünün derinden ilerlediği, ancak henüz tamamlanmadığı; bununla beraber kapasite inşasının, bütünlük motivasyonunun ve özerklik arayışlarının devam ettiği paradoksal bir yapının sürdüğü değerlendirilmiştir.

Anahtar Kelimeler: *Avrupa Birliği, Avrupa Güvenliği, Siber Güvenlik, Stratejik Özerklik, Ukrayna-Rusya Savaşı.*

Makale Geliş Tarihi: 28.10.2026

Makale Kabul Tarihi: 03.11.2026

[1] Dr., Uluslararası İlişkiler.
Email: mehmetemir019@gmail.com.
ORCID: 0000-0003-3143-1439.
[2] (E) Korgeneral, Eski Genelkurmay İstihbarat Başkanı.

THE TRANSFORMATION OF EUROPEAN UNION SECURITY INITIATIVES IN THE CONTEXT OF THE UKRAINE-RUSSIA WAR: THE SHARPENING OF FRIEND AND FOE PERCEPTIONS (2022-2026)

Abstract: The war between Ukraine and Russia, which began in early 2022, has fundamentally altered the European Union's security approach—a framework that, since the end of the Cold War, has centered on the EU's identity as a "civilian power" and a rule-setter. This study examines how the ongoing conflict has affected the European Union's security initiatives, covering the period before the war, the conflict's duration, and the institutionalization phase spanning 2024–2026. It also analyzes shifts in cybersecurity and perceptions of "friends" and "enemies". The research uses a qualitative process-tracing design, integrating ontological security, collective securitization, and institutional construction during times of crisis. The European Union has transformed not primarily through its Common Security and Defense Policy, but through its powers over markets, budgets, industry, and regulation; consequently, this transformation is conceptualized here as "security through the market". In cybersecurity, the EU has shifted from neutral regulation toward a "cyber-sovereignty" approach—rooted in geopolitics and a legal framework that distinguishes between friends and enemies within supply chains. At the level of perception, the ongoing war has led to the framing of Russia as an "enemy", while the United States has transitioned from being viewed as a reliable ally to an actor now regarded with suspicion. Faced with this reality, the European Union faces a profound dilemma: caught between its military dependence on others and the fear of being left to fend for itself. The study concludes that while the European Union's security transformation is well underway, it remains incomplete; the EU continues to exist within a paradoxical structure characterized by ongoing capacity-building, a drive toward internal cohesion, and a persistent quest for strategic autonomy.

Keywords: *European Union, European Security, Cybersecurity, Strategic Autonomy, Ukraine-Russia War.*

DOI: 10.5281/zenodo.24254334

Giriş

Ukrayna ve Rusya arasında 24 Şubat 2022 tarihinde başlayan savaş, İkinci Dünya Savaşı'nın ardından Avrupa'da yaşanan en kapsamlı konvansiyonel savaş olarak, Avrupa Birliği'nin (AB) Soğuk Savaş sonrası güvenlik yaklaşımını temelden dönüştürmüştür. Bu dönüşümde, özellikle devletlerarası karşılıklı bağımlılığın barışa katkı sağlayacağı, devlet sınırlarının zorla değiştirilemeyeceği ve Avrupa'nın güvenliğinin Amerika Birleşik Devletleri (ABD) ile Kuzey Atlantik Antlaşması Örgütü (NATO) tarafından sağlanacağı varsayımları etkisini yitirmiştir.[3] Ukrayna-Rusya Savaşı'nın AB bütünleşmesi için, özellikle ortak savunma anlayışında, önemli bir dönüm noktası (*zeitenwende*) olup olmayacağı ise hâlâ tartışma konusu olmaya devam etmektedir.[4]

Savaşın 4 yılı aşan sürecinde AB tarafından atılan adımlar, bugüne kadarki Birliğin geleneksel uygulamalarıyla karşılaştırıldığında olağanüstü dikkat çekicidir. Bu bağlamda, ilk kez Avrupa Barış Tesisi (European Peace Facility/EPF) aracılığıyla üçüncü devletlere silah verilmiş, 2022 yılı Mart ayında Stratejik Pusula kabul edilmiş ve 2026 yılı Temmuz ayında da Rusya'ya yönelik yeni bir yaptırım paketi uygulamaya konulmuştur.[5] Bunun yanı sıra, Ukrayna ve Moldova'ya adaylık statüsü tanınmış[6], üye devletlerin ortak savunma ihtiyaçlarının karşılanması için 150 milyar avroya kadar kredi sağlayan Avrupa için Güvenlik Eylemi (Security Action for Europe/SAFE) programı oluşturulmuş ve Ukrayna'nın 2026-2027 ihtiyaçlarının karşılanması için 90 milyar avroluk bir destek kredisinin sağlanması konusunda 2025 yılı Aralık ayında uzlaşılmıştır.[7] Bütün bu adımlar, aslında Birliğin geleneksel anlamda

[3] Mitchell A. Orenstein (2023), "The European Union's Transformation after Russia's Attack on Ukraine", *Journal of European Integration*, 45(3), ss. 333–340.
[4] Daniel Fiott (2023), "In Every Crisis an Opportunity? European Union Integration in Defence and the War on Ukraine", *Journal of European Integration*, 45(3), ss. 447–460; Bernhard Blumenau (2022), "Breaking with Convention? Zeitenwende and the Traditional Pillars of German Foreign Policy", *International Affairs*, 98(6), ss. 1895–1913.
[5] Avrupa Birliği Konseyi (2026), "21st Package of Sanctions: EU Hits Russian Energy, Financial Services and Crypto Hard", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2026/07/23/21st-package-of-sanctions-eu-hits-russian-energy-financial-services-and-crypto-hard/.
[6] Avrupa Konseyi (2022), "European Council Conclusions, 23-24 June 2022", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2022/06/24/european-council-conclusions-23-24-june-2022/.
[7] Avrupa Birliği Konseyi (2025), "SAFE: Council Adopts €150 Billion Boost for Joint Procurement on European Security and Defence", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2025/05/27/safe-council-adopts-150-billion-boost-for-joint-procurement-on-european-security-and-defence/pdf/; Avrupa Konseyi (2025), "European Council, 18 December 2025 - Main Results", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/meetings/european-council/2025/12/18/; Avrupa Birliği Konseyi (2025), "Establishing the Security Action for Europe (SAFE) through the Reinforcement of the European Defence Industry Instrument", Erişim Tarihi: 18.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2025/1106/oj/eng.

bir savunma örgütüne dönüşmediğini; buna karşın devam eden savaşa, genişleme ve mali destek ile enerji gibi askeri alan dışındaki konular üzerinden güvenlikleştirme yoluyla tepki verdiğini göstermektedir.[8]

Bu görünüm, AB hakkında farklı değerlendirmelere yol açmıştır. Bir yaklaşıma göre, Avrupa Birliği'nin krizler ve zorluklar çerçevesinde ilerlediği doğrulanmış ve bu bağlamda özellikle Avrupa Birliği Komisyonu daha ön plana çıkarak jeopolitik bir aktöre dönüşmüştür.[9] Diğer bir yaklaşıma göre ise, bu savaş odağında AB'nin tepkisi, dikkat çekici bir dönüm noktası olmasından çok, onlarca yıllık dış politikadaki iş birliği potansiyelini ve bunun sınırlarını ortaya çıkaran bir farkındalık sağlamıştır.[10] Son yaklaşıma göre, krizler ve zorluklar aslında Avrupa'yı her seferinde çok katmanlı bir doğrultuda biçimlendirmektedir.[11]

Araştırma, söz konusu yaklaşımlara dair şu soruyla katkı sağlamayı amaçlamaktadır: Halen devam eden Ukrayna-Rusya Savaşı, AB'nin güvenlik girişimini hangi mekanizmalar vasıtasıyla, hangi alanlarda ve hangi boyutta dönüştürmüştür ve bu dönüşüm, Birlik seviyesinde siber güvenlik yaklaşımını ve dost-düşman algısını nasıl yeniden tanımlamıştır? Çalışmanın argümanı ise 3 parçadan oluşmaktadır. Öncelikle AB'nin dönüşümü Ortak Güvenlik ve Savunma Politikası'nın (OGSP) hükümetler arası odağına nazaran Birliğin piyasa modelini uyguladığı, sanayi, bütçe ve düzenleme yetkileriyle gerçekleşmektedir. İkincisi, siber güvenlik alanında, AB, teknik olarak tarafsız bir düzenleyici rolünden, tedarik zincirlerinde devletler seviyesinde endişe verici ve yüksek riskli gibi kategorileri fiilen tanımlayan bir jeopolitik siber güvenlik yaklaşımına yönelmiştir. Son olarak, savaş bağlamında Rusya doğrudan bir düşman olarak tanımlanırken, ABD ise güvenilir bir müttefikten şüphe duyulan bir aktöre dönüşmüştür.[12] Bu çerçevede, Birlik, yalnız bırakılma ile askeri bağımlılık arasında bir sorunla karşı karşıya kalmıştır.

---

[8] Mitchell A. Orenstein (2026), "Securitisation of EU Policy: How Russia's Invasion of Ukraine is Changing Europe", *Journal of European Public Policy*, 33(7), ss. 1763–1778.

[9] Calle Håkansson (2024), "The Ukraine War and the Emergence of the European Commission as a Geopolitical Actor", *Journal of European Integration,* 46(1), ss. 25–39; Pierre Haroche (2023), "A 'Geopolitical Commission': Supranationalism Meets Global Power Competition", *JCMS: Journal of Common Market Studies*, 61(4), ss. 970–983.

[10] Heidi Maurer & Richard G. Whitman, & Nicholas Wright (2023), "The EU and the Invasion of Ukraine: A Collective Responsibility to Act?", *International Affairs*, 99(1), ss. 219–238.

[11] Veronica Anghel & Erik Jones (2023), "Is Europe Really Forged through Crisis? Pandemic EU and the Russia–Ukraine War", *Journal of European Public Policy*, 30(4), ss. 766-781.

[12] Frida Ghitis (2026), "Trump's Pro-Russian Turn Puts Ukraine—and Europe—on Edge", *World Politics Review*, 15.10.2026, Erişim Tarihi: 19.10.2026, Erişim Adresi: https://www.worldpoliticsreview.com/trump-putin-pro-russia-ukraine-zelenskyy-europe/; The White House (2025), "National Security Strategy of the United States of America", Erişim Tarihi: 30.09.2026, Erişim Adresi: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf; Léonie Allard & Rachel Rizzo (2025), "Transatlantic Security in a New Era", *Survival*, 67(2), ss. 85–93; Avrupa Birliği Komisyonu & Yüksek

Araştırma, teorik çerçevenin değerlendirilmesinin ardından, savaş öncesi yaklaşımı, savaşın başlangıcındaki yaklaşımı (2022-2024), devam eden kurumsallaşma sürecini (2024-2026), siber güvenliği ve dost-düşman algısını analiz ederek, son olarak da dönüşümün tamamlanmamış niteliğini üç yapısal çıkmaz üzerinden değerlendirmektedir.

1. Teorik ve Yöntemsel Çerçeve

Avrupa Birliği'nin güvenlik dönüşümünün tek bir teoriyle açıklanması gerek AB'nin kendine özgü yapısı, gerekse de dönüşümün çok boyutlu yapısı nedeniyle yetersiz kalmaktadır. Bu nedenle, çalışmada ontolojik güvenlik, kolektif güvenlikleştirme ve kriz anlarında (savaş gibi) kurumsal inşa modeli birbirini tamamlayacak şekilde kullanılmıştır.

Kopenhag Okulu çerçevesinde güvenlikleştirme yaklaşımı: güvenliğin nesnel bir durumdan çok sorunun varoluşsal bir tehdit olarak gösterilmesi ve olağan politikanın dışına çıkılarak alınacak tedbirlerin meşrulaştırıldığı söz edimiyle başlatılan süreci kapsamaktadır.[13] Buna karşın, güvenlikleştirmenin AB'ye uyarlanmasıyla, tehdit tanımının Birlik kurumsal yapısı tarafından ve üye devletlerin ortaklaşa tesis ettiği bütüncül bir politika tepkisiyle kurumsallaştığı kolektif güvenlikleştirme modeli önerilmiştir.[14] Önerilen bu model, savaş durumuna göre uyarlanarak AB liderlerinin söz edimi vasıtasıyla genişleme, göç, enerji ve yaptırım gibi alanlarda hızla güvenlikleştirme yaptığını ve bu sayede olağan normlara aykırı politikaların izlendiğini göstermektedir.[15] Bu yaklaşım, tehdidin nasıl inşa edildiğini ve olağanüstü tedbirlerin nasıl meşrulaştırıldığını açıklamak için oldukça uygun bir çerçeve sunmaktadır.

Aktörlerin fiziki güvenliğinin yanı sıra, ötekilerle anlamlı ve rutinleşmiş ilişkiler aracılığıyla sürdürülen istikrarlı benlik algısı, yani benliğin güvenliği, ontolojik güvenlik üzerinden vurgulanmaktadır.[16] Ukrayna-Rusya Savaşı, aynı zamanda AB'nin kural koyucu ve sivil güç benliğini sarsarak ontolojik bir güvenlik krizini tetikleyen bir olaydır[17]; bu durum karşısında

Temsilcilik (2025), "Joint White Paper for European Defence Readiness 2030 - Join(2025) 120 Final", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0120.

[13] Barry Buzan & Ole Waever, & Jaap de Wilde (1998), *Security: A New Framework for Analysis*, Boulder, Colorado: Lynne Rienner Publishers.

[14] James Sperling & Mark Webber (2019), "The European Union: Security Governance and Collective Securitisation", *West European Politics*, 42(2), ss. 228–254.

[15] Mitchell A. Orenstein (2026), "Securitisation of EU Policy: How Russia's Invasion of Ukraine is Changing Europe", ss. 1764–1778.

[16] Jennifer Mitzen (2006), "Ontological Security in World Politics: State Identity and the Security Dilemma", *European Journal of International Relations,* 12(3), ss. 341–365.

[17] Vincent Della Sala (2023), "Ontological Security, Crisis and Political Myth: The Ukraine War and the European Union", *Journal of European Integration*, 45(3), ss. 361–371; François Duchêne (1972), "Europe's Role in World Peace", içinde (editör: Richard Mayne) *Europe Tomorrow: Sixteen Europeans Look Ahead*,

Birlik, bu rollerini terk ederek ya da yeniden tanımlayarak yanıt vermiştir.[18] Dolayısıyla, AB kendini Rusya ve Ukrayna gibi ötekilere karşı yeniden inşa etmiştir.[19] Bu bakış açısı, dost ve düşman algısındaki değişimin, diğer bir ifadeyle, AB'nin kim olduğu ve kime karşı konumlandığını anlamada vazgeçilmezdir.

Karşılaştırmalı siyasette krizler ve savaşlar devlet oluşumunu açıklamak için sıklıkla kullanılmaktadır.[20] AB'nin güçlü bir hukuki otoritesi bulunmasına rağmen[21], zorlayıcı, idari ve mali açıdan zayıf kalmasının bir nedeni de tarihsel bağlamda askeri tehditlerden çok piyasa mekanizmasıyla şekillenmiş olmasıdır.[22] Rusya ve Ukrayna arasındaki savaş, dış bir tehdit oluşturarak Birliğin kurumsal yapısındaki dönüşümü hızlandırmıştır.[23] Bu bağlamda, her ne kadar krizler ve savaşlar kurumsal gelişime yönelik hamleler üretse de, bu politikaların yeni reform döngüleriyle birlikte başarısız olma ihtimali vardır.[24] Bu bakış açısı, AB'nin dönüşümünün hangi kurumlar aracılığıyla ve hangi sınırlar içinde gerçekleştiğini açıklamaya yardımcı olacaktır.

Araştırma nitel bir tasarıma dayanırken, süreç izleme yöntemini belge analiziyle birlikte ele almaktadır. Çalışmanın birincil kaynakları; Avrupa Güvenlik Stratejisi (2003), AB Küresel Strateji Belgesi (2016), Stratejik Pusula (2022), Avrupa Savunma Sanayisi Stratejisi (2024), Avrupa Savunması Beyaz Kitabı (2025), SAFE Tüzüğü, Siber Güvenlik Yasası revizyon önerisi

---

Londra: Fontana, ss. 32–47; Hedley Bull (1982), "Civilian Power Europe: A Contradiction in Terms?", *JCMS: Journal of Common Market Studies*, 21(2), ss. 149–170.

[18] Gordon M. Friedrichs & Jule Sommer (2025), "Ontological Security Crisis and Role Conception Change: The Impact of the Russian Invasion of Ukraine on the European Union's Role Conceptions", *European Journal of International Relations,* 31(1), ss. 126–145.

[19] Kateryna Pishchikova (2025), "European Identity Construction after the Russian Full-Scale Invasion of Ukraine: Dialogic (Re)Construction of Self and Others", *JCMS: Journal of Common Market Studies,* 63(5), ss. ss. 1571–1586.

[20] Charles Tilly (1990), *Coercion, Capital, and European States, Ad 990-1992,* Cambridge, Massachusetts: Basil Blackwell.

[21] Philipp Genschel (2022), "Bellicist Integration? The War in Ukraine, the European Union and Core State Powers", *Journal of European Public Policy*, 29(12), ss. 1885–1898.

[22] R. Daniel Kelemen & Kathleen R. McNamara (2022), "State-Building and the European Union: Markets, War, and Europe's Uneven Political Development", *Comparative Political Studies*, 55(6), ss. 963–984; Pierre Haroche (2024), "Geoeconomic Power Europe: When Global Power Competition Drives EU Integration", *JCMS: Journal of Common Market Studies* 62(4), ss. 939–949; Kathleen R. McNamara (2024), "Transforming Europe? The EU's Industrial Policy and Geopolitical Turn", *Journal of European Public Policy,* 31(9), ss. 2374–2387; Anna Herranz-Surrallés & Chad Damro, & Sandra Eckert (2024), "The Geoeconomic Turn of the Single European Market? Conceptual Challenges and Empirical Trends", *JCMS: Journal of Common Market Studies,* 62(4), ss. 921–931.

[23] Philipp Genschel & Lauren Leek, & Jordy Weyns (2023), "War and Integration. The Russian Attack on Ukraine and the Institutional Development of the EU", *Journal of European Integration*, 45(3), ss. 343–357.

[24] Julian Bergmann & Patrick Müller (2021), "Failing Forward in the EU's Common Security and Defense Policy: The Integration of EU Crisis Management", *Journal of European Public Policy*, 28(10), ss. 1669–1682; Erik Jones & R. Daniel Kelemen, & Sophie Meunier (2021), "Failing Forward? Crises and Patterns of European Integration", *Journal of European Public Policy,* 28(10), ss. 1525–1533.

(2026) ve Avrupa Konseyi sonuç bildirgelerinden oluşmaktadır. Nicel açıklamalar için Avrupa Savunma Kurumu'nun (ASK) verileri kullanılmıştır. İkincil kaynak olarak internet üzerinden akademik veri tabanları taranarak, kuramsal klasiklerin yanında özellikle 2021-2026 yılları arasında yayımlanmış hakemli makalelerden yararlanılmıştır. Çalışmadaki temel sınırlılık, Ukrayna-Rusya Savaşı'nın hâlâ devam ediyor olması ve resmî belgelerin çoğunlukla gerçekleşen politikalardan ziyade beyan edilen niyetleri yansıtmasıdır. Bu nedenle, araştırma söylem ve uygulama arasındaki ilişkiyi gözlemleyerek ilerleyecektir.

2. AB'nin Savaş Öncesi Güvenlik Yaklaşımı: Kural Koyan Güç, Karşılıklı Bağımlılık ve Stratejik Özerklik

2.1. Stratejik Belgelerde Rusya: Yakınlaşmadan Stratejik Meydan Okuyan Aktöre Dönüşüm

Avrupa Birliği'nin savaş öncesindeki güvenlik yaklaşımı kural koyan bir Avrupa olarak kavramsallaştırılmıştır.[25] Bu kavram, Birliğin etkisini askeri kapasiteden çok normların yayılmasıyla göstermeye çalıştığı bir kimlik anlayışı etrafında şekillenmiştir. Bu bağlamda, Avrupa Güvenlik Stratejisi (2003), Avrupa'nın refah seviyesinin yüksek, güvenli ve özgür olduğu iyimserliğiyle açılmış ve tehdit kaynaklarını terörizm, başarısız devletler, bölgesel çatışmalar, organize suç ve kitle imha silahlarının yayılması olarak tanımlamıştır.[26] Bu belgede, Rusya, Avrupa açısından daha yakın ilişkilerin kurulması gereken ve aynı zamanda Avrupa'nın refahı ve güvenliği için önemli bir aktör olarak görülmüştür.

Rusya'nın Gürcistan ile savaşı (2008) ve Kırım'ın ilhakı (2014) Avrupa Birliği ile olan ilişkilerini zayıflatmıştır. AB Küresel Stratejisi (2016), ilkeli pragmatizm ve toplumsal dayanıklılık kavramlarına odaklanarak Birliğin dış politika tercihinin daha realist bir bakış açısına yöneldiğini göstermiştir.[27] Rusya'nın politikaları bu belgede önemli bir stratejik meydan okuma olarak değerlendirilmiş[28]; ancak seçici uygulamaları da içeren rekabet ve iş birliği

[25] Ian Manners (2002), "Normative Power Europe: A Contradiction in Terms?", *JCMS: Journal of Common Market Studies,* 40(2), ss. 235–254; Chad Damro (2012), "Market Power Europe", *Journal of European Public Policy*, 19(5), ss 682–698; Anu Bradford (2020), *The Brussels Effect: How the European Union Rules the World*, New York: Oxford University Press, ss. 7–24.
[26] Avrupa Birliği Konseyi (2009), "Secure Europe in a Better World: European Security Strategy", Erişim Tarihi: 26.09.2026, Erişim Adresi: https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf.
[27] Ana E. Juncos (2017), "Resilience as the New EU Foreign Policy Paradigm: A Pragmatist Turn?", *European Security,* 26(1), ss. 1–15; Nathalie Tocci (2017), "From the European Security Strategy to the EU Global Strategy: Explaining the Journey", *International Politics*, 54(4), ss. 487–501.
[28] Avrupa Birliği (2016), "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

arasında belirsiz bir konumlandırma benimsenmiştir. Küresel Strateji Belgesi, dış politikanın yansımasının yanı sıra Birliğin içsel amaçları ve kimliğine yönelik bir güvence arayışıdır.[29] Rusya'nın 2014 yılındaki Kırım ilhakına rağmen, AB, normları koruyan ve sivil güç ilkeleri gereği bu aktörü belirsiz bir ortak olarak tanımlamayı tercih etmiştir.[30]

Bu belirsizliğin temeli, enerji alanındaki karşılıklı bağımlılığa dayanmıştır. Komisyon verilerine göre AB, tükettiği doğal gazın yaklaşık yüzde 90'ını ithal ederken, bu ithalatın yüzde 45'i Rusya'dan sağlanıyordu.[31] Rusya tarafından Kırım'ın ilhakı sonrasında bile taraflar arasında Kuzey Akımı 2 projesinin devam etmesi, ekonomik karşılıklı bağımlılığın siyasal dönüşüm ve barış üreteceği varsayımına dayanmıştır.[32]

Avrupa Birliği strateji belgelerinde (2003-2025) temel aktörlerin konumlandırılmasına bakıldığında, bu dönemdeki dönüşüm kolaylıkla anlaşılmaktadır.[33] Avrupa Güvenlik Stratejisi'nde (2003), Rusya daha yakın ilişkiler kurulması gereken, güvenlik ve refah açısından önemli bir aktör olarak tanımlanmıştır. ABD ise, Avrupa'nın güvenliği açısından yeri doldurulamaz bir transatlantik müttefik olarak konumlandırılmıştır. Belgede, Çin, stratejik ortaklığın geliştirilmesi gereken bir aktör olarak anılmıştır. AB Küresel Strateji Belgesi'nde (2016), Rusya, stratejik olarak meydan okuyan bir aktör olarak görülürken, politikalarda seçici angajman yöntemi benimsenmiştir. NATO ve ABD ise, güçlü bağlara dayanan transatlantik ortaklıklar olarak değerlendirilmiştir.[34] Çin bağlamında ise hukukun üstünlüğüne ve karşılıklı

[29] Maria Mälksoo (2016), "From the ESS to the EU Global Strategy: External Policy, Internal Purpose", *Contemporary Security Policy*, 37(3), ss. 374–384.
[30] Gordon M. Friedrichs & Jule Sommer (2025), "Ontological Security Crisis and Role Conception Change: The Impact of the Russian Invasion of Ukraine on the European Union's Role Conceptions", ss. 126–145.
[31] Avrupa Birliği Komisyonu (2022), "Repowereu Plan (Com(2022) 230 Final)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0230; Avrupa Birliği Komisyonu (2022), "Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Repowereu: Joint European Action for More Affordable, Secure and Sustainable Energy (Com/2022/108 Final)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/resource.html?uri=cellar:71767319-9f0a-11ec-83e1-01aa75ed71a1.0001.02/DOC_1&format=PDF,
[32] Mitchell A. Orenstein (2023), "The European Union's Transformation after Russia's Attack on Ukraine", ss. 1897–1907.
[33] Avrupa Birliği Konseyi (2009), "Secure Europe in a Better World: European Security Strategy", Erişim Tarihi: 26.09.2026, Erişim Adresi: https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf; Avrupa Birliği (2016), "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf; Avrupa Birliği Komisyonu & Yüksek Temsilcilik (2019), "EU-China – a Strategic Outlook (Join(2019) 5 Final)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0005; Avrupa Birliği Komisyonu & Yüksek Temsilcilik (2025), "Joint White Paper for European Defence Readiness 2030 - Join(2025) 120 Final", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0120.
[34] Catherine Hoeffler & Stéphanie C. Hofmann, & Frédéric Mérand (2024), "The Polycrisis and EU Security and Defence Competences", *Journal of European Public Policy,* 31(10), ss. 3224–3244.

saygıya dayalı ilişkilere önem verildiği belirtilmiştir. AB-Çin Stratejik Bakış Belgesi'nde (2019), Çin, iş birliği ve müzakere edilebilir, ancak aynı zamanda hem ekonomik, hem de sistemsel bir rakip olarak görülmüştür. Stratejik Pusula Belgesi'nde (2022), Rusya, Avrupa güvenliği için uzun vadeli ve doğrudan bir tehdit olarak tanımlanmıştır. ABD ise, en önemli stratejik aktör olarak görülmüştür. Çin'e yönelik iş birliği ortamıyla birlikte hem ekonomik, hem de sistemsel bir rakip olarak konumlandırma yaklaşımı korunmuştur. Beyaz Kitap / Hazırlık 2030 Belgesi'nde (2025) ise, Rusya, yakın gelecekte temel bir tehdit kaynağı olarak görülmüştür. ABD ise, verdiği güvenceleri belirsizleşen ve Avrupa'dan daha fazla sorumluluk üstlenmesini bekleyen bir aktör olarak tanımlanmıştır. Çin ise rekabetin ve kaygıların derinleştiği bir aktör olarak anılmıştır.

2.2. Savunmanın Dağınıklığı ve Stratejik Özerklik Yaklaşımı

Ukrayna-Rusya Savaşı'ndan önce AB'nin savunma boyutuyla ilgili etkisi, beklentilerle kapasite arasında bir boşluk olduğu yönündeydi.[35] Avrupa savunma ve güvenliği için 2016 yılı sonrasında Daimî Yapılandırılmış İş Birliği (PESCO), Koordineli Yıllık Savunma Gözden Geçirme (CARD) ve Avrupa Savunma Fonu (ASF) uygulamaya konulmuştur. Bu yeni dönüşüme yönelik farklı bakış açıları ortaya konmuştur. Bir görüşe göre ASF'nin oluşumu Komisyon'un girişimiyle başlamış bir neofonksiyonalist yaklaşımken[36], diğer bir görüşe göre ise bu fonun oluşumuyla Komisyon'un devlet düzenleri ve ulusal askeri kapasiteler üzerindeki etkileri tartışılmıştır.[37] Diğer bir görüş ise, savunma pazarına yönelik AB'nin piyasa atılımının, sanayi politikasına doğru bir jeoekonomik dönüşümü işaret ettiğini belirtmektedir.[38]

Ancak AB'nin kurumsal girişimleri, üye devletlerin ulusal savunma planlarındaki farklılıkları çok az ölçüde giderebilmiştir. ASK'nın verilerine göre, 2014 yılında üye devletlerin toplam savunma harcaması 147 milyar avroyken, bu harcama 2025 yılında 418 milyar avroya yükselmiştir. Ancak savunma harcamalarındaki bu artış, büyük ölçüde ortak tedarik ve entegre kapasitenin geliştirilmesinden değil, ulusal devletler aracılığıyla gerçekleşmiştir.[39] Stratejik

[35] Christopher Hill (1993), "The Capability-Expectations Gap, or Conceptualizing Europe's International Role", *Journal of Common Market Studies,* 31(3), ss. 305–326.
[36] Pierre Haroche (2020), "Supranationalism Strikes back: a Neofunctionalist Account of the European Defence Fund", *Journal of European Public Policy*, 27(6), ss. 853–867.
[37] Catherine Hoeffler (2023), "Beyond the Regulatory State? The European Defence Fund and National Military Capacities", *Journal of European Public Policy,* 30(7), ss. 1281–1300.
[38] Daniel Fiott (2024), "From Liberalisation to Industrial Policy: Towards a Geoeconomic Turn in the European Defence Market?", *JCMS: Journal of Common Market Studies,* 62(4), ss. 1012–1024.
[39] Avrupa Savunma Kurumu (2026), "Defence Data Portal: Aggregated Data (All Member States)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.eda.europa.eu/publications-and-data/defence-data; Antonio Calcara & Luis Simón (2021), "Market Size and the Political Economy of European Defense", *Security Studies*, 30(5), ss. 865–892.

özerklik kavramı da AB içinde tartışmalı bir konu olarak kalmıştır. Stratejik özerkliğin NATO için bir tehdit değil, buna karşın bir fırsat olabileceği ve Avrupa'nın sorumluluk paylaşımının transatlantik ilişkileri güçlendirebileceği fikri ortaya konmuştur.[40] Ancak kavramın farklı şekillerde değerlendirildiği görüşler de vardır.[41] Bu bağlamda, stratejik özerkliğin ABD'den bağımsız bir üçüncü yol olduğu gerekçesiyle Orta ve Doğu Avrupa aktörleri arasında olumsuzluk hâkimken, Fransa ise (çekincelerle birlikte Almanya da dahil olmak üzere) kavramın belirsizleşen uluslararası düzende zorunlu bir güvence stratejisi olduğunu savunmuştur.[42] Ayrıca savunma konsepti, teknolojinin egemenliğine doğru genişleyen hegemonik bir dönüşümün gerçekleştiğini göstermektedir.[43] Sonuç olarak, savaş öncesinde AB jeopolitik bir güç olma iddiasını fikir olarak ortaya koyan ancak bunu kurumsal, mali ve askeri yönleriyle gerçekleştiremeyen bir aktör görünümündeydi.

3. Savaşta Kriz Yönetiminden Taraf Olmaya Dönüşüm (2022-2024)

3.1. Avrupa Barış Tesisi, Stratejik Pusula ve Zihinsel Kalıpların Dönüşümü

Ukrayna-Rusya Savaşı'nın henüz başlangıcında AB'nin uzun süredir uyguladığı güvenlik kalıpları hızla değişmiştir. 2021 yılında bütçenin dışında bir araç olarak oluşturulan Avrupa Barış Tesisi (EPF), ilk kez 28 Şubat 2022 tarihinde üçüncü bir devlete öldürücü askeri teçhizat sağlamak için kullanılmıştır. Savaş öncesinde şartlarının belirlendiği bu fon sistemi, savaşla birlikte önemli bir destek aracı haline gelmiştir.[44] Diğer yandan, üye devletlerin yaptırımlar ve

[40] Jolyon Howort (2018), "Strategic Autonomy and EU-NATO Cooperation: Threat or Opportunity for Transatlantic Defence Relations?", *Journal of European Integration,* 40(5), ss. 523–534; Mason Clark (2026), "The Russian Military Campaign against Europe: Defining the Threat", Institute for the Study of War (ISW), 16.09.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://understandingwar.org/research/defense-of-europe/the-russian-military-campaign-against-europe-defining-the-threat. Avrupa Birliği'nin stratejik özerklik planı diğer taraftan Rusya'nın Avrupalı devletleri daha belirgin bir tehdit öznesi olarak görmesine neden olmuştur. Dolayısıyla, stratejik özerklik planının çok daha geniş yansımaları vardır. Ayrıntılı bilgi için bakınız; Dmitry Adamsky (2026), "How Russia Sees the World Now - the Kremlin's New Mental Map Is Changing the War in Ukraine—and the Confrontation with the West", *Foreign Affairs*, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/russia/how-russia-sees-world-now.

[41] Luuk Schmitz & Timo Seidl (2023), "As Open as Possible, as Autonomous as Necessary: Understanding the Rise of Open Strategic Autonomy in EU Trade Policy", *JCMS: Journal of Common Market Studies,* 61(3), ss. 836–849; Niklas Helwig & Ville Sinkkonen (2022), "Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term", *European Foreign Affairs Review*, 27(Special), ss. 3–19.

[42] Niklas Helwig (2023), "EU Strategic Autonomy after the Russian Invasion of Ukraine: Europe's Capacity to Act in Times of War", *Journal of Common Market Studies,* 61(1), ss. 57–62.

[43] Raluca Csernatoni (2022), "The EU's Hegemonic Imaginaries: From European Strategic Autonomy in Defence to Technological Sovereignty", *European Security*, 31(3), ss. 395–411.

[44] Julian Bergmann & Patrick Müller (2021), "Failing Forward in the EU's Common Security and Defense Policy: The Integration of EU Crisis Management", ss. 1669–1682; Avrupa Birliği Konseyi (2022), "Council Decision (CFSP) 2022/338 of 28 February 2022 on an Assistance Measure under the European Peace Facility for the Supply to the Ukrainian Armed Forces of Military Equipment, and Platforms, Designed to Deliver Lethal Force", Erişim Tarihi: 18.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2022/338/2023-04-13/eng; Katariina Mustasilta & Tyyne Karjalainen (2026), "European Strategic Cultures in Flux? Case Study on the European Peace Facility", *European Journal of International Security,* 11(4), ss. 600–622.

mülteciler konusundaki dayanışmasını, AB'nin uyumu ve kimliği çerçevesinde hak temelli normlardan kaynaklanan ahlaki bir yükümlülük duygusuyla açıklamak mümkündür.[45]

Versay Bildirgesi (10-11 Mart 2022) ve Stratejik Pusula (21 Mart 2022) savaşa karşı verilen tepkinin kurumsal yansımalarıdır.[46] Stratejik Pusula çerçevesinde, 5.000 askere ulaşabilen hızlı bir konuşlanma kapasitesine ulaşılması, hibrit tehditlere karşı önlemlerin alınması ve Rusya'nın Avrupa güvenliği açısından uzun vadeli ve doğrudan bir tehdit olduğu vurgulanmıştır.[47] Her ne kadar savaştan önce taslak metni hazırlanmış olsa da, Stratejik Pusula AB'nin güvenlik yaklaşımına dair ihtiyatlı bir iyimserliği ortaya çıkarmıştır.[48] Aynı dönemde Danimarka'nın savunma alanına yönelik muafiyetini referandumla sonlandırması, Finlandiya'nın (2023) ve İsveç'in (2024) NATO'ya katılması, Avrupa'nın güvenlik alanını kuzeye ve doğuya doğru yeniden tanımlamıştır.[49]

Bu dönemin en önemli değişimi AB'nin küresel rol algılarında görülmüştür.[50] Avrupa Konseyi sonuç bildirgelerinde ve Komisyon raporlarında, Ukrayna-Rusya Savaşı sonrasında Birliğin uzlaştırıcı/arabulucu rolünü terk ettiği ve normları koruma ile askeri güvenliği sağlama yönüne ağırlık verdiği belirtilmiştir.[51] Ancak bu duyurulara rağmen AB'nin tanımladığı rollerin neredeyse tamamı yine de askeri olmayan araçlara dayanmıştır. Dolayısıyla, AB sivil güç kimliğini terk etmeden, bu kimliğini güvenlik yönüyle yeniden uygulamaktadır.

3.2. Güvenlik Politikasının Yayılması: Enerji, Yaptırımlar ve Genişleme

[45] Giselle Bosse (2022), "Values, Rights, and Changing Interests: The EU's Response to the War against Ukraine and the Responsibility to Protect Europeans", *Contemporary Security Policy,* 43(3), ss. 531–541.
[46] Avrupa Konseyi (2022), "The Versailles Declaration, 10 and 11 March 2022", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2022/03/11/the-versailles-declaration-10-11032022/; Avrupa Birliği Konseyi (2022), "A Strategic Compass for Security and Defence", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.
[47] *A.g.e.*
[48] Simon Sweeney & Neil Winn (2022), "Understanding the Ambition in the EU's Strategic Compass: A Case for Optimism at Last?", *Defence Studies*, 22(2), ss. 192–206; Monika Sus (2024), "Exploring the Dynamics of Policy Change in EU Security and Defence: Policy Entrepreneurs Behind the Strategic Compass", *West European Politics*, 47*(*4), ss. 942–960.
[49] Mitchell A. Orenstein (2023), "The European Union's Transformation after Russia's Attack on Ukraine", ss. 333–340; NATO (2023), "Finland Joins NATO as 31st Ally", 04.04.2023, Erişim Tarihi: 18.10.2026, Erişim Adresi: https://www.nato.int/en/news-and-events/articles/news/2023/04/04/finland-joins-nato-as-31st-ally?selectedLocale=; NATO (2024), "Sweden Officially Joins NATO", 07.03.2024, Erişim Tarihi: 18.10.2026, Erişim Adresi: https://www.nato.int/en/news-and-events/articles/news/2024/03/07/sweden-officially-joins-nato.
[50] Mehmet Emir (2025), "Varoluşsal Tehdit Algısının Dinamik Güvenlikleştirmeye Dönüşümü: Ukrayna-Rusya Savaşında Aktör Stratejilerinin Analizi", *Politik Ekonomik Kuram*, 9(4), ss. 1698–1703; Oriol Costa & Esther Barbé (2023), "A Moving Target. Eu Actorness and the Russian Invasion of Ukraine", *Journal of European Integration*, 45(3), ss. 433–442.
[51] Gordon M. Friedrichs & Jule Sommer (2025), "Ontological Security Crisis and Role Conception Change: The Impact of the Russian Invasion of Ukraine on the European Union's Role Conceptions", ss. 129–145.

Ukrayna-Rusya Savaşı, güvenlik yaklaşımının OGSP'nin daha dar anlamlı sınırlarını aşarak AB'nin hemen hemen her alanına yayılmasına neden olmuştur. AB tarafından REPowerEU (2022 yılı Mayıs ayında) planı çerçevesinde Rusya'dan alınan enerji kaynaklarına bağımlılığın hızla azaltılması hedeflenmiş, ancak bu dönüşüm beraberinde farklı fosil yakıt tedariki ihtiyacını da getirmiştir.[52] Ayrıca bu yönelim, Birliğin yeşil dönüşüm hedefleriyle de tezat teşkil etmiştir.[53] Bu nedenle, AB'nin enerji politikaları, iklim ve piyasa odağından jeopolitik güvenlik alanına kaymıştır.

Avrupa Birliği tarafından 2026 Temmuz ayında 21. Yaptırım Paketi kabul edilmiştir.[54] Bu son yaptırım paketi enerji, kripto varlıklar sektörü ve finansal hizmetleri hedef almış ve 2022 yılından beri daha kapsamlı bireysel yaptırımları içermiştir.[55] Yaptırımlar yalnızca Rusya'yı kapsamamış, bununla beraber yaptırımların delinmesine neden olan üçüncü ülkeleri de hedeflemiştir. Bu durum karşısında yaptırım paketi, yalnızca bir cezalandırma mekanizması olmanın ötesinde, küresel düzeyde ekonomik güvenlik rejimini inşa etmiştir. Birliğin genişleme politikası da güvenlik mantığı çerçevesinde yeniden ele alınmıştır.[56] Bu bağlamda, Ukrayna ve Moldova'ya 2022 yılı Haziran ayında adaylık statüsünün verilmesi ve sonrasında katılım müzakerelerinin başlatılması, Birlik seviyesinde genişlemenin teknokratik koşullardan jeopolitik bir istikrar arayışına evrildiğini göstermektedir. Halen devam eden savaş, AB'nin

[52] Caroline Kuzemko & Mathieu Blondeel & Claire Dupont, & Marie Claire Brisbois (2022), "Russia's War on Ukraine, European Energy Policy Responses & Implications for Sustainable Transformations", *Energy Research & Social Science*, 93, ss. 1–7.

[53] Marco Siddi (2023), "Europe's Energy Dilemma: War and the Green Transition", *Current History,* 122(842), ss. 83–88; Andreas C. Goldthau & Richard Youngs (2023), "The EU Energy Crisis and a New Geopolitics of Climate Transition", *JCMS: Journal of Common Market Studies*, 61, ss. 115–122.

[54] Avrupa Birliği Konseyi (2026), "Council Regulation (EU) 2026/1844 of 23 July 2026 Amending Regulation (EU) No 269/2014 Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2026/1844/oj; Avrupa Birliği Konseyi (2026), "Council Decision (CFSP) 2026/1845 of 23 July 2026 Amending Decision 2014/145/Cfsp Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2026/1845/oj; Katharina Meissner & Chiara Graziani (2023), "The Transformation and Design of EU Restrictive Measures against Russia", *Journal of European Integration*, 45(3), ss. 379–391.

[55] Avrupa Birliği Konseyi (2026), "21st Package of Sanctions: EU Hits Russian Energy, Financial Services and Crypto Hard", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2026/07/23/21st-package-of-sanctions-eu-hits-russian-energy-financial-services-and-crypto-hard/.

[56] Veronica Anghel & Jelena Džankić (2023), "Wartime EU: Consequences of the Russia–Ukraine War on the Enlargement Process", *Journal of European Integration,* 45(3), ss. 487–497; Avrupa Konseyi (2023), "European Council Conclusions, 14 and 15 December 2023", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2023/12/15/european-council-conclusions-14-and-15-december-2023/; Avrupa Birliği Komisyonu (2024), "EU Opens Accession Negotiations with Ukraine", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://enlargement.ec.europa.eu/news/eu-opens-accession-negotiations-ukraine-2024-06-25_en; Nadiia Koval & Milada Anna Vachudova (2024), "European Union Enlargement and Geopolitical Power in the Face of War", *Journal of Common Market Studies,* 62, ss. 136–143; Tom Hunter & Natasha Wunsch & Marie-Eve Bélanger (2025), "A Geopolitical Turning Point? Enlargement Discourse after the Russian Invasion of Ukraine", *European Union Politics*, 26(4), ss. 690–710.

mevcut koşullarda iç sahasını korumaya, buna karşın güç gösterilmesi açısından dış sınırlarını daha katı bir şekilde savunmasına neden olabilir.[57]

Ukrayna-Rusya Savaşı, ayrıca AB'nin stratejik özerklik arayışının koruma, sürdürme ve koşullar çerçevesinde yansıtma boyutlarıyla ortak karar alma yeteneğinin sınandığı bir süreçtir.[58] Bu durum, 2022-2024 yılları arasında AB'nin rol gerekleri bağlamında belirli kalıpların kırıldığını, ancak yerlerine henüz kalıcı bir yapının inşa edilmediğini göstermektedir.[59]

4. Devam Eden Süreçte Kurumsallaşma: Savunma ve Sanayi Alanlarındaki İş Birliği ile Hazırlık 2030 (2024-2026)

4.1. Komisyonun Jeopolitik Seviyede Aktörlüğü ve SAFE

Ukrayna-Rusya Savaşı'nın üçüncü yılından itibaren AB'nin bu olaya tepkisi kriz yönetiminden kalıcı bir kurumsallaşmaya doğru değişmiştir. Bu bağlamda, Komisyon, AB'nin savunma alanındaki zayıflığının da etkisiyle yetkisini genişleterek Birliğin bütünleşmesi için savaşın seyrini stratejik bir çerçevede değerlendirmiştir.[60] AB'nin savunma ve güvenlik alanındaki dönüşümü için 2023 yılında Mühimmat Üretimini Destekleme Yasası (ASAP) ve ortak tedarik aracı (EDIRPA) ile birlikte, 2024 yılı Mart ayında ilk kez Avrupa Savunma Sanayi Stratejisi (EDIS) yayımlanmıştır.[61] EDIS çerçevesinde 2030 yılına kadar savunma teçhizatının en az yüzde 40'ının ortak tedarik usulüyle temin edilmesi ve tedarik bütçesinin en az yüzde 50'sinin Avrupa savunma sanayisi için harcanması hedeflenmiştir.[62] Bu hedefler doğrultusunda, 2024

[57] Mitchell A. Orenstein (2023), "The European Union's Transformation after Russia's Attack on Ukraine", ss. 339–340.
[58] Niklas Helwig (2023), "EU Strategic Autonomy after the Russian Invasion of Ukraine: Europe's Capacity to Act in Times of War", ss. 58–65.
[59] Christian Freudlsperger & Frank Schimmelfennig (2023), "Rebordering Europe in the Ukraine War: Community Building without Capacity Building", *West European Politics,* 46(5), ss. 843–866.
[60] Calle Håkansson (2024), "The Ukraine War and the Emergence of the European Commission as a Geopolitical Actor", ss. 25–39.
[61] Jan Joel Andersson & Malena Britz (2025), "The European Union's Role in European Defence Industry Policy", *Defence Studies*, 25(2), ss. 322–338; Avrupa Birliği Parlamentosu & Konseyi (2023), "Regulation (EU) 2023/1525 of the European Parliament and of the Council of 20 July 2023 on Supporting Ammunition Production (ASAP)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2023/1525/oj; Avrupa Birliği Parlamentosu & Konseyi (2023), "Regulation (EU) 2023/2418 of the European Parliament and of the Council of 18 October 2023 on Establishing an Instrument for the Reinforcement of the European Defence Industry through Common Procurement (EDIRPA)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2023/2418/oj; Avrupa Birliği Parlamentosu & Konseyi (2025), "Regulation (EU) 2025/2643 of the European Parliament and of the Council of 16 December 2025 Establishing the European Defence Industry Programme and a Framework of Measures to Ensure the Timely Availability and Supply of Defence Products ('EDIP Regulation') (Text with EEA Relevance)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2025/2643/oj.
[62] Avrupa Birliği Komisyonu & Yüksek Temsilcilik (2024), "A New European Defence Industrial Strategy: Achieving EU Readiness through a Responsive and Resilient European Defence Industry (Join(2024) 10 Final)",

yılı Aralık ayında Komisyon'da ilk kez Savunma ve Uzay Komiserinin görev alması dikkat çekicidir.[63]

AB'nin güvenlik ve savunma dönüşümünün bir diğer önemli safhası 2025 yılında ABD'de gerçekleşen görev değişimidir. 2025 yılı Mart ayında açıklanan Avrupa Savunması Beyaz Kitabı ve ReArm Europe/Hazırlık 2030 planı, AB üye devletlerinin savunma harcamalarına 800 milyar avro yatırım potansiyelini öngörmektedir.[64] Bu planın ilk safhası olan SAFE, 27 Mayıs 2025 tarihinde kabul edilmiş ve AB üyesi devletler için ortak savunma tedariklerine yönelik olarak 150 milyar avroya kadar uzun vadeli kredi olanağı sunulmuştur.[65] SAFE için 19 üye devlet başvururken, Konsey tarafından 11 Şubat – 10 Nisan 2026 tarihleri arasında yapılan değerlendirme sonucunda 18 üye devletin savunma yatırım planı onaylanmıştır. Sunulan savunma yatırım planlarından 15'i Ukrayna ile ortak projeleri içermektedir.[66] SAFE, savunma planı için en az iki ülkeyi kapsayan ortak tedarik koşulu, tedarik maliyetinin en az yüzde 65'inin AB, Avrupa Ekonomik Alanı/EFTA veya Ukrayna menşeli olması şartı ve üçüncü ülkelerin katılımını da ikili antlaşmalara bağlayan yapısıyla özellikle Avrupa'yı tercih eden bir mekanizma kurmuştur.[67]

AB'nin bu dönüşümünde en özgün finansman yeniliği Ukrayna'nın desteklenmesidir.[68] Rusya'ya ait finansal varlıkların tazminat kredisi olarak Ukrayna'ya aktarılması önerisi, bu varlıkların büyük bir bölümünün bulunduğu Belçika tarafından hukuki gerekçelerle riskli bulunmuş ve bu plan uygulanamamıştır.[69] Bu planın yerine Avrupa Konseyi tarafından 18-19

Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024JC0010.

[63] Avrupa Birliği Komisyonu (2026), "Andrius Kubilius, Commissioner (2024-2029), Defence and Space", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://commission.europa.eu/about/organisation/college-commissioners/andrius-kubilius_en.

[64] Avrupa Birliği Komisyonu & Yüksek Temsilcilik (2025), "Joint White Paper for European Defence Readiness 2030 - Join(2025) 120 Final", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0120, ss. 16–17. Beyaz Kitap'ta bu projeksiyon kademeli bir kullanım olarak varsayılmıştır. Dolayısıyla, ek finansman/mali alan tahmini olarak değerlendirilmelidir.

[65] Avrupa Birliği Konseyi (2025), "SAFE: Council Adopts €150 Billion Boost for Joint Procurement on European Security and Defence", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2025/05/27/safe-council-adopts-150-billion-boost-for-joint-procurement-on-european-security-and-defence/pdf.

[66] Avrupa Birliği Konseyi (2026), "What Is Security Action for Europe (Safe)?", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/safe/.

[67] Avrupa Birliği Konseyi (2025), "Establishing the Security Action for Europe (SAFE) through the Reinforcement of the European Defence Industry Instrument", Erişim Tarihi: 18.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2025/1106/oj/eng.

[68] Eric Ciaramella (2026), "Ukraine Can Turn Imminent Peril to Its Advantage - How a True "Energy Cease-Fire" Can Curb Putin", *Foreign Affairs*, 15.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/ukraine/ukraine-can-turn-imminent-peril-its-advantage.

[69] Dmytro Kuleba (2026), "Russia's Plan to Break Ukraine - What Kyiv Needs to Survive", *Foreign Affairs*, 30.09.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/united-states/russias-plan-break-ukraine-dmytro-kuleba.

Aralık 2025 tarihinde AB'nin sermaye piyasalarından borçlanmasına dayanan 90 milyar avroluk bir destek kredisi üzerinde anlaşmaya varılmıştır.[70] Güçlendirilmiş iş birliği prosedürüyle 24 üye ülkenin katılımıyla sağlanan bu kredi desteğinin 60 milyar avroluk kısmı Ukrayna'nın savunma sanayi kapasitesinin geliştirilmesi ve askeri teçhizat tedarikinin sağlanmasına tahsis edilmiştir. Kredinin geri ödemesi ise Rusya'nın savaş tazminatı ödemesine bağlanmıştır. AB'nin Ukrayna'ya sağladığı toplam destek 231,5 milyar avroya ulaşmıştır.[71]

Ukrayna'ya sağlanan bu destek, piyasa ile savaş arasındaki ilişkiye yeni bir boyut kazandırmıştır.[72] Ukrayna-Rusya Savaşı, AB'nin tarihinde eksik kalan dış tehdit baskısını ortaya koymuştur. Bu bağlamda, dış tehdit baskısı, AB Antlaşması'nın savunma odağından (AB Antlaşması madde 42) değil, sanayi (AB'nin İşleyişi Hakkında Antlaşma (ABİHA) madde 173) ve ekonomik acil durum (ABİHA madde 122) hükümleri çerçevesinde gerçekleşmektedir. Diğer bir ifadeyle, AB savunma alanındaki devlet kapasitelerini, yani sanayi planlaması, tedarik koordinasyonu ve ortak borçlanma gereksinimlerini, piyasa gücü sayesinde sağlamaktadır. Piyasa yoluyla güvenliğin sağlanması, bir nevi hibrit bir devletleşme yapısını ortaya çıkarmaktadır. Birlik, önlem almaya zorlayıcı gücün kendisini değil, zorlayıcı gücün maddi altyapısına odaklanmıştır. Hükümetler, uluslarüstü kurumlar, şirketler ve finansal kaynakların çok düzeyli ve görüşmeye açık ilişkileri bir nevi karmaşık ve birbirine bağlı politik ekonomi boyutunun hibritliğini yansıtmaktadır.[73]

4.2. Savunma Harcamalarındaki Artışlar ve Niteliksel Sınırlar

Avrupa Birliği dönüşümünün en görünür göstergesi savunma harcamalarındaki artıştır. 2021 yılında AB üyesi devletlerin toplam savunma harcaması 214 milyar avroyken, bu harcama 2024 yılında 343 milyar avroya ve 2025 yılında ise 418 milyar avroya yükselmiştir. Savunma harcamaları Birlik toplam GSYİH'nin yüzde 2,2'sine karşılık gelmiş ve 2026 yılı için 454 milyar avro (yüzde 2,4) olarak öngörülmüştür. 2025 yılında Birlik üyesi 23 devlet,

[70] Avrupa Birliği Parlamentosu & Konseyi (2026), "AP ve Konsey Tüzüğü (AB) 2026/467", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://lawplayer.com/eu/act/32026R0467.

[71] Avrupa Birliği Konseyi (2026), "EU Financial Assistance to Ukraine", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/ukraine-solidarity-financial-support/. Bu destek, bilgiye erişim tarihi itibariyle yapılan yardımı ifade etmektedir. Gelecek zaman serisinde destek miktarının da değişeceği hesaba katılmalıdır.

[72] R. Daniel Kelemen & Kathleen R. McNamara (2022), "State-Building and the European Union: Markets, War, and Europe's Uneven Political Development", ss. 963–984; Kathleen R. McNamara (2024), "Transforming Europe? The EU's Industrial Policy and Geopolitical Turn", ss. 2371–2389; Philipp Genschel (2022), "Bellicist Integration? The War in Ukraine, the European Union and Core State Powers", ss. 1885–1898.

[73] Nicholas Marsh & Bruno Oliveira Martins & Jocelyn Mawdsley (2026), "The European Iron Network: The Remaking of the Political Economy of European Defence Production Following the Ukraine War", *Journal of European Integration,* 48*(*5), ss. 835–851; Kaija Schild (2023), "Weaponising Europe? Rule-Makers and Rule-Takers in the EU Regulatory Security State", *Journal of European Public Policy,* 30(7), ss. 1255–1272.

GSYİH'lerinin en az yüzde 2'sini savunma harcamalarına ayırmıştır. Mevcut harcamaların seyrine göre 2029 yılında Birlik savunma harcamalarının 547 milyar avroya ulaşacağı tahmin edilmektedir.[74]

Savunma harcamalarındaki artış aynı zamanda niteliksel bütünleşmeyi de beraberinde getirmemektedir. 2025 yılında askeri teçhizat ihtiyaçlarının yalnızca yüzde 24'ü ortak tedarikle karşılanmıştır.[75] Bu oran ASK'nın yüzde 35'lik ortak tedarik ölçütünün ve EDIS'in 2030 yılına kadar belirlediği yüzde 40'lık hedefin gerisindedir.[76] Bu çerçevede araştırma-geliştirme harcamaları için 17 milyar avro harcanmış olsa da bu tutar, toplam savunma harcamasının yalnızca yüzde 4'ünü oluşturmaktadır.[77] Bu görünüm, ulusal algı, inanç ve hedeflerdeki farklılıkların Birlik savunma bütünleşmesi için hâlâ yeterince uyum sağlamadığını göstermektedir.[78] Dolayısıyla, savunma harcamaları kapsamında AB bütünleşmesinde sınırlı ve hedefin gerisinde bir ilerleme olduğu görülmektedir.

5. AB'nin Siber Güvenlik Dönüşümü: Düzenleyici Aktörden Jeopolitik Siber Egemenliğe[79]

5.1. Savaş Öncesi Yaklaşım ve Savaşın Siber Boyutu

Avrupa Birliği'nin siber güvenlik politikası, öncelikle iç pazarı korumaya dönük bir ekonomi odağından doğmuş; ancak zamanla güvenlik söylemiyle daha sık anılmaya başlamıştır.[80]

[74] Avrupa Savunma Kurumu (2026), "EU Defence Spending: €418 Billion in 2025, Projected to €454 Billion in 2026", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eda.europa.eu/news-and-events/news/2026/07/16/eu-defence-spending---418-billion-in-2025--projected-to--454-billion-in-2026.

[75] Juan Carlos De la Tore (2026), "Europe's Defence Spending Is Surging, but Fragmented Procurement Is Holding Industry Back", Digitalshield, 19.10.2026, Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.escudodigital.com/en/defense/europe/europes-defence-spending-is-surging-but-fragmented-procurement-is-holding-industry-back.html.

[76] Avrupa Birliği (2024), "Edis - European Defence Industrial Strategy", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://defence-industry-space.ec.europa.eu/document/download/333faee1-a851-44a6-965b-713247515d39_en?filename=DEFIS_EDIS_factsheet.pdf; Linda Tothova & Sebastian Clapp (2026), "EU Joint Defence Procurement", EPThinktank, Erişim Tarihi: 24.10.2026, Erişim Adresi: https://epthinktank.eu/2026/03/13/eu-joint-defence-procurement/.

[77] Avrupa Savunma Kurumu (2026), "EU Defence Spending: €418 Billion in 2025, Projected to €454 Billion in 2026", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eda.europa.eu/news-and-events/news/2026/07/16/eu-defence-spending---418-billion-in-2025--projected-to--454-billion-in-2026.

[78] Eva Michaels & Monika Sus (2024), "(Not) Coming of Age? Unpacking the European Union's Quest for Strategic Autonomy in Security and Defence", *European Security,* 33(3), ss. 383–396.

[79] Siber egemenlik kavramı, dijital egemenliği ve teknolojik egemenliği kapsayan bir kavram olarak belirtilmiştir. Ayrıntılı okuma için bakınız; Rocco Bellanova & Helena Carrapico & Denis Duez (2022), "Digital/Sovereignty and European Security Integration: An Introduction", *European Security*, 31(3), ss. 337–351.

[80] Helena Carrapico & Benjamin Farrand (2020), "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy", *Journal of European Integration,* 42(8), ss. 1111–1123; Avrupa Birliği Parlamentosu & Konseyi (2020), "Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018.

AB'nin bu konudaki kurumsal atılımları sırasıyla Siber Güvenlik Stratejisi (2013), Ağ ve Bilgi Sistemleri Güvenliği (NIS) Direktifi (2016), Siber Diplomasi Paketi (2017) ve Siber Güvenlik Yasası'na (2019) dayanmaktadır.[81] Bu atılımlar sayesinde siber alan AB'nin kolektif güvenlikleştirme konusu olurken[82], diğer taraftan bu politikanın uygulanmasında Birlik seviyesinde farklılıklar ve uyumsuzluklar görülmüştür.[83] Buna karşın, AB'nin siber güvenlik politikasının düzenleyici kapitalizmden düzenleyici merkantilizme dönüştüğü de savunulmuştur.[84]

Ukrayna-Rusya Savaşı, AB'nin siber dönüşüm sürecini hızlandırmıştır. 24 Şubat 2022'de başlayan savaşın ardından Viasat şirketine ait KA-SAT uydu ağının siber saldırıya uğraması sonucu Ukrayna'nın yanı sıra birçok AB üyesi devletin vatandaşları da bu durumdan etkilenmiştir. AB, kurumsal olarak ve üye ülkeler nezdinde bu saldırıyı Rusya'ya atfetmiştir.[85] Savaşta siber güvenlik bir yönüyle önemli, ancak belirleyici olmayan bir unsur olarak görülürken[86], diğer taraftan siber güvenliğin sınırları hız, yoğunluk ve kontrol seviyesine bağlı olarak olumsuz etkilere yol açabilir.[87] Rusya'nın siber saldırıları neticesinde AB'nin kurumsal yapısı ve üye devletlerin politikaları, stratejik amaçları doğrultusunda yoğunlaştırılmış; bu bağlamda siber diplomasi daha etkin kullanılmış, bunun yanı sıra özel aktörlerle daha yakın

[81] Avrupa Birliği Parlamentosu & Konseyi (2013), "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001; Avrupa Birliği Parlamentosu & Konseyi (2016), "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dir/2016/1148/oj; Avrupa Birliği Konseyi (2017), "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf; Avrupa Birliği Parlamentosu & Konseyi (2019), "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA Relevance)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[82] George Christou (2019), "The Collective Securitisation of Cyberspace in the European Union", *West European Politics*, 42(2), ss. 278–295.

[83] Helena Carrapico & André Barrinha (2017), "The EU as a Coherent (Cyber) Security Actor?", *JCMS: Journal of Common Market Studies*, 55(6), ss. 1254–1268.

[84] Benjamin Farrand & Helena Carrapico (2022), "Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity", *European Security,* 31(3), ss. ss. 435–450.

[85] Avrupa Birliği Konseyi (2022), "Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

[86] Marcus Willett (2022), "The Cyber Dimension of the Russia–Ukraine War", *Survival,* 64(5), ss. 7–24; Nadiya Kostyuk & Erik Gartzke (2022), "Why Cyber Dogs Have yet to Bark Loudly in Russia's Invasion of Ukraine", *Texas National Security Review,* 5(3), ss. 114–123.

[87] Lennart Maschmeyer (2021), "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations", *International Security,* 46(2), ss. 51–90.

koordinasyon kurularak yasal çerçeveler içinde azami işlevsellik sağlanmıştır.[88] Böylece, savaşın siber boyutu cephedeki etkisinin yanı sıra Avrupa toplumlarının dayanma sınırlarını ölçen bir hibrit saldırı yöntemi olarak daha görünür olmuştur.[89]

5.2. Hibrit Tehditler, Kritik Altyapının ve Tedarik Zincirlerinin Güvenlikleştirilmesi

Ukrayna-Rusya Savaşı sürecinde AB'nin siber güvenlik mevzuatı hem kapsam, hem de nitelik açısından genişletilmiştir. Bu bağlamda birtakım önemli adımlar atılmıştır. 2022 yılı Aralık ayında kabul edilen NIS2 Direktifinin (Directive (EU) 2022/2555) kapsamı genişletilmiş ve kritik sektörlerin yönetim organları doğrudan sorumlu tutulmuştur.[90] 2024 yılında Siber Dayanıklılık Yasası (Regulation (EU) 2024/2847) çerçevesinde dijital ürünlerin tasarımından itibaren güvenlik sağlama yükümlülüğü getirilmiştir.[91] 2025 yılında yürürlüğe giren Siber Dayanışma Yasası (Regulation (EU) 2025/38) kapsamında ortak uyarı altyapısı, acil durum mekanizması ve AB siber güvenlik rezervi gibi operasyonel seçenekler oluşturulmuştur.[92] AB'nin siber ve fiziki altyapı güvenliğini tehdit edebilecek risklere karşı hibrit bir yaklaşım benimsenmiş[93] ve bu bağlamda 2024 yılı Ekim ayında kabul edilen yaptırım çerçevesi uygulanmıştır.[94]

---

[88] Nicolò Fasola & Sonia Lucarelli & Francesco Niccolò Moro (2025), "Cyber Diplomacy and the Russia–Ukraine War", *The Hague Journal of Diplomacy*, 20*(*4), ss. 749–764; Nadiya Kostyuk & Aaron Brantly (2022), "War in the Borderland through Cyberspace: Limits of Defending Ukraine through Interstate Cooperation", *Contemporary Security Policy,* 43(3), ss. 498–510.

[89] Mikael Wigell (2021), "Democratic Deterrence: How to Dissuade Hybrid Interference", *The Washington Quarterly*, 44(1), ss. 49–64.

[90] Avrupa Birliği Parlamentosu & Konseyi (2022), "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (Nis 2 Directive) (Text with Eea Relevance)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[91] Avrupa Birliği Parlamentosu & Konseyi (2024), "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA Relevance)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2024/2847/oj.

[92] Avrupa Birliği Parlamentosu & Konseyi (2025), "Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 Laying down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cyber Threats and Incidents and Amending Regulation (EU) 2021/694 (Cyber Solidarity Act)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2025/38/oj.

[93] Christian Bueger & Tobias Liebetrau (2023). "Critical Maritime Infrastructure Protection: What's the Trouble?", *Marine Policy*, 155, ss. 1–6; Avrupa Birliği Parlamentosu & Konseyi (2022), "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC (Text with EEA Relevance)", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dir/2022/2557/oj.

[94] Avrupa Birliği Konseyi (2024), "Hybrid Threats: Council Paves the Way for Deploying Hybrid Rapid Response Teams", Erişim Tarihi: 17.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/; Avrupa

Siber güvenliğe dair en dikkat çekici adım Komisyon'un 20 Ocak 2026 tarihinde sunduğu Siber Güvenlik Yasası revizyon önerisidir.[95] Bu öneri çerçevesinde, Komisyon'a teknik ve yapısal riskler taşıyan üçüncü ülkelerin siber güvenlik boyutuyla kaygı uyandıran aktörler olarak tanımlanması, teknik ve diğer kriterler bağlamında yüksek riskli tedarikçi listelerinin oluşturulması ve 18 kritik sektörde temel bilgi ve iletişim teknolojisi (BİT) varlıklarını tanımlama yetkisi verilmesi öngörülmüştür. Ayrıca yüksek riskli tedarikçilerin kademeli olarak önemli ağ işlevlerinden çıkarılması da planlanmıştır. Dolayısıyla, AB'nin siber güvenlik hukuku teknik açıdan tarafsızlık mantığından dost ve düşman ayrımını yapan bir jeopolitik kodlama mantığına dönüşmüştür.[96] Diğer bir ifadeyle, düzenleyici merkantilizm eğilimi[97] kavramından hareketle savaş koşullarında düzenleyici güvenlikleştirmeye evrilmektedir.

Avrupa Birliği'nin siber ve teknoloji dönüşümü yalnızca düşmanlık üzerinden değil müttefiklere karşı da tanımlanmıştır. ABD'nin Ulusal Güvenlik Stratejisi'ne (2025) göre AB'nin sıkı düzenleyici yaklaşımı ve politika yönelimi sert bir şekilde eleştirilmiştir.[98] AB'nin bulut altyapısı ve yapay zekâ konularında ABD'ye olan bağımlılığı ise dijital egemenlik tartışmalarında transatlantik ilişkilerin gerilmesine yol açmıştır. AB'nin siber ve teknolojik egemenlik motivasyonu yalnızca Rusya ve Çin'e karşı değil bunun yanı sıra kuşku duyulan müttefiklere karşı da dönüşen bir strateji olmuştur.[99]

Birliği Konseyi (2024), "Council Decision (CFSP) 2024/2643 of 8 October 2024 Concerning Restrictive Measures in View of Russia's Destabilising Activities", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2024/2643/2025-05-22/eng; Avrupa Birliği Konseyi (2024), "Council Regulation (EU) 2024/2642 of 8 October 2024 Concerning Restrictive Measures in View of Russia's Destabilizing Activities", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2024/2642/oj.

[95] Avrupa Birliği Komisyonu (2026), "Proposal for a Regulation on Enisa, the European Cybersecurity Certification Framework, and Ict Supply Chain Security and Repealing Regulation (Eu) 2019/881 (Com(2026) 11 Final)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0011.

[96] Tero Poutala & Elina Sinkkonen & Mikael Mattlin (2022), "EU Strategic Autonomy and the Perceived Challenge of China: Can Critical Hubs Be De-Weaponized?", *European Foreign Affairs Review*, 27(Special), ss. 79–97.

[97] Benjamin Farrand & Helena Carrapico (2022), "Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity", ss. 435–450.

[98] The White House (2025), "National Security Strategy of the United States of America", Erişim Tarihi: 30.09.2026, Erişim Adresi: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf, ss. 25–27.

[99] Raluca Csernatoni (2022), "The EU's Hegemonic Imaginaries: From European Strategic Autonomy in Defence to Technological Sovereignty", ss. 395–411; Dennis Broeders & Fabio Cristiano & Monica Kaminska (2023), "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions", *JCMS: Journal of Common Market Studies,* 61(5), ss. 1263–1274; Avrupa Birliği Parlamentosu & Konseyi (2023), "Joint Communication to the European Parliament, the European Council and the Council on European Economic Security Strategy", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0020; Linda Monsees & Daniel Lambach (2022), "Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity", *European Security,* 31(3), ss. 379–389.

6. Dost ve Düşman Algısının Yeniden Tanımlanması

6.1. Rusya: Belirsiz Ortaklıktan Tehdit Öznesine Dönüşüm

Ukrayna-Rusya Savaşı'nın AB için algısal boyutuyla en önemli sonucu, Rusya'nın belirsiz bir ortaktan düşman konumuna dönüştürülmesidir. Stratejik Pusula'da Rusya uzun vadede ve doğrudan bir tehdit olarak tanımlanırken, 2025 yılındaki Beyaz Kitap'ta Rusya'nın öngörülebilir gelecekte Avrupa güvenliği için temel bir tehdit unsuru olarak kalacağı vurgulanmıştır.[100] Ontolojik güvenlik bağlamında bu dönüşüm AB'nin Rusya'ya karşı uzlaştırıcı/arabulucu rolünün başarıya ulaşmaması sonucunda yeniden tanımlanmış ve daha keskin bir politika olarak görülmüştür.[101] AB, yeni rol tanımlamasında barışı sağlama misyonunu ve normatif güç olma pozisyonunu korurken, bununla beraber Birliğin jeopolitik odaklanmasını da güçlü bir şekilde vurgulamıştır.[102]

Düşman imgesinin görünürlüğü yalnızca elitlerin söylemleriyle sınırlı kalmamıştır. AB üyesi 24 devlette ve İngiltere'de 40 bini aşan katılımcıyla yapılan araştırmada, güvenlik ve savunma alanında dış tehdit algısının bütünleşmeye daha olumlu yansıdığı ve Avrupa yanlıları kadar Avrupa şüphecileri arasında da güçlü bir destek gördüğü tespit edilmiştir.[103] Savaşın başlamasından beş hafta sonra 16 ülkeden toplanan veriler sonucunda, tehdit algısının Avrupa kimliğinin benimsenmesini pozitif yönde etkilediği; özellikle Orta ve Doğu Avrupa'daki dışlayıcı milliyetçiler arasında bunun daha belirgin olduğu ve nihayetinde bu bağın ortak Avrupa Ordusu'na güçlü bir destek olarak yansıdığı görülmüştür.[104] Bu tespitler, üye ülkeler arasında AB'nin zayıf yanlarının algısal etkisinin tehdit karşısında güvenilen bir sığınağa

[100] Avrupa Birliği Komisyonu & Yüksek Temsilcilik (2025), "Joint White Paper for European Defence Readiness 2030 - Join(2025) 120 Final", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0120, s. 2.
[101] Gordon M. Friedrichs & Jule Sommer (2025), "Ontological Security Crisis and Role Conception Change: The Impact of the Russian Invasion of Ukraine on the European Union's Role Conceptions", s. 148.
[102] Kateryna Pishchikova (2025), "European Identity Construction after the Russian Full-Scale Invasion of Ukraine: Dialogic (Re)Construction of Self and Others", ss. 1571–1586.
[103] Matthias Mader & Konstantin Gavras & Stephanie C. Hofmann & Jason Reifler & Harald Schoen & Catarina Thomson (2024), "International Threats and Support for European Security and Defence Integration: Evidence from 25 Countries", *European Journal of Political Research,* 63(2), ss. 433–450. Bu araştırma, 2020 yılı Ekim ayında yapılmıştır. Malta, Güney Kıbrıs Rum Yönetimi ve Lüksemburg dahil edilmemiştir.
[104] Julia Schulte-Cloos & Lenka Dražanová (2026), "Shelter from the Storm: External Threat, Social Identity, and Support for the EU", *European Union Politics,* 27(3), ss. 444–462.

dönüştüğünü ortaya koymaktadır.[105] Rusya'nın düşman olarak görülmesi post-fonksiyonalist teorinin kimlik temelli çekincelerini[106] en azından güvenlik boyutuyla gevşetmiştir.[107]

6.2. ABD: Güvenilir Müttefikten Belirsizlik Kaynağına Dönüşen Aktör

Ukrayna-Rusya Savaşı'nın ilk yılında ABD'nin Avrupa'daki caydırıcılık yönündeki ağırlığını arttırması ve Ukrayna'ya kritik askeri istihbarat ile lojistik destek sağlaması, Birliğin stratejik özerklik planını geçici olarak geri plana itmiştir.[108] Trump yönetiminin ikinci döneminin başlangıcı, transatlantik ilişkiler açısından önemli bir dönüm noktası olmuştur.[109] Washington yönetimi ABD ve Avrupa arasında çıkarların ve değerlerin ayrışmaya başladığını ve ülkenin Avrupa'ya yönelik güvenlik vaatlerinin küresel güç projeksiyonları çerçevesinde sorun teşkil ettiğini duyurmuştur.[110] 2025 yılı Aralık ayında yayımlanan ABD Ulusal Güvenlik Stratejisi, Avrupa'nın ekonomik durgunluktan daha fazla medeniyetinin silinmesi etkisiyle karşı karşıya kaldığı, bazı Avrupalı aktörlerin güvenilir müttefik olup olmadığının sorgulandığı ve dikkat çekici bir bakış açısı olarak Rusya'nın hasımdan çok Avrupa ile farklılıkları bulunan ve istikrar için bu sorunların giderilmesi gereken bir aktör olarak tanımlandığı bir belgedir.[111] Grönland krizi (2026) ise, aktörler arasındaki belirsizliği doruk noktasına taşımıştır. ABD'nin Grönland talebinin yanı sıra, bu talebini 8 Avrupa ülkesine yönelik gümrük tarifesi tehdidiyle desteklemesine karşı, AB yeniden ve daha ciddi bir biçimde müttefik ülke hakkında zorlamaya karşı koruma aracını (*anti-coercion instrument*) uygulamayı tartışmıştır.[112]

---

[105] Nils D. Steiner & Ruxanda Berlinschi & Etienne Farvaque & Jan Fidrmuc & Philipp Harms & Alexander Mihailov & Michael Neugart & Piotr Stanek (2023). "Rallying around the EU Flag: Russia's Invasion of Ukraine and Attitudes toward European Integration", *JCMS: Journal of Common Market Studies*, 61(2), ss. 283–299.
[106] Liesbet Hooghe & Gary Marks (2009), "A Postfunctionalist Theory of European Integration: From Permissive Consensus to Constraining Dissensus", *British Journal of Political Science,* 39(1), ss. 1–23.
[107] Zbigniew Truchlewski & Ioana-Elena Oana & Alexandru D. Moise (2023), "A Missing Link? Maintaining Support for the European Polity after the Russian Invasion of Ukraine", *Journal of European Public Policy*, 30(8), ss. 1662–1676. Avrupa Birliği içinde Rusya'ya yönelik olarak diplomasinin halen önemli bir sorun çözme aracı olarak gören aktörler de vardır. Bu bağlamda ayrıntılı bilgi için bakınız: Alexander Gabuev (2026), "How Europe Can Get Putin's Attention - the Continent Must Overcome Its Russia Predicament", *Foreign Affairs*, 07.07.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/russia/how-europe-can-get-putins-attention.
[108] Niklas Helwig (2023), "EU Strategic Autonomy after the Russian Invasion of Ukraine: Europe's Capacity to Act in Times of War", ss. 57–65.
[109] Justin Logan & Jennifer Kavanagh (2026), "Leave Europe to the Europeans", CATO Institute, 28.08.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.cato.org/commentary/leave-europe-europeans.
[110] Léonie Allard & Rachel Rizzo (2025), "Transatlantic Security in a New Era", ss. 85–93; Sarah Bauerle Danzman & Sophie Meunier (2024), "The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator", *JCMS: Journal of Common Market Studies*, 62(4), ss. 1098–1112.
[111] The White House (2025), "National Security Strategy of the United States of America", Erişim Tarihi: 30.09.2026, Erişim Adresi: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.
[112] Council on Foreign Relation (2026), "Trump Will Attend Davos Talks on Greenland", 20.01.2026, Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.cfr.org/articles/trump-will-attend-davos-talks-on-greenland; Christian Freudlsperger & Sophie Meunier (2024), "When Foreign Policy Becomes Trade Policy: The EU's Anti-

Aktörler arasındaki bu gerilim ittifak içi güvenlik ikileminin görünürlüğünü doğrulamıştır.[113] İttifak üyeleri müttefikleri tarafından terk edilmek ile müttefiklerinin çatışmalarına sürüklenme korkusuna dair ihtiyatlı bir kaygıyı daima hissederler. Soğuk Savaş sonrasında, özellikle 2003 yılındaki Irak Savaşı'nda Batı Avrupalı aktörlerin en belirgin kaygıları ABD'nin yanında çatışmalara sürüklenmekti; bu durum, 2025 yılında terk edilme korkusuyla daha belirgin hale gelmiştir. Ancak AB nükleer caydırıcılık, stratejik lojistik hatlarının kurulması ve işlerliği, uzun menzilli vuruş yeteneği ve güçlü istihbarat konularında ABD'nin yerini dolduracak kapasitede değildir.[114] Dolayısıyla, büyük bir sorun ortaya çıkmıştır: AB'nin askerî açıdan ABD'ye en çok ihtiyaç duyduğu dönem, politik olarak ABD'ye en az güvendiği dönemle çakışmıştır.[115] AB'nin stratejik özerklik planındaki AB-NATO ortaklığının tesis edilmesi aynı zamanda ABD'nin de Avrupa'yı eşit bir ortak olarak görme yaklaşımıyla gerçekleşebilir.[116]

AB ve ABD arasındaki sorunların en görünür kısmı nükleer alana yöneliktir. Ukrayna-Rusya Savaşı, AB'nin nükleer silah tartışmalarını daha güçlü bir şekilde ele almasına neden olmuştur.[117] 2 Mart 2026 tarihinde Fransa Cumhurbaşkanı Emmanuel Macron tarafından

---

Coercion Instrument", *JCMS: Journal of Common Market Studies,* 62(4, ss. 1063–1076; Avrupa Birliği Parlamentosu & Konseyi (2023), "Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the Protection of the Union and Its Member States from Economic Coercion by Third Countries", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2023/2675/oj.

[113] Glenn H. Snyder (1984), "The Security Dilemma in Alliance Politics", *World Politics,* 36(4), ss. 461–495; Marianne Riddervold & Akasemi Newsome (2022), "Introduction: Out with the Old, in with the New? Explaining Changing EU–US Relations", *Politics and Governance,* 10(2), ss. 128–132.

[114] Hugo Meijer & Stephen G. Brooks (2021), "Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back", *International Security,* 45(4), ss. 7–43; Claas Mertens & Ngaire Woods (2026), "Europe's Credibility Gap - Dependence on America Has Left It with Little to Offer Would-Be Partners", *Foreign Affairs*, 19.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/europe/europes-credibility-gap; Benjamin Giltner (2026), "Europe's Nuclear Shortcut Would Be a Strategic Mistake", CATO Institute, 31.03.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.cato.org/commentary/europes-nuclear-shortcut-would-be-strategic-mistake. ABD'nin nükleer caydırıcılık kapasitesindeki hakimiyeti için bakınız; Eric S. Edelman & Franklin C. Miller & Yonatan Touval & Janice Gross Stein & Rose Gottemoeller (2026), "Who Needs the Bomb? The Purpose of Nuclear Deterrence", *Foreign Affairs*, 20.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/responses/who-needs-bomb-edelman-miller-touval-stein.

[115] Judah Grunstein (2026), "Rubio's Vision of Western Primacy Is Just Empire by Another Name", *World Politics Review*, 16.10.2026, Erişim Tarihi: 19.10.2026, Erişim Adresi: https://www.worldpoliticsreview.com/rubio-athens-western-civilization/; Jolyon Howorth (2025), "European Defence and NATO: From Competition to Co-Operation to Replacement?", *Journal of Common Market Studies*, 63, ss. 156–164; Doug Bandow (2026), "An Independent Europe Means No More U.S. Rooster in the Henhous", CATO Institute, 19.08.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.cato.org/commentary/independent-europe-means-no-more-us-rooster-henhous.

[116] Nele Marianne Ewers-Peters (2025), "EU-NATO Cooperation Reloaded: The Impact of European Strategic Autonomy", *Defence Studies*, 25(4), ss. 864–879.

[117] Ulrich Krotz & Danilo Di Mauro & Jonas J. Driedger (2026), "War as External Cause: Russia's Invasion of Ukraine, the Theorising of European Integration and EU Politics, and the EU's Arduous Formation in Foreign and Security Policy", *Journal of European Public Policy,* 33(8), ss. 2202, 2218–2220; Kjølv Egeland & Benoît Pélopidas (2021), "European Nuclear Weapons? Zombie Debates and Nuclear Realities", *European Security*, 30(2), s. 237; Dimitry Adamsky (2026), "How Russia Sees the World Now - the Kremlin's New Mental Map Is Changing the War in Ukraine—and the Confrontation with the West", *Foreign Affairs*, Erişim Tarihi: 23.10.2026,

duyurulan ileri caydırıcılık yaklaşımı, savaş başlığının arttırılmasını ve müttefiklerle nükleer iş birliğini güçlendirmeyi öngörmekle birlikte, nükleer silah kullanma kararının tamamen Fransa Cumhurbaşkanı'nda olmasını talep ederken aynı zamanda bu konsepti NATO'nun nükleer caydırıcılığına tamamlayıcı bir öneri olarak sunmuştur.[118] Macron'un bu yaklaşımı, ABD'den kopmadan ona olan bağımlılığı dengeleyecek ara bir çözüm önerisidir.

6.3. Dost-Düşman Algısındaki Diğer Aktörler: Çin, Ukrayna ve Türkiye

Dost ve düşman algısının keskinleştiği bir dönemde, diğer dikkate değer aktörlerin önemi de artmıştır. 2019 yılında AB tarafından Çin, aynı anda hem iş birliği ve müzakere ortağı hem de ekonomik ve sistemsel rakip olarak tanımlanırken[119], sonrasında Ukrayna-Rusya Savaşıyla birlikte rakip odaklı bir yaklaşım benimsenmiştir. Ancak AB'nin ABD'yle belirsizleşen ilişkileri neticesinde, Birliğin Çin politikası tamamen ayrışma ve kopuş yerine daha ihtiyatlı ve riskten korunmaya dayalı olmuştur.[120]

Ukrayna ise Birliğe komşu ve yardım edilen bir ülkeden Avrupa güvenliğine katkı sağlayan bir aktöre dönüşmüştür. SAFE programı kapsamında üye devletlerle eşit koşullarda ortak tedarike katılması ve 90 milyar avroluk kredinin büyük bölümünün Ukrayna savunma sanayi kapasitesine ayrılması sonucunda, bu aktör Avrupa savunma sanayi tabanının uygulamada bir parçası haline gelmiştir. Ancak Ukrayna, AB'nin güvenliğine katkı sağlayan bir dış unsur olarak eşikte tutulurken, diğer taraftan Birliğin dayanışma ve kapsayıcılık rolüyle güvenlikleştirme ve sınırların yeniden belirlenmesi arasında bir uyumsuzluk vardır.[121]

AB'nin stratejik özerklik projesinin kapsamı açısından Türkiye dikkat çekici bir aktördür. NATO'nun ikinci büyük ordusuna sahip olmasına, Karadeniz'de Montrö Sözleşmesi

---

Erişim Adresi: https://www.foreignaffairs.com/russia/how-russia-sees-world-now. AB'nin nükleer tartışmaları özellikle Fransa tarafından yürütülmektedir.

[118] Wannes Verstraete (2026), "Dissuasion Avancée: Macron's Realistic Complement to Nato Nuclear Deterrence", Egmont Royal Institute for International Relations Vrije Universiteit Brussel, Erişim Tarihi: 19.09.2026, Erişim Adresi: https://cris.vub.be/ws/portalfiles/portal/224454951/Wannes-Verstraete_Policy_Brief_403.pdf, ss. 1-5.

[119] Avrupa Birliği Komisyonu & Yüksek Temsilcilik (2019), "EU-China – a Strategic Outlook (Join(2019) 5 Final)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0005.

[120] Léonie Allard & Rachel Rizzo (2025), "Transatlantic Security in a New Era", s. 85; Andreea Budeanu & Caterina Carta, & Stephan Klose (2026), "Mind the Perception Gap: Chinese Responses to EU De-Risking", *European Journal of International Security*, ss. 1–22; Henry Farrell & Abraham Newman & Yeling Tan (2026), "The Chokepoint Trap - How the Search for Economic Security Will End in Geopolitical Calamity", *Foreign Affairs*, 20.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/united-states/chokepoint-trap-economics-farrell-newman-tan; Xuechen Chen & Xinchuchu Gao (2022), "Analysing the EU's Collective Securitisation Moves Towards China", *Asia Europe Journal,* 20(2), ss. 199–212.

[121] Kateryna Pishchikova (2025), "European Identity Construction after the Russian Full-Scale Invasion of Ukraine: Dialogic (Re)Construction of Self and Others", ss. 1571–1586.

kapsamında kritik rolüne ve hızla gelişen savunma sanayisine rağmen, Türkiye, SAFE projesinin daha geniş kapsamlı katılımı için gerekli olan ikili antlaşmanın, Yunanistan ve Güney Kıbrıs Rum Yönetimi'nin itirazları nedeniyle dışında kalmıştır.[122] Diğer taraftan, Kanada ise benzeri bir antlaşmayı 2026 yılı Haziran ayında tamamlamıştır.[123] Her ne kadar Ukrayna-Rusya Savaşı Türkiye-AB ilişkilerinde farklı bir boyut açabilecek nitelikte olsa da, bu durum tarihsel olarak kaçırılmış fırsatların döngüsel niteliğinin devamı olmuştur.[124] Türkiye, kurumsal düzeyde dışarıda tutulurken, devletler seviyesinde Türk savunma sanayisi şirketlerinin önemli anlaşmalar yapması özerkliğin aktöre göre dışlayıcılığını da belirginleştirmiştir. AB düşman algısını netleştirirken, dostluk çemberini de seçici genişleme ve Türkiye'nin dışlanması gibi örneklerle daraltmaktadır. Ayrıca, ihtiyaç duyulan ortaklıklar, kendi iç mekanizmalarındaki itirazlar nedeniyle dışarıda bırakılmaktadır.

7. Tartışmalar: Dönüşümün Tamamlanmaması ve Üç Çelişki

Avrupa Birliği'nin savunma dönüşümü girişimleri yapısal gerilimler üreten üç safhadan oluşmuştur. 2022-2026 yıllarını kapsayan üç safha; şok ve kalıpların kırılması (2022-2023), savunma sanayisinin kurumsallaşması (2023-2024) ve terk edilme kaygısı altında özerkleşme çalışmaları (2025-2026) çerçevesinde şekillenmiştir.

Ukrayna-Rusya Savaşı'nın başlamasının ardından, şok ve kalıpların kırılması safhasında (2022-2023) AB'nin baskın mantığı kolektif güvenlikleştirme ve bu duruma acil tepki vermekti. Bu safhanın temel araçları EPF, yaptırımlar, Stratejik Pusula, REPowerEU ve bazı ülkelere aday statüsü verilmesidir. Sürecin siber boyutuyla ilgili olarak Viasat saldırısının sorumlusu Rusya olarak görülmüş ve NIS2 direktifinin uygulanması kabul edilmiştir. Bu safhada, dost ve düşman algısı çerçevesinde Rusya doğrudan bir tehdit olarak görülürken, ABD ise güvence veren bir müttefik olarak görülmüştür. AB için temel sınırlılıklar, kararlarda oybirliğinin sağlanmasındaki zorluklar ve kapasitenin dağınık olmasıdır.

Savunma sanayisinin kurumsallaşma safhasında (2023-2024) ise Komisyon'un girişimciliğine ve sanayi politikasına verilen ağırlık dikkat çekmiştir. Bu safhanın temel araçları ASAP, EDIRPA, EDIS ve Ukrayna için Avrupa Barış Tesisi (veya olanağı) projeleridir. Siber boyutuyla

[122] Avrupa Birliği Konseyi (2026), "What Is Security Action for Europe (Safe)?", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/safe/.
[123] Avrupa Birliği Konseyi (2026), "Safe: Council Concludes Agreement with Canada", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2026/06/15/safe-council-concludes-agreement-with-canada/.
[124] Ziya Öniş (2023), "Historic Missed Opportunities and Prospects for Renewal: Turkey-EU Relations in a Post-Western Order", *Turkish Studies,* 24(3-4), ss. 691–709.

Siber Dayanıklılık ve Siber Dayanışma yasalarının çıkarılmasına ve hibrit tehdit çerçevelerinin oluşturulmasına ağırlık verilmiştir. Dost-düşman algısı bağlamında Rusya uzun vadeli bir tehdit olarak tanımlanırken, Çin ise sistemik bir rakip olarak görülmüştür. Bu safhadaki temel sınırlılık ise savunma sanayisinde beklenen ortak tedarik oranının düşük olmasıdır.

Terk edilme kaygısı altında özerklik çalışmaları safhasında (2025-2026) hazırlık planları, mali kapasite analizleri ve özerklik tartışmaları önem kazanmıştır. Bu dönemin temel araçları Beyaz Kitap, SAFE ve Ukrayna için tahsis edilen 90 milyar avroluk kredidir. Siber boyutuyla tedarik zincirlerinin jeopolitik düzlemde değerlendirilmesi ve Siber Güvenlik Yasası'nın revizyon önerisi dikkat çekmiştir. Dost-düşman algısı çerçevesinde Rusya temel tehdit öznesi olarak görülürken, ABD ise belirsiz bir müttefik olarak değerlendirilmiştir. Bu safhanın temel sınırlılıkları ise bütünleşme sürecine yönelik farklılaşmanın görülmesi ve özerklik arayışında dışlayıcı bir yaklaşımın benimsenmesi olmuştur.

AB'nin güvenlik dönüşümünde ilk çelişki kapasite alanında ortaya çıkmıştır. Savaş öncesinde AB'nin temel sorunu, beklenti ile kapasite arasındaki açık farktır.[125] Ancak daha sonrasında Birliğin kaynakları artarken, bu kaynakların ortak kapasiteye dönüşmesi beklenen ölçüde gerçekleşmemiştir. Dolayısıyla, kaynak ve entegrasyon uyumsuzluğu nedeniyle ortak tedarikin yüzde 24 seviyesinde kalması ve büyük ölçüde ulusal yönde gelişmesi sonrasında savunma pazarının parçalı hale gelmesi riski görülmektedir. Savunma sanayisine yön verecek aktörler arasındaki uyuşmazlık ve Avrupa savunma pazarının oluşturulması çabalarındaki ikilem büyük bir yapısal soruna neden olmaktadır.[126]

Güvenlik dönüşümü girişimlerine yönelik ikinci çelişki birlik alanıyla ilgilidir. AB, söylemsel olarak Rusya'ya karşı kusursuz bir birlik görüntüsü verse de, bunu farklı araçlarla sağlamaktadır. Ukrayna'ya verilecek kredinin güçlendirilmiş iş birliği yoluyla 24 üye devlet tarafından sağlanmış olması, oybirliği gerektiren prosedürlerin tıkandığı zaman diğer hukuki seçeneklerin pratik bir şekilde uygulanabildiğini göstermiştir. Bu durum, AB'nin olaylara yanıt verirken biçim değiştirebilen çok katmanlı ve çok boyutlu bir aktör olabildiğini doğrulamıştır.[127] Güvenlik alanında görülen farklılık, bütünleşmenin istisnası olmaktan çıkıp kural olarak uygulanabileceğini göstermiştir.

---

[125] Christopher Hill (1993), "The Capability-Expectations Gap, or Conceptualizing Europe's International Role", ss. 305–326.

[126] Jan Joel Andersson & Malena Britz (2025), "The European Union's Role in European Defence Industry Policy", ss. 322–338.

[127] Veronica Anghel & Erik Jones (2023), "Is Europe Really Forged through Crisis? Pandemic EU and the Russia–Ukraine War", ss. 766–781.

Üçüncü ve son çelişki ise özerklik alanı ile ilgilidir. AB'nin stratejik özerklik beklentisi ABD'ye olan bağımlılığı azaltmayı hedeflerken, bu hedefin gerçekleştirilmesi sürecinde bağımlılık devam etmektedir. Bunun yanı sıra, Türkiye gibi önemli bir aktör Avrupa savunmasından dışarıda bırakılarak stratejik özerklik projesi coğrafi ve kurumsal olarak daraltılmaktadır. Dolayısıyla, özerkliğin gerçekleşmesi için gerekli olan bir kapasiteden mahrum kalınmaktadır. Ukrayna-Rusya Savaşı, AB'yi ideal bir devlet seviyesine ulaştıramamış; ancak Birliği, güvenlik yönüyle piyasa, mali ve düzenleme araçlarını kullanarak hibrit bir güvenlik aktörüne dönüştürmüştür.[128] Savaşın güvenlik, savunma ve dış politika üzerindeki etkileri kapsamlı bir şekilde görülse de henüz üniter ve güç projeksiyonlarının etkin bir şekilde yansıtıldığı bir aktör dönüşümü söz konusu değildir.[129]

Sonuç

Bu çalışmada, Ukrayna-Rusya Savaşı çerçevesinde AB güvenlik girişimlerinin hangi mekanizmalar aracılığıyla ve hangi derinlikte dönüştürüldüğü analiz edilmiştir. Araştırma, savaş öncesindeki kural koyucu güç kimliği, enerji alanındaki karşılıklı bağımlılık ve özellikle söylemsel stratejik özerklik arayışıyla tanımlanan güvenlik yaklaşımının; savaş döneminde belirli kalıpların çöküşünü ve güvenliğin enerji, yaptırım ve genişleme yoluyla farklı alanlara yayılmasını, 2024-2026 yılları arasında ise savunma sanayisi ve finansmanı alanında kurumsallaşma yoluyla dönüşümünü ortaya koymuştur.

Güvenlik girişimi dönüşümünde temel mekanizmanın piyasa yoluyla güvenlik sağlamaya dayandığı tespit edilmiştir. AB'nin OGSP'sinin hükümetler arası odaklı yaklaşımında sınırlı bir değişim görülse de ortak tedarik, ortak savunma ve ortak borçlanma planlamasında piyasa ve bütçe yetkileri aracılığıyla daha geniş bir kapasite sağlanmıştır. Bu hibrit güvenlik girişimi, savaşın AB'nin tarihsel olarak eksik kalan dış tehdit baskısını sağladığını; ancak bu baskının Birliğin mevcut kurumsal yapısı içinde çözülmeye çalışıldığını göstermektedir. AB'nin siber

[128] hilipp Genschel & Lauren Leek, & Jordy Weyns (2023), "War and Integration. The Russian Attack on Ukraine and the Institutional Development of the EU", ss. 343–357; Kathleen R. McNamara (2024), "Transforming Europe? The EU's Industrial Policy and Geopolitical Turn", ss. 2371–2389; Pierre Haroche (2024), "Geoeconomic Power Europe: When Global Power Competition Drives EU Integration", ss. 938–949. Hibrit yöntemlerle mücadele aynı ölçüde Rusya tarafından da uygulanmaktadır. Dolayısıyla hibrit mücadele yöntemi çok aktörlü bir durum üzerinden sürdürülmektedir. Konu hakkında ayrıntılı bilgi için bakınız; Julianne Smith (2026), "Russia's Hybrid War Has Entered a Dangerous New Phase - and the West Has Done Far Too Little to Deter It", *Foreign Affairs*, 07.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/russia/russias-hybrid-war-has-entered-dangerous-new-phase; Benjamino Irdi (2026), "Europe Is Asking the Wrong Question About Russia's Hybrid War", *Foreign Policy*, 22.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://foreignpolicy.com/2026/10/22/europe-russia-hybrid-war-escalation/.

[129] Ulrich Krotz & Danilo Di Mauro & Jonas J. Driedger (2026), "War as External Cause: Russia's Invasion of Ukraine, the Theorising of European Integration and EU Politics, and the EU's Arduous Formation in Foreign and Security Policy", ss. 2199–2220.

güvenlik boyutu odağında, 2026 yılındaki Siber Güvenlik Yasası revizyon önerisiyle, teknik ve tarafsız bir sınıflandırma yöntemiyle dost ve düşman ayrımı yapan, ayrıca tedarik zinciri ağına işlerlik kazandıran düzenleyici bir güvenlik mantığını yerleştiren bir düzene geçtiği tespit edilmiştir. Ukrayna-Rusya Savaşı algısal yönüyle de büyük bir güvenlik dönüşümünü ortaya çıkarmıştır. Rusya'nın düşmanlığı tartışmasız olarak netleşirken, ABD'nin ise güvenilir bir müttefikten belirsiz bir aktöre dönüştüğü tespit edilmiştir. Ayrıca ABD'ye karşı askeri bağımlılık ile politik güvensizlik arasında güvenlik ikilemi sürmektedir.

AB'nin güvenlik dönüşümü her ne kadar ilerlemiş olsa da henüz tamamlanmamıştır. Kaynak ve entegrasyon açığı, farklılaşan birlik uyumu ve dışlayıcı özerklik olarak tanımlanan üç çelişki, AB'nin savaş sonrasında Avrupa güvenlik düzeninde nasıl bir aktör olacağını ortaya koyacaktır. Bu bağlamda, Türkiye gibi AB üyesi olmayan bir NATO üyesinin AB savunma girişiminden dışlanması ve bununla birlikte Kanada ile tanımlanmış bir ortaklık çerçevesinin oluşturulması, özerklik planında maliyetin hesaplanmasını zorlaştırmaktadır. Gelecekte yapılacak araştırmalarda SAFE'nin uygulama kapasitesi, Siber Güvenlik Yasası revizyonunun yasama süreci ve savaşın gidişatındaki değişimlerin AB'nin tehdit algısı üzerindeki etkisinin ampirik olarak incelenmesi, bu araştırmadaki argümanların sınanması açısından önem taşımaktadır.

KAYNAKÇA

- Adamsky, Dimitry (2026), "How Russia Sees the World Now - the Kremlin's New Mental Map Is Changing the War in Ukraine—and the Confrontation with the West", *Foreign Affairs*, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/russia/how-russia-sees-world-now.
- Allard, Léonie & Rizzo, Rachel (2025), "Transatlantic Security in a New Era", *Survival*, 67(2), ss. 85–96.
- Andersson, Jan Joel & Britz, Malena (2025), "The European Union's Role in European Defence Industry Policy", *Defence Studies*, 25(2), ss. 322–341.
- Anghel, Veronica & Džankić, Jelena (2023), "Wartime EU: Consequences of the Russia–Ukraine War on the Enlargement Process", *Journal of European Integration,* 45(3), ss. 487–501.
- Anghel, Veronica & Jones, Erik (2023), "Is Europe Really Forged through Crisis? Pandemic EU and the Russia–Ukraine War", *Journal of European Public Policy*, 30(4), ss. 766–786.
- Avrupa Birliği (2016), "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.
- Avrupa Birliği (2024), "Edis - European Defence Industrial Strategy", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://defence-industry-space.ec.europa.eu/document/download/333faee1-a851-44a6-965b-713247515d39_en?filename=DEFIS_EDIS_factsheet.pdf.
- Avrupa Birliği Komisyonu (2022), "Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Repowereu: Joint European Action for More Affordable, Secure and Sustainable Energy (Com/2022/108 Final)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/resource.html?uri=cellar:71767319-9f0a-11ec-83e1-01aa75ed71a1.0001.02/DOC_1&format=PDF,
- Avrupa Birliği Komisyonu (2022), "Repowereu Plan (Com(2022) 230 Final)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0230.
- Avrupa Birliği Komisyonu (2024), "EU Opens Accession Negotiations with Ukraine", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://enlargement.ec.europa.eu/news/eu-opens-accession-negotiations-ukraine-2024-06-25_en.
- Avrupa Birliği Komisyonu (2026), "Andrius Kubilius, Commissioner (2024-2029), Defence and Space", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://commission.europa.eu/about/organisation/college-commissioners/andrius-kubilius_en.
- Avrupa Birliği Komisyonu (2026), "Proposal for a Regulation on Enisa, the European Cybersecurity Certification Framework, and Ict Supply Chain Security and Repealing Regulation (Eu) 2019/881 (Com(2026) 11 Final)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52026PC0011.

- Avrupa Birliği Komisyonu & Yüksek Temsilcilik (2019), "EU-China – a Strategic Outlook (Join(2019) 5 Final)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0005.
- Avrupa Birliği Komisyonu & Yüksek Temsilcilik (2024), "A New European Defence Industrial Strategy: Achieving EU Readiness through a Responsive and Resilient European Defence Industry (Join(2024) 10 Final)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024JC0010.
- Avrupa Birliği Komisyonu & Yüksek Temsilcilik (2025), "Joint White Paper for European Defence Readiness 2030 - Join(2025) 120 Final", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025JC0120.
- Avrupa Birliği Konseyi (2009), "Secure Europe in a Better World: European Security Strategy", Erişim Tarihi: 26.09.2026, Erişim Adresi: https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf.
- Avrupa Birliği Konseyi (2017), "Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf.
- Avrupa Birliği Konseyi (2022), "A Strategic Compass for Security and Defence", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.
- Avrupa Birliği Konseyi (2022), "Council Decision (CFSP) 2022/338 of 28 February 2022 on an Assistance Measure under the European Peace Facility for the Supply to the Ukrainian Armed Forces of Military Equipment, and Platforms, Designed to Deliver Lethal Force", Erişim Tarihi: 18.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2022/338/2023-04-13/eng.
- Avrupa Birliği Konseyi (2022), "Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.
- Avrupa Birliği Konseyi (2024), "Council Decision (CFSP) 2024/2643 of 8 October 2024 Concerning Restrictive Measures in View of Russia's Destabilising Activities", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2024/2643/2025-05-22/eng.
- Avrupa Birliği Konseyi (2024), "Council Regulation (EU) 2024/2642 of 8 October 2024 Concerning Restrictive Measures in View of Russia's Destabilizing Activities", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2024/2642/oj.
- Avrupa Birliği Konseyi (2024), "Hybrid Threats: Council Paves the Way for Deploying Hybrid Rapid Response Teams", Erişim Tarihi: 17.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/hybrid-threats-council-paves-the-way-for-deploying-hybrid-rapid-response-teams/.

- Avrupa Birliği Konseyi (2025), "Establishing the Security Action for Europe (SAFE) through the Reinforcement of the European Defence Industry Instrument", Erişim Tarihi: 18.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2025/1106/oj/eng.
- Avrupa Birliği Konseyi (2025), "SAFE: Council Adopts €150 Billion Boost for Joint Procurement on European Security and Defence", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2025/05/27/safe-council-adopts-150-billion-boost-for-joint-procurement-on-european-security-and-defence/pdf/.
- Avrupa Birliği Konseyi (2026), "21st Package of Sanctions: EU Hits Russian Energy, Financial Services and Crypto Hard", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2026/07/23/21st-package-of-sanctions-eu-hits-russian-energy-financial-services-and-crypto-hard/.
- Avrupa Birliği Konseyi (2026), "Council Decision (CFSP) 2026/1845 of 23 July 2026 Amending Decision 2014/145/Cfsp Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dec/2026/1845/oj.
- Avrupa Birliği Konseyi (2026), "Council Regulation (EU) 2026/1844 of 23 July 2026 Amending Regulation (EU) No 269/2014 Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2026/1844/oj.
- Avrupa Birliği Konseyi (2026), "EU Financial Assistance to Ukraine", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/ukraine-solidarity-financial-support/.
- Avrupa Birliği Konseyi (2026), "Safe: Council Concludes Agreement with Canada", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2026/06/15/safe-council-concludes-agreement-with-canada/.
- Avrupa Birliği Konseyi (2026), "What Is Security Action for Europe (Safe)?", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/policies/safe/.
- Avrupa Birliği Parlamentosu & Konseyi (2013), "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001.
- Avrupa Birliği Parlamentosu & Konseyi (2016), "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.
- Avrupa Birliği Parlamentosu & Konseyi (2019), "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013

(Cybersecurity Act) (Text with EEA Relevance)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

- Avrupa Birliği Parlamentosu & Konseyi (2020), "Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018.
- Avrupa Birliği Parlamentosu & Konseyi (2022), "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (Nis 2 Directive) (Text with Eea Relevance)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
- Avrupa Birliği Parlamentosu & Konseyi (2022), "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC (Text with EEA Relevance)", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/dir/2022/2557/oj.
- Avrupa Birliği Parlamentosu & Konseyi (2023), "Joint Communication to the European Parliament, the European Council and the Council on European Economic Security Strategy", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0020.
- Avrupa Birliği Parlamentosu & Konseyi (2023), "Regulation (EU) 2023/1525 of the European Parliament and of the Council of 20 July 2023 on Supporting Ammunition Production (ASAP)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2023/1525/oj.
- Avrupa Birliği Parlamentosu & Konseyi (2023), "Regulation (EU) 2023/2418 of the European Parliament and of the Council of 18 October 2023 on Establishing an Instrument for the Reinforcement of the European Defence Industry through Common Procurement (EDIRPA)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2023/2418/oj.
- Avrupa Birliği Parlamentosu & Konseyi (2023), "Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the Protection of the Union and Its Member States from Economic Coercion by Third Countries", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2023/2675/oj.
- Avrupa Birliği Parlamentosu & Konseyi (2024), "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA Relevance)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2024/2847/oj.
- Avrupa Birliği Parlamentosu & Konseyi (2025), "Regulation (EU) 2025/2643 of the European Parliament and of the Council of 16 December 2025 Establishing the European Defence Industry Programme and a Framework of Measures to Ensure the Timely Availability and Supply of Defence Products ('EDIP Regulation') (Text with EEA Relevance)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2025/2643/oj.

- Avrupa Birliği Parlamentosu & Konseyi (2025), "Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 Laying down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cyber Threats and Incidents and Amending Regulation (EU) 2021/694 (Cyber Solidarity Act)", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://eur-lex.europa.eu/eli/reg/2025/38/oj.
- Avrupa Birliği Parlamentosu & Konseyi (2026), "AP ve Konsey Tüzüğü (AB) 2026/467", Erişim Tarihi: 23.10.2026, Erişim Adresi: https://lawplayer.com/eu/act/32026R0467.
- Avrupa Konseyi (2022), "European Council Conclusions, 23-24 June 2022", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2022/06/24/european-council-conclusions-23-24-june-2022/.
- Avrupa Konseyi (2022), "The Versailles Declaration, 10 and 11 March 2022", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2022/03/11/the-versailles-declaration-10-11032022/.
- Avrupa Konseyi (2023), "European Council Conclusions, 14 and 15 December 2023", Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.consilium.europa.eu/en/press/press-releases/2023/12/15/european-council-conclusions-14-and-15-december-2023/.
- Avrupa Konseyi (2025), "European Council, 18 December 2025 - Main Results", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.consilium.europa.eu/en/meetings/european-council/2025/12/18/.
- Avrupa Savunma Kurumu (2026), "Defence Data Portal: Aggregated Data (All Member States)", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.eda.europa.eu/publications-and-data/defence-data.
- Avrupa Savunma Kurumu (2026), "EU Defence Spending: €418 Billion in 2025, Projected to €454 Billion in 2026", Erişim Tarihi: 29.09.2026, Erişim Adresi: https://eda.europa.eu/news-and-events/news/2026/07/16/eu-defence-spending---418-billion-in-2025--projected-to--454-billion-in-2026.
- Bandow, Doug (2026), "An Independent Europe Means No More U.S. Rooster in the Henhous", CATO Institute, 19.08.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.cato.org/commentary/independent-europe-means-no-more-us-rooster-henhous.
- Bellanova, Rocco & Carrapico, Helena & Duez, Denis (2022), "Digital/Sovereignty and European Security Integration: An Introduction", *European Security*, 31(3), ss. 337–355.
- Bergmann, Julian & Müller, Patrick (2021), "Failing Forward in the EU's Common Security and Defense Policy: The Integration of EU Crisis Management", *Journal of European Public Policy*, 28(10), ss. 1669–1687.
- Blumenau, Bernhard (2022), "Breaking with Convention? Zeitenwende and the Traditional Pillars of German Foreign Policy", *International Affairs*, 98(6), ss. 1895–1913.

- Bosse, Giselle (2022), "Values, Rights, and Changing Interests: The EU's Response to the War against Ukraine and the Responsibility to Protect Europeans", *Contemporary Security Policy,* 43(3), ss. 531–546.
- Bradford, Anu (2020), *The Brussels Effect: How the European Union Rules the World.* New York: Oxford University Press.
- Broeders, Dennis & Cristiano, Fabio & Kaminska, Monica (2023), "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions", *JCMS: Journal of Common Market Studies,* 61(5), ss. 1261–1280.
- Budeanu, Andreea & Carta, Caterina & Klose, Stephan (2026), "Mind the Perception Gap: Chinese Responses to EU De-Risking", *European Journal of International Security*, ss. 1–22.
- Bueger, Christian & Liebetrau, Tobias (2023). "Critical Maritime Infrastructure Protection: What's the Trouble?", *Marine Policy*, 155, ss. 1–8.
- Bull, Hedley (1982), "Civilian Power Europe: A Contradiction in Terms?", *JCMS: Journal of Common Market Studies*, 21(2), ss. 149–170.
- Buzan, Barry & Waever, Ole & de Wilde, Jaap (1998), *Security: A New Framework for Analysis*, Boulder, Colorado: Lynne Rienner Publishers.
- Calcara, Antonio & Simón, Luis (2021), "Market Size and the Political Economy of European Defense", *Security Studies*, 30(5), ss. 860–892.
- Carrapico, Helena & Barrinha, André (2017), "The EU as a Coherent (Cyber) Security Actor?", *JCMS: Journal of Common Market Studies*, 55(6), ss. 1254–1272.
- Carrapico, Helena & Farrand, Benjamin (2020), "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy", *Journal of European Integration,* 42(8), ss. 1111–1126.
- Chen, Xuechen & Gao, Xinchuchu (2022), "Analysing the EU's Collective Securitisation Moves Towards China", *Asia Europe Journal,* 20(2), ss. 195–216.
- Christou, George (2019), "The Collective Securitisation of Cyberspace in the European Union", *West European Politics*, 42(2), ss. 278–301.
- Ciaramella, Eric (2026), "Ukraine Can Turn Imminent Peril to Its Advantage - How a True "Energy Cease-Fire" Can Curb Putin", *Foreign Affairs*, 15.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/ukraine/ukraine-can-turn-imminent-peril-its-advantage.
- Clark, Mason (2026), "The Russian Military Campaign against Europe: Defining the Threat." Institute for the Study of War (ISW), 16.09.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://understandingwar.org/research/defense-of-europe/the-russian-military-campaign-against-europe-defining-the-threat/.
- Costa, Oriol & Barbé, Esther (2023), "A Moving Target. Eu Actorness and the Russian Invasion of Ukraine", *Journal of European Integration*, 45(3), ss. 431–446.
- Council on Foreign Relation (2026), "Trump Will Attend Davos Talks on Greenland." 20.01.2026, Erişim Tarihi: 29.09.2026, Erişim Adresi: https://www.cfr.org/articles/trump-will-attend-davos-talks-on-greenland.

- Csernatoni, Raluca (2022), "The EU's Hegemonic Imaginaries: From European Strategic Autonomy in Defence to Technological Sovereignty", *European Security*, 31(3), ss. 395–414.
- Damro, Chad (2012), "Market Power Europe", *Journal of European Public Policy*, 19(5), ss. 682–699.
- Danzman, Sarah Bauerle & Meunier, Sophie (2024), "The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator", *JCMS: Journal of Common Market Studies*, 62(4), ss. 1097–1115.
- De la Torre, Juan Carlos (2026), "Europe's Defence Spending Is Surging, but Fragmented Procurement Is Holding Industry Back", Digitalshield, 19.10.2026, Erişim Tarihi: 24.10.2026, Erişim Adresi: https://www.escudodigital.com/en/defense/europe/europes-defence-spending-is-surging-but-fragmented-procurement-is-holding-industry-back.html.
- Della Sala, Vincent (2023), "Ontological Security, Crisis and Political Myth: The Ukraine War and the European Union", *Journal of European Integration*, 45(3), ss. 361–375.
- Duchêne, François (1972), "Europe's Role in World Peace", içinde (editör: Richard Mayne) *Europe Tomorrow: Sixteen Europeans Look Ahead*, Londra: Fontana, ss. 32–47.
- Edelman, Eric S. & Miller, Franklin C. & Touval, Yonatan & Stein, Janice Gross & Gottemoeller, Rose (2026), "Who Needs the Bomb? The Purpose of Nuclear Deterrence", *Foreign Affairs*, 20.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/responses/who-needs-bomb-edelman-miller-touval-stein.
- Egeland, Kjølv & Pélopidas, Benoît (2021), "European Nuclear Weapons? Zombie Debates and Nuclear Realities", *European Security*, 30(2), ss. 237–258.
- Emir, Mehmet (2025), "Varoluşsal Tehdit Algısının Dinamik Güvenlikleştirmeye Dönüşümü: Ukrayna-Rusya Savaşında Aktör Stratejilerinin Analizi", *Politik Ekonomik Kuram*, 9(4), ss. 1687–1705.
- Ewers-Peters, Nele Marianne (2025), "EU-NATO Cooperation Reloaded: The Impact of European Strategic Autonomy", *Defence Studies*, 25(4), ss. 864–883.
- Farrand, Benjamin & Carrapico, Helena (2022), "Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity", *European Security,* 31(3), ss. 435–453.
- Farrell, Henry & Newman, Abraham & Tan, Yeling (2026), "The Chokepoint Trap - How the Search for Economic Security Will End in Geopolitical Calamity", *Foreign Affairs*, 20.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/united-states/chokepoint-trap-economics-farrell-newman-tan.
- Fasola, Nicolò & Lucarelli, Sonia & Moro, Francesco Niccolò (2025), "Cyber Diplomacy and the Russia–Ukraine War", *The Hague Journal of Diplomacy*, 20*(*4), ss. 749–764.

- Fiott, Daniel (2023), "In Every Crisis an Opportunity? European Union Integration in Defence and the War on Ukraine", *Journal of European Integration*, 45(3), ss. 447–462.
- Fiott, Daniel (2024), "From Liberalisation to Industrial Policy: Towards a Geoeconomic Turn in the European Defence Market?", *JCMS: Journal of Common Market Studies,* 62(4), ss. 1012–1027.
- Freudlsperger, Christian & Schimmelfennig, Frank (2023), "Rebordering Europe in the Ukraine War: Community Building without Capacity Building", *West European Politics,* 46(5), ss. 843–871.
- Freudlsperger, Christian & Meunier, Sophie (2024), "When Foreign Policy Becomes Trade Policy: The EU's Anti-Coercion Instrument", *JCMS: Journal of Common Market Studies,* 62(4, ss. 1063–1079.
- Friedrichs, Gordon M. & Sommer, Jule (2025), "Ontological Security Crisis and Role Conception Change: The Impact of the Russian Invasion of Ukraine on the European Union's Role Conceptions", *European Journal of International Relations,* 31(1), ss. 126–151.
- Gabuev, Alexander (2026), "How Europe Can Get Putin's Attention - the Continent Must Overcome Its Russia Predicament", *Foreign Affairs*, 07.07.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/russia/how-europe-can-get-putins-attention.
- Genschel, Philipp (2022), "Bellicist Integration? The War in Ukraine, the European Union and Core State Powers", *Journal of European Public Policy*, 29(12), ss. 1885–1900.
- Genschel, Philipp & Leek, Lauren & Weyns, Jordy (2023), "War and Integration. The Russian Attack on Ukraine and the Institutional Development of the EU", *Journal of European Integration*, 45(3), ss. 343–360.
- Ghitis, Frida (2026), "Trump's Pro-Russian Turn Puts Ukraine—and Europe—on Edge", *World Politics Review*, 15.10.2026, Erişim Tarihi: 19.10.2026, Erişim Adresi: https://www.worldpoliticsreview.com/trump-putin-pro-russia-ukraine-zelenskyy-europe/.
- Giltner, Benjamin (2026), "Europe's Nuclear Shortcut Would Be a Strategic Mistake." CATO Institute, 31.03.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.cato.org/commentary/europes-nuclear-shortcut-would-be-strategic-mistake.
- Goldthau, Andreas C. & Youngs, Richard (2023), "The EU Energy Crisis and a New Geopolitics of Climate Transition", *JCMS: Journal of Common Market Studies*, 61, ss. 115–124.
- Grunstein, Judah (2026), "Rubio's Vision of Western Primacy Is Just Empire by Another Name", *World Politics Review*, 16.10.2026, Erişim Tarihi: 19.10.2026, Erişim Adresi: https://www.worldpoliticsreview.com/rubio-athens-western-civilization/.
- Håkansson, Calle (2024), "The Ukraine War and the Emergence of the European Commission as a Geopolitical Actor", *Journal of European Integration,* 46(1), ss. 25–45.

- Haroche, Pierre (2020), "Supranationalism Strikes Back: A Neofunctionalist Account of the European Defence Fund", *Journal of European Public Policy*, 27(6), ss. 853–872.
- Haroche, Pierre (2023), "A 'Geopolitical Commission': Supranationalism Meets Global Power Competition", *JCMS: Journal of Common Market Studies*, 61(4), ss. 970–987.
- Haroche, Pierre (2024), "Geoeconomic Power Europe: When Global Power Competition Drives EU Integration", *JCMS: Journal of Common Market Studies*, 62(4), ss. 938–954.
- Helwig, Niklas (2023), "EU Strategic Autonomy after the Russian Invasion of Ukraine: Europe's Capacity to Act in Times of War", *Journal of Common Market Studies,* 61(1), ss. 57–67.
- Helwig, Niklas & Sinkkonen, Ville (2022), "Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term", *European Foreign Affairs Review*, 27(Special), ss. 1–20.
- Herranz-Surrallés, Anna & Damro, Chad & Eckert, Sandra (2024), "The Geoeconomic Turn of the Single European Market? Conceptual Challenges and Empirical Trends". *JCMS: Journal of Common Market Studies,* 62(4), ss. 919–937.
- Hill, Christopher (1993), "The Capability-Expectations Gap, or Conceptualizing Europe's International Role", *Journal of Common Market Studies,* 31(3), ss. 305–328.
- Hoeffler, Catherine (2023), "Beyond the Regulatory State? The European Defence Fund and National Military Capacities", *Journal of European Public Policy,* 30(7), ss. 1281–1304.
- Hoeffler, Catherine & Hofmann, Stéphanie C. & Mérand, Frédéric (2024), "The Polycrisis and EU Security and Defence Competences", *Journal of European Public Policy,* 31(10), ss. 3224–3248.
- Hooghe, Liesbet & Marks, Gary (2009), "A Postfunctionalist Theory of European Integration: From Permissive Consensus to Constraining Dissensus", *British Journal of Political Science,* 39(1), ss. 1–23.
- Howorth, Jolyon (2018), "Strategic Autonomy and EU-NATO Cooperation: Threat or Opportunity for Transatlantic Defence Relations?", *Journal of European Integration,* 40(5), ss. 523–537.
- Howorth, Jolyon (2025), "European Defence and NATO: From Competition to Co-Operation to Replacement?", *Journal of Common Market Studies*, 63, ss. 156–168.
- Hunter, Tom & Wunsch, Natasha & Bélanger, Marie-Eve (2025), "A Geopolitical Turning Point? Enlargement Discourse after the Russian Invasion of Ukraine", *European Union Politics*, 26(4), ss. 689–713.
- Irdi, Benjamino (2026), "Europe Is Asking the Wrong Question About Russia's Hybrid War", *Foreign Policy*, 22.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://foreignpolicy.com/2026/10/22/europe-russia-hybrid-war-escalation/.
- Jones, Erik & Kelemen, R. Daniel & Meunier, Sophie (2021), "Failing Forward? Crises and Patterns of European Integration", *Journal of European Public Policy,* 28(10), ss. 1519–1536.

- Juncos, Ana E. (2017), "Resilience as the New EU Foreign Policy Paradigm: A Pragmatist Turn?", *European Security,* 26(1), ss. 1–18.
- Kelemen, R. Daniel & R. McNamara, Kathleen (2022), "State-Building and the European Union: Markets, War, and Europe's Uneven Political Development", *Comparative Political Studies*, 55(6), ss. 963–991.
- Kostyuk, Nadiya & Gartzke, Erik (2022), "Why Cyber Dogs Have yet to Bark Loudly in Russia's Invasion of Ukraine", *Texas National Security Review,* 5(3), ss. 113–126.
- Kostyuk, Nadiya & Brantly, Aaron (2022), "War in the Borderland through Cyberspace: Limits of Defending Ukraine through Interstate Cooperation", *Contemporary Security Policy,* 43(3), ss. 498–515.
- Koval, Nadiia & Vachudova, Milada Anna (2024), "European Union Enlargement and Geopolitical Power in the Face of War", *Journal of Common Market Studies,* 62, ss. 135–146.
- Krotz, Ulrich & Di Mauro, Danilo & Driedger, Jonas J. (2026), "War as External Cause: Russia's Invasion of Ukraine, the Theorising of European Integration and EU Politics, and the EU's Arduous Formation in Foreign and Security Policy", *Journal of European Public Policy,* 33(8), ss. 2199–2227.
- Kuleba, Dmytro (2026), "Russia's Plan to Break Ukraine - What Kyiv Needs to Survive", *Foreign Affairs*, 30.09.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/united-states/russias-plan-break-ukraine-dmytro-kuleba.
- Kuzemko, Caroline & Blondeel, Mathieu & Dupont, Claire & Brisbois, Marie Claire (2022), "Russia's War on Ukraine, European Energy Policy Responses & Implications for Sustainable Transformations", *Energy Research & Social Science*, 93, ss. 1–8.
- Logan, Justin & Kavanagh, Jennifer (2026), "Leave Europe to the Europeans." CATO Institute, 28.08.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.cato.org/commentary/leave-europe-europeans.
- Mader, Matthias & Gavras, Konstantin & Hofmann, Stephanie C. & Reifler, Jason & Schoen, Harald & Thomson, Catarina (2024), "International Threats and Support for European Security and Defence Integration: Evidence from 25 Countries", *European Journal of Political Research,* 63(2), ss. 433–454.
- Mälksoo, Maria (2016), "From the ESS to the EU Global Strategy: External Policy, Internal Purpose", *Contemporary Security Policy*, 37(3), ss. 374–388.
- Manners, Ian (2002), "Normative Power Europe: A Contradiction in Terms? *JCMS: Journal of Common Market Studies,* 40(2), ss. 235–258.
- Marsh, Nicholas & Martins, Bruno Oliveira & Mawdsley, Jocelyn (2026), "The European Iron Network: The Remaking of the Political Economy of European Defence Production Following the Ukraine War", *Journal of European Integration,* 48*(*5), ss. 835–855.
- Maschmeyer, Lennart (2021), "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations", *International Security,* 46(2), ss. 51–90.

- Maurer, Heidi & Whitman, Richard G. & Nicholas Wright (2023), "The EU and the Invasion of Ukraine: A Collective Responsibility to Act?", *International Affairs*, 99(1), ss. 219–238.
- McNamara, Kathleen R. (2024), "Transforming Europe? The EU's Industrial Policy and Geopolitical Turn", *Journal of European Public Policy,* 31(9), ss. 2371–2396.
- Meijer, Hugo & Brooks, Stephen G. (2021), "Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back", *International Security,* 45(4), ss. 7–43.
- Meissner, Katharina & Graziani, Chiara (2023), "The Transformation and Design of EU Restrictive Measures against Russia", *Journal of European Integration*, 45(3), ss. 377–394.
- Mertens, Claas & Woods, Ngaire (2026), "Europe's Credibility Gap - Dependence on America Has Left It with Little to Offer Would-Be Partners", *Foreign Affairs*, 19.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/europe/europes-credibility-gap.
- Michaels, Eva & Sus, Monika (2024), "(Not) Coming of Age? Unpacking the European Union's Quest for Strategic Autonomy in Security and Defence", *European Security,* 33(3), ss. 383–405.
- Mitzen, Jennifer (2006), "Ontological Security in World Politics: State Identity and the Security Dilemma", *European Journal of International Relations,* 12(3), ss. 341–370.
- Monsees, Linda & Lambach, Daniel (2022), "Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity", *European Security,* 31(3), ss. 377–394.
- Mustasilta, Katariina & Karjalainen, Tyyne (2026), "European Strategic Cultures in Flux? Case Study on the European Peace Facility", *European Journal of International Security,* 11(4), ss. 600–622.
- NATO (2023), "Finland Joins NATO as 31st Ally", 04.04.2023, Erişim Tarihi: 18.10.2026, Erişim Adresi: https://www.nato.int/en/news-and-events/articles/news/2023/04/04/finland-joins-nato-as-31st-ally?selectedLocale=.
- NATO (2024), "Sweden Officially Joins NATO", 07.03.2024, Erişim Tarihi: 18.10.2026, Erişim Adresi: https://www.nato.int/en/news-and-events/articles/news/2024/03/07/sweden-officially-joins-nato.
- Orenstein, Mitchell A. (2023), "The European Union's Transformation after Russia's Attack on Ukraine", *Journal of European Integration*, 45(3), ss. 333–342.
- Orenstein, Mitchell A. (2026), "Securitisation of EU Policy: How Russia's Invasion of Ukraine Is Changing Europe", *Journal of European Public Policy*, 33(7), ss. 1763–1784.
- Öniş, Ziya (2023), "Historic Missed Opportunities and Prospects for Renewal: Turkey-EU Relations in a Post-Western Order", *Turkish Studies,* 24(3-4), ss. 691–713.
- Pishchikova, Kateryna (2025), "European Identity Construction after the Russian Full-Scale Invasion of Ukraine: Dialogic (Re)Construction of Self and Others", *JCMS: Journal of Common Market Studies,* 63(5), ss. 1571–1593.

- Poutala, Tero & Sinkkonen, Elina & Mattlin, Mikael (2022), "EU Strategic Autonomy and the Perceived Challenge of China: Can Critical Hubs Be De-Weaponized?", *European Foreign Affairs Review*, 27(Special), ss. 79–98.
- Riddervold, Marianne & Newsome, Akasemi (2022), "Introduction: Out with the Old, in with the New? Explaining Changing EU–US Relations", *Politics and Governance,* 10(2), ss. 128–133.
- Schilde, Kaija (2023), "Weaponising Europe? Rule-Makers and Rule-Takers in the EU Regulatory Security State", *Journal of European Public Policy,* 30(7), ss. 1255–1280.
- Schmitz, Luuk & Seidl, Timo (2023), "As Open as Possible, as Autonomous as Necessary: Understanding the Rise of Open Strategic Autonomy in EU Trade Policy", *JCMS: Journal of Common Market Studies,* 61(3), ss. 834–852.
- Schulte-Cloos, Julia & Dražanová, Lenka (2026), "Shelter from the Storm: External Threat, Social Identity, and Support for the EU", *European Union Politics,* 27(3), ss. 444–467.
- Siddi, Marco (2023), "Europe's Energy Dilemma: War and the Green Transition", *Current History,* 122(842), ss. 83–88.
- Smith, Julianne (2026), "Russia's Hybrid War Has Entered a Dangerous New Phase - and the West Has Done Far Too Little to Deter It", *Foreign Affairs*, 07.10.2026, Erişim Tarihi: 23.10.2026, Erişim Adresi: https://www.foreignaffairs.com/russia/russias-hybrid-war-has-entered-dangerous-new-phase.
- Snyder, Glenn H. (1984), "The Security Dilemma in Alliance Politics", *World Politics,* 36(4), ss. 461–495.
- Sperling, James & Webber, Mark (2019), "The European Union: Security Governance and Collective Securitisation", *West European Politics*, 42(2), ss. 228–260.
- Steiner, Nils D. & Berlinschi, Ruxanda & Farvaque, Etienne & Fidrmuc, Jan & Harms, Philipp & Mihailov, Alexander & Neugart, Michael & Stanek, Piotr (2023). "Rallying around the EU Flag: Russia's Invasion of Ukraine and Attitudes toward European Integration", *JCMS: Journal of Common Market Studies*, 61(2), ss. 283–301.
- Sus, Monika (2024), "Exploring the Dynamics of Policy Change in EU Security and Defence: Policy Entrepreneurs Behind the Strategic Compass", *West European Politics*, 47*(*4), ss. 942–966.
- Sweeney, Simon & Winn, Neil (2022), "Understanding the Ambition in the EU's Strategic Compass: A Case for Optimism at Last?", *Defence Studies*, 22(2), ss. 192–210.
- The White House (2025), "National Security Strategy of the United States of America", Erişim Tarihi: 30.09.2026, Erişim Adresi: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.
- Tilly, Charles (1990), *Coercion, Capital, and European States, Ad 990-1992,* Cambridge, Massachusetts: Basil Blackwell.
- Tocci, Nathalie (2017), "From the European Security Strategy to the EU Global Strategy: Explaining the Journey", *International Politics*, 54(4), ss. 487–502.

- Tothova, Linda & Clapp, Sebastian (2026), "EU Joint Defence Procurement", EPThinktank, Erişim Tarihi: 24.10.2026, Erişim Adresi: https://epthinktank.eu/2026/03/13/eu-joint-defence-procurement/.
- Truchlewski, Zbigniew & Oana, Ioana-Elena & Moise, Alexandru D. (2023), "A Missing Link? Maintaining Support for the European Polity after the Russian Invasion of Ukraine", *Journal of European Public Policy*, 30(8), ss. 1662–1678.
- Verstraete, Wannes (2026), "Dissuasion Avancée: Macron's Realistic Complement to Nato Nuclear Deterrence", Egmont Royal Institute for International Relations Vrije Universiteit Brussel, Erişim Tarihi: 19.09.2026, Erişim Adresi: https://cris.vub.be/ws/portalfiles/portal/224454951/Wannes-Verstraete_Policy_Brief_403.pdf, ss. 1–5.
- Wigell, Mikael (2021), "Democratic Deterrence: How to Dissuade Hybrid Interference", *The Washington Quarterly*, 44(1), ss. 49–67.
- Willett, Marcus (2022), "The Cyber Dimension of the Russia–Ukraine War", *Survival,* 64(5), ss. 7–26.

TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARI[1]

Prof. Dr. Ozan ÖRMECİ[2]

Öz: Bu çalışma, Türkiye'nin siber güvenlik politikalarının 2013-2028 döneminde geçirdiği kurumsal ve hukuki dönüşümü, ulusal güvenlik ve siber dayanıklılık perspektifinden incelemektedir. Araştırmanın temel sorusu, Türkiye'nin siber güvenlik alanında geliştirdiği strateji, kurum ve mevzuatın kritik altyapıların korunması, kurumsal koordinasyon, caydırıcılık ve uluslararası iş birliği bakımından nasıl bir politika modeli ortaya koyduğudur. Çalışmada nitel doküman analizi yöntemi kullanılmış; ulusal strateji belgeleri, mevzuat, kurumların görev tanımları ve konuya ilişkin akademik çalışmalar amaçlı örnekleme yoluyla değerlendirilmiştir. Analiz, Türkiye'nin 2025 yılında Siber Güvenlik Başkanlığı'nın kurulması ve 7545 sayılı Siber Güvenlik Kanunu'nun kabulüyle merkezi koordinasyonu güçlendiren yeni bir kurumsal aşamaya geçtiğini göstermektedir. Bununla birlikte, kurumlar arası görev paylaşımı, uygulama kapasitesi, kritik altyapılarda ölçülebilir dayanıklılık, nitelikli insan kaynağı ve yerli teknolojilerin sürdürülebilirliği bakımından politika hedefleri ile uygulama sonuçları arasında değerlendirilmesi gereken alanlar bulunmaktadır. Çalışmanın özgün katkısı, Türkiye'nin siber güvenlik mimarisini yalnızca kurum ve mevzuat envanteri olarak sunmak yerine, güvenliğin genişlemesi ve siber caydırıcılık yaklaşımları çerçevesinde koordinasyon, kapasite ve dış iş birliği eksenlerinde değerlendirmesidir.

Anahtar Kelimeler: *Siber Güvenlik, Türkiye, Siber Caydırıcılık, Kritik Altyapılar, Siber Güvenlik Başkanlığı*.

Makale Geliş Tarihi: 28.10.2026

Makale Kabul Tarihi: 11.11.2026

DOI: 10.5281/zenodo.24254394

[1] Bu çalışmanın bazı bölümleri şu önceki çalışmadan özetlenmiştir; Ozan Örmeci & Eren Alper Yılmaz & Ahmet Emre Köker (2022), "Turkey's Cyber Security Policies", içinde *Cyber Environment and International Politics* (editörler: Hasret Çomak & Burak Şakir Şeker & Yaprak Civelek & Çağla Arslan Bozkuş), Londra: TPLondon, ss. 67-91.

[2] Siyaset Bilimi Profesörü, Uluslararası Politika Akademisi (UPA) Genel Koordinatörü, ESUPA (Elektronik Sanat ve Uluslararası Politika Enstitüsü) Başkanı.
Email: ozanormeci@gmail.com.
ORCID: 0000-0001-8850-6089.

TÜRKİYE'S CYBERSECURITY POLICIES

Abstract: This study examines the institutional and legal transformation of Türkiye's cybersecurity policies during 2013–2028 from the perspectives of national security and cyber resilience. It asks how Türkiye's strategies, institutions and legislation constitute a policy model in terms of critical infrastructure protection, institutional coordination, deterrence and international cooperation. The study employs qualitative document analysis, examining national strategy documents, legislation, institutional mandates and relevant academic studies selected through purposive sampling. The analysis indicates that the establishment of the Cybersecurity Presidency in 2025 and the adoption of Cybersecurity Law No. 7545 marked a new phase aimed at strengthening central coordination. Nevertheless, the relationship between policy objectives and implementation outcomes requires further assessment in areas such as inter-agency responsibilities, implementation capacity, measurable resilience of critical infrastructure, skilled human resources and the sustainability of domestic technologies. The study's contribution is to assess Türkiye's cybersecurity architecture not merely as an inventory of institutions and legislation, but through the analytical dimensions of coordination, capacity and external cooperation, informed by the expansion of security and cyber deterrence approaches.

Keywords: *Cybersecurity, Türkiye, Cyber Deterrence, Critical Infrastructure, Cybersecurity Presidency*.

Giriş

İnternet teknolojilerinin ve sosyal medyanın gelişmesiyle birlikte, son 30 yılda tüm sektörlerin ve yaşamın çeşitli alanlarının daha çok internet tabanlı veya çevrimiçi hale geldiği yadsınamaz bir gerçektir. Son Covid-19 (koronavirüs) pandemisi sırasında, çevrimiçi eğitim sistemlerinin hızla yayılması ve e-ticaretin patlamasıyla birlikte, internetin yoğun etkileri daha da belirgin hale geldi. İnternetin hayatı kolaylaştırdığı ve daha konforlu hale getirdiği şüphesizdir. Bu teknoloji, kişisel özgürlükleri önemli ölçüde arttırmıştır. Ancak, kötü niyetli, suçlu kişiler, terör örgütleri ve düşman devletler de internet özgürlüklerinden faydalanmaktadır. Bu nedenle, siber güvenlik son 20 yılda tüm devletler için büyük bir mesele haline gelmiştir. Gelişmekte olan bir ülke olarak, Türkiye de bu konuda istisna değildir ve bu nedenle internetin doğasında var olan koşullara uyum sağlamaya çalışmaktadır.

1990'ların başlarından itibaren, küreselleşme sürecinde bilgi kavramı büyük bir rol oynamıştır. Gelişmiş ülkelerde bilgi ve iletişim teknolojilerinin hızla yayılması ve devletlere yönelik tehditlere ilişkin yeni algılar nedeniyle "*güvenlik*" kavramı yeniden tanımlanmıştır. Organize suç, insan kaçakçılığı, yasadışı göç, kara para aklama vb. suç eylemleri uluslararası sistemin dengesini bozmuş ve devletler için yeni düşmanlar ortaya çıkmıştır. Özellikle 11 Eylül 2001 (9/11) felaketinden sonra artan gerilim, "*Dijital Felaket*" senaryolarına yol açmış ve Batı'ya karşı siber terörizm (siber terör) eylemleri korkusunu yaratmıştır. Son yıllarda, IŞİD/DEAŞ benzeri köktendinci terör örgütlerinin ortaya çıkışı da siber terörizm olgusuyla aynı zamana denk gelmiş ve bu tarz radikal örgütlerin faaliyetlerinde interneti özgürce kullanabilmeleri eleştirilere neden olmuştur.

Bu çalışma, Türkiye'nin siber güvenlik politikalarını ulusal güvenlik ve siber dayanıklılık bağlamında incelemektedir. Araştırmanın temel sorusu şudur: Türkiye'nin strateji belgeleri, kurumsal yapılanması ve mevzuatı; kritik altyapıların korunması, kurumlar arası koordinasyon, siber caydırıcılık ve uluslararası iş birliği bakımından ne ölçüde tutarlı ve işlevsel bir politika çerçevesi oluşturmaktadır? Bu soruya bağlı olarak, çalışma, Türkiye'de siber güvenlik yönetişiminin 2013-2028 dönemindeki gelişimini ve özellikle 2025 yılında ortaya çıkan kurumsal-hukuki dönüşümü değerlendirmeyi amaçlamaktadır. Araştırmanın kapsamı ulusal strateji belgeleri, ilgili mevzuat, Siber Güvenlik Başkanlığı ve diğer kamu kurumlarının görevleri ile NATO ve uluslararası iş birliği boyutlarıyla sınırlıdır. Yöntem olarak nitel doküman analizi

benimsenmiştir. Belgeler; (i) kurumsal yetki ve koordinasyon, (ii) kritik altyapıların korunması ve olaylara müdahale, (iii) caydırıcılık ve savunma kapasitesi, (iv) insan kaynağı ve yerli teknoloji, (v) uluslararası iş birliği ölçütleri üzerinden tematik olarak değerlendirilmiştir. Resmî belgeler politika hedeflerini ve hukuki yetki dağılımını; akademik çalışmalar ise bu hedeflerin kavramsal ve analitik bağlamını anlamak amacıyla kullanılmıştır. Kamuya açık performans verilerinin sınırlılığı nedeniyle, çalışma, kurumların operasyonel başarısına ilişkin ölçülmemiş nicel sonuçlar ileri sürmemekte; politika tasarımı ve kurumsal kapasite üzerinden nitel bir değerlendirme sunmaktadır.

Bu yaklaşımın literatüre katkısı, Türkiye örneğini yalnızca tarihsel gelişmelerin ve kurumların sıralandığı betimleyici bir anlatı olarak değil, güvenlik politikalarının genişlemesiyle ortaya çıkan yeni tehditlere verilen kurumsal yanıtın tutarlılığı üzerinden ele almasıdır. Güvenliğin genişlemesi yaklaşımı, siber alanın yalnızca teknik bir mesele olmadığını; ekonomik düzen, kamu hizmetleri, askerî kapasite, bireysel haklar ve siyasal istikrarla doğrudan ilişkili olduğunu göstermektedir. Siber caydırıcılık literatürü ise, saldırganın kimliğinin tespiti, misillemenin inandırıcılığı, savunma kapasitesi ve orantılılık gibi sorunların siber alanda caydırıcılığı güçleştirdiğine işaret etmektedir. Bu iki yaklaşım, aşağıdaki Türkiye incelemesinde analitik ölçütler olarak kullanılacaktır.

1. 'Siber' Kavramları

"*Siber*" (*Cyber*) terimi, genel olarak internet ve sanal ortamı olarak tanımlanan bilgisayarları, bilgisayar ağlarını ve bunlarla ilgili şeyleri ifade eder.[3] Ancak bu terim, literatürde sıklıkla "*siber uzay"* (*cyber space*) terimiyle eşanlamlı olarak kullanılmaktadır.Birleşmiş Milletler (BM), siber alanı "*genel olarak ağ olarak bilinen, internete bağlı bilgisayarların, iletişim altyapılarının, çevrimiçi konferans kuruluşlarının, veri tabanlarının ve bilgi hizmetlerinin küresel sistemler sistemi*" olarak tanımlar.[4] Bu, çoğunlukla internet anlamına gelir, ancak terim aynı zamanda bir ordunun, bir şirketin ve/veya bir hükümetin belirli ve sınırlı elektronik bilgi ortamını belirtmek için de kullanılabilir.[5]

Singer ve Friedman, siber uzay için temel bir tanım olarak, "*bilgisayarlardan füzelere ve güneşten*

[3] Merriam-Webster, "Cyber", Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.merriam-webster.com/dictionary/cyber.
[4] UNTerm, "Cyber space", Erişim Tarihi: 04.10.2026, Erişim Adresi: https://unterm.un.org/unterm2/en/.
[5] Jason Andress & Steve Winterfield (2014), *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham, MA: Elsevier Inc., s. 4.

gelen ışınlara kadar elektronik ve elektromanyetik spektrumun kullanımının karakterize ettiği alan" ifadesini kullanmışlardır.[6] Başka bir tanıma göre ise, siber uzay, "*dünyanın ve uzayın tamamına yayılmış bilgi sistemlerinden, bu sistemleri birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamdır*."[7] Öte yandan, ABD Ordusu'nun Siber Uzay Operasyonlarına İlişkin Ulusal Askeri Stratejisi, siber uzayı "*elektronik ve elektromanyetik spektrumun ağ üzerinden veri depolamak, değiştirmek ve alışverişi yapmak için kullanıldığı alan*" olarak tanımlar.[8]

Siber uzay, fiziksel ve sanal olmak üzere iki bileşik yapıdan oluşur. Fiziksel yapı, her türlü bilgi ve iletişim sistemini içerir. Bunlar arasında dijital elektronik cihazlar, bilgisayarlar, akıllı telefonlar, akıllı nesneler, sensörler/dedektörler, uydu sistemleri ve tüm bilgisayar ağları yer almaktadır. Sanal yapı ise, özellikle fiziksel ortamdaki işletim sistemleri olmak üzere, yazılım ve kodlarla üretilen, depolanan, iletilen ve çeşitli amaçlar için kullanılan her türlü veri ve bilgiyi içerir.[9]

Siber uzayın karmaşıklığını anlayabilmek için, öncelikle, iki ayrı uygulama alanını birbirinden ayırarak başlayalım. İlk olarak, halkın günlük faaliyetlerine hizmet eden ve genellikle devlet dışı aktörlerin hedefi olan ticari interneti ele alalım. Bu alanın kırılganlığı, sırasıyla Nisan-Mayıs 2007 ve Ağustos 2008'de Estonya ve Gürcistan'da gerçekleşen siber saldırılarla ortaya çıktı. İkincisi, askeri ağlar ve diğer devletlerin güvenliğini tehdit edebilecek şekilde önem kazandı. Son 20 yılda, çeşitli devletlerin orduları, ağ merkezli savaş yoluyla savaş yeteneklerini geliştirmeye çalıştı. Örneğin, Carafano ve Sayers'a göre, Amerika Birleşik Devletleri'ne askeri olarak daha zayıf olan Çin Halk Cumhuriyeti (Çin) ve Rusya Federasyonu (Rusya) gibi devletler, ABD siber alanının kırılganlığını tespit etmiş ve casusluk yoluyla elde edilen askeri bilgilerden yararlanmak için ayrıntılı çalışmalar yürütmüştür.[10]

---

[6] P. W. Singer & Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford: Oxford University Press, s. 13.
[7] Republic of Turkey Ministry of Transport Maritime Affairs, and Communications, *2016-2019 National Cyber Security Strategy,* Erişim Tarihi: 04.10.2026, Erişim Adresi: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusalsibereng.pdf, s. 7.
[8] Jason Andress & Steve Winterfield (2014), *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, s. 3.
[9] Mustafa Şenol (2020), "Türkiye'nin Ulusal Siber Güvenlik Strateji ve Politikalarının Olusturulması Çerçevesinde Caydırıcılık", Doktora Tezi, İstanbul Teknik Üniversitesi, İstanbul, Türkiye, s. 9.
[10] James Carafano & Eric Sayers (2008), "Building Cyber Security Leadership for the 21st Century", The Heritage Foundation, 16.12.2008, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.heritage.org/defense/report/building-cyber-security-leadership-the-21st-century.

1.1. Siber Güvenlik

Siber güvenlik (*cyber security*), kurumların, kuruluşların ve kullanıcıların siber ortamdaki güvenlik risklerine karşı koyabilecek şekilde güvenlik özelliklerini oluşturmayı ve sürdürmeyi amaçlar. Bu tanım, personelini, altyapılarını, uygulamalarını, hizmetlerini, elektronik iletişim sistemlerini ve kurumların, kuruluşların ve kullanıcıların siber ortamında iletilen ve depolanan tüm bilgileri içerir.[11] Türkiye'nin 2016-2019 Ulusal Siber Güvenlik Stratejisi'ne göre, siber güvenlik, "*siber uzayı oluşturan bilgi sistemlerinin saldırılardan korunması, bu ortamda işlenen bilgi/verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, karşı önlem mekanizmalarının devreye sokulması ve sistemlerin siber güvenlik olayından önceki duruma geri döndürülmesi*" anlamına gelmektedir.[12]

Siber güvenliğin temel ilkeleri, ülkeleri siber risklere ve tehditlere karşı korumak için bilgi güvenliğinin özünü oluşturur. "*CIA üçgeni*" olarak bilinen gizlilik, bütünlük ve erişilebilirlik ilkelerinin herhangi birine zarar verilirse, güvenlik tehlikeye girer. Veriye ilişkin bu üç temel ilkeye zarar verildiğinde, bilgi sistemlerini içeren altyapılar can kaybına, büyük ölçekli ekonomik kayıplara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına neden olabilir.[13]

1.2. Siber Caydırıcılık

Genel olarak, caydırıcılığı (*deterrence*), "*diğerlerini düşmanca eylemlerde bulunmaktan caydırmak*" olarak açıklayan Libicki, siber caydırıcılığı (*cyber deterrence*) ise "*siber ortamda saldırganın eylemini cezalandırarak ve bir tür tehdit oluşturarak saldırganı siber saldırıdan caydırmak*" olarak tanımlar.[14]

Cezalandırıcı önlemler, düşmanın siber saldırganlığın maliyetlerinin faydalarından daha ağır basıp basmadığına dair hesaplamalarına katkıda bulunur. Iasiello'nun görüşüne göre, "*siber caydırıcılık, savunma yapan bir devletin, düşmanın karar alma mekanizmasını hedef alarak ve etkileyerek, ilk saldırganın daha büyük bir misillemeden korkması nedeniyle yıkıcı siber faaliyetlerde bulunmaktan kaçınmasını sağlayarak, düşmanca siber faaliyetleri caydırma niyetini işaret ederek*

[11] M. Emin Ulaşanoğlu & Ramazan Yılmaz & M. Alper Tekin (2010), *Bilgi Güvenliği: Riskler ve Öneriler*, Ankara: Bilgi Teknolojileri ve İletişim Kurumu (BTK), s. 8.
[12] Republic of Turkey Ministry of Transport Maritime Affairs, and Communications, *2016-2019 National Cyber Security Strategy,* Erişim Tarihi: 04.10.2026, Erişim Adresi: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusalsibereng.pdf, s. 10.
[13] *A.g.e.*, s. 9.
[14] Martin C. Libicki (2009), *Cyber Deterrence and Cyberwar*, California: RAND Corporation, s. 28.

statükoyu korumaya çalıştığı bir stratejidir."[15]

Siber caydırıcılık, başarılı caydırıcılık sonuçlarına ulaşmak için uygulanması gereken birçok tekniği içerdiğinden, uygulanması oldukça zordur. Bir siber caydırıcılık stratejisinin, işleyişini sağlayan bazı temel parametrelere sahip olması gerekir.Bu parametreler olmadan, saldırgan savunmacının niyetini alıp işleyemez; bu nedenle devletler yanlış anlama veya yanlış yorumlama riskleriyle karşı karşıya kalabilir. Bu parametreler; iletişim, sinyal verme, atıf ve orantılılıktır.[16]

1.3. Siber Suç

Uluslararası bir sorun gibi görünen siber suç, genel olarak şu şekilde anlaşılmaktadır: "*Bilgilerin otomatik olarak işlenmesini içeren ve bilgisayarlar aracılığıyla veri aktarımı hakkındaki kanuna aykırılık teşkil eden eylemler*."[17] 2002 yılında, Suçun Önlenmesi ve Suçluların Islahı konulu Onuncu Birleşmiş Milletler Kongresi'nde, bu durum, "*bilgi sistemi güvenliğini/veri işlemlerini hedef alan ve bilgi sistemi/ağı aracılığıyla gerçekleştirilen yasadışı eylemler*" olarak tanımlanmıştır.[18]

Siber suç, suçluların hırsızlık yapmak veya başka türlü yasa dışı faaliyetlerde bulunmak için dijital araçları kullanması olarak da tanımlanır. En yaygın siber suç türü, kimlik bilgilerinin çalınması veya hesap bilgilerinin finansal ve ödeme sistemlerini dolandırmak için kötüye kullanılmasıdır. Bu sistemler arasında kredi kartları, ATM hesapları ve çevrimiçi bankacılık hesapları yer almaktadır.[19] Avrupa Konseyi Siber Suçlar Sözleşmesi (2004), yetkisiz erişim, sistemik müdahale ve dolandırıcılık suçlarına ek olarak, yaygın bilgi ve internet sistemlerini kullanan çocuk pornografisi ve telif hakkı ihlalleri gibi niceliksel olarak artan eylemlerin de siber suç kapsamına dahil olduğunu belirlemiştir.[20]

1.4. Siber Terörizm/Siber Terör

Günümüzün modern terör örgütleri, örgütlerini yapılandırmak, personel temin etmek ve eylemlerini

[15] Emilio Iasiello (2014), "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security*, 7(1), Bahar 2014, s. 55.
[16] *A.g.e.*, ss. 56-59.
[17] Hüseyin Çakır & M. Serkan Kılıç (2014), *Güncel Tehdit Siber Suçlar*, Ankara: Seçkin Yayınları, s. 50.
[18] Oğuzhan Turhan (2006), "Bilgisayar Ağları İle İlgili Suçlar", Planlama Uzmanlığı Tezi, DPT Müsteşarlığı, Ankara, Türkiye, s. 30.
[19] P. W. Singer & Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, s. 85.
[20] Mehmet Yayla (2014), "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", *Hacettepe Hukuk Fakültesi Dergisi*, 4(2), s. 190.

organize etmek için bilgi teknolojilerini yaygın olarak kullanmaktadır. Bu tarz yapılar, kirli amaçlarına ulaşmak için, kamu ve özel kurumların bilgi sistemlerine karşı siber saldırılar düzenlemektedir. Özellikle 2000'li yıllarda yoğunlaşan siber terörizm (*cyber terrorism*) eylemleri, kilit kurumları hedef alarak gizli bilgi ve para akışını sağlamayı amaçlamaktadır. Yayla, siber terörizmi genel olarak şu şekilde tanımlar: "*Siyasi veya sosyal hedefleri gerçekleştirmek, devletleri ve vatandaşlarını tehdit etmek, devletleri politikalarını değiştirmeye zorlamak amacıyla bilgi teknolojisi olanaklarını kullanarak bilgisayarlara, ağ sistemlerine ve veri tabanlarına yönelik yasadışı tehditler ve zarar verici saldırılar*."[21] Amerikan Federal Soruşturma Bürosu (FBI) ise, siber terörizmi "*ulusal altı gruplar veya gizli ajanlar tarafından, savaşçı olmayan hedeflere karşı şiddete yol açan, bilgiye, bilgisayar sistemlerine, bilgisayar programlarına ve verilere yönelik önceden planlanmış, siyasi amaçlı bir saldırı*" olarak tanımlar.[22] Bu değerlendirme, yasadışı ve zarar verici saldırıları da içermektedir.

Jalil, siber terörizmi aşağıdaki kategoriler altında analiz etmektedir:[23]

Saldırı: Siber teröristlerin bu tarz eylemlerdeki temel amacı, bir ağa erişerek bilgi edinmek veya sistemdeki bilgileri değiştirerek karşı tarafa karşı avantaj sağlamaktır. Bu yöntem, çok yaygın ve yüksek başarı oranıyla geniş çapta kullanılmaktadır.

Yıkım: Buradaki asıl amaç, bilgisayar sistemlerini yok etmek veya zarar vermektir. Bu tür bir saldırının sonuçları korkunç olabilir; kuruluşlar büyük zarar görebilir. Saldırıların şiddeti nedeniyle belirsiz bir süre boyunca operasyonlardan uzak kalmak zorunda bile kalınabilir.

Dezenformasyon: Buradaki amaç, söylentiler yayarak ve bilgileri kirleterek devlet içinde korku ve kaos ortamı yaratmaktır. Bu tür saldırıları kontrol etmek çok zordur; çünkü hedefteki bilgisayar ve ağ sistemlerine erişime gerek kalmadan neredeyse anında gerçekleştirilebilir.

1.5. Siber Savaş

Siber savaş (*cyberwarfare*), temel olarak "*bir devletin başka bir devletin bilgisayar sistemlerine ve ağlarına sızarak zarar verme veya aksamaya neden olma eylemi*" anlamına gelir.[24] Bu tanıma

[21] *A.g.e.*, s. 195.
[22] P. W. Singer & Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, s. 96.
[23] Shamsuddin Abdul Jalil (2003), "Countering Cyber Terrorism Effectively: Are We Ready to Rumble?", GIAC, Haziran 2003, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154, s. 8.
[24] Richard A. Clark & Robert K. Knake (2011), *Siber Savaş*, Çeviri: Murat Erduran, İstanbul: İstanbul Kültür

göre, siber savaş, devletler arasında siber uzayda gerçekleşir. Buna göre, Steven A. Hildreth tarafından 2001 yılında hazırlanan bir kongre raporuna göre, siber savaş, "*bilgisayar ağlarını siber uzaydaki saldırılardan korumak ve düşmanın gelecekte aynı saldırıyı başlatma yeteneğini engellemek için çok çeşitli unsurları*" içerir.[25]

Siber savaş, devletler veya devlet destekli gruplar tarafından yürütülen simetrik veya asimetrik, saldırgan veya savunma amaçlı dijital ağ faaliyetleridir. Bu faaliyetler, siber ağlarda aksamalara yol açar. Hedef, ülkedeki kritik ulusal altyapıları, askeri sistemleri ve/veya ciddi endüstriyel yapıları tehdit etmektir. Siber savaş olgusu, son yıllarda Rusya ve Çin tarafından desteklenen bilgisayar korsanlarının Ukrayna da dahil olmak üzere diğer bazı Batılı ülkelere saldırılar düzenlediğine dair raporlarla birlikte gündeme gelmiştir. Hatta Birleşik Krallık'ta bile, İngiliz Ordusu'nun kötü amaçlı yazılımları askeri bir araç olarak kullanmanın yollarını araştırdığı bildirilmiştir.[26]

2. Soğuk Savaş Sonrası Güvenlik Algısı/Perspektifinde Değişim: Soğuk Savaş Sonrası Dönemde Güvenlik Perspektifindeki Değişim

Soğuk Savaş döneminde silah temelli güvenlik stratejileri ve "*dehşet dengesi*" gibi kavramlar ön planda yer aldı. İki büyük blok (Batı bloku: ABD; Doğu bloku: Sovyetler Birliği) tarafından şekillendirilen uluslararası sistem, büyük güç rekabeti ve nükleer karşılıklı bağımlılık tarafından belirleniyordu. Karşılıklı güvence altına alınmış yıkım (*mutually assured destruction*) düşüncesi, doğrudan büyük ölçekli bir ABD-Sovyet savaşı riskini sınırlarken, vekâlet savaşlarını ise ortadan kaldırmadı. Nitekim bu yıllarda, "*nükleer denge*"nin yarattığı büyük varoluşsal risk, iç ve dış politikalarda durgun bir istikrarı koruyordu.[27] Burada, karşılıklı olarak güvence altına alınmış yıkımı sağlamak amacıyla "*terör/dehşet dengesi*" stratejisi izlenmiştir. Neticede, Soğuk Savaş, büyük ölçekli dünya savaşlarının ortaya çıkmasını engellemede başarılı oldu, ancak ABD ile diğer ülkeler arasında vekalet savaşları yoluyla küçük ölçekli başka savaşlar yaşandı. Sonunda, Sovyetler Birliği'nin dağılması ve Soğuk Savaş'ın sona ermesiyle, 1990'ların başındaki birleşmeyle dünya bambaşka bir yer haline geldi.

1989'da Berlin Duvarı'nın yıkılması, 3 Ekim 1990'da Almanya'nın yeniden birleşmesi ve Aralık

Üniversitesi Yayınları, s. 8.

[25] Steven A. Hildreth (2001), "Cyberwarfare", CRS Report for Congress, 19.06.2001, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-014.pdf.

[26] Jane McCallion (2022), "What is cyber warfare?", ITPro, 20.05.2022, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.itpro.com/security/28170/what-is-cyber-warfare.

[27] Ali Karaosmanoğlu (2015), "Savunma Planlaması ve Stratejik Belirsizlik", *Bilge Strateji,* 7(12), ss. 23-45.

1991'de Sovyetler Birliği'nin dağılması, birbirleriyle bağlantılı ancak farklı tarihsel süreçlerdi. Soğuk Savaş'ın sona ermesiyle uluslararası sistemin güç dengeleri ve güvenlik gündemi dönüşmüş; devlet dışı aktörler, ekonomik karşılıklı bağımlılık ve bilgi-iletişim teknolojileri güvenlik analizlerinde daha görünür hale gelmiştir.

Yeni paradigma, başlangıçta tek kutuplu dünya sistemi gibi görünse de, ABD'nin bile dünyayı kontrol edemeyeceği kısa sürede anlaşıldı. Dolayısıyla, 21. yüzyılın ayırt edici özelliği, giderek artan çok kutupluluk eğilimleri oldu. 21. yüzyılın yeni dünya düzeni, ABD ve Rusya'nın giderek güç kaybetmesiyle birlikte, Çin'in hızlı yükselişi ve 27 Avrupa ülkesi arasında güçlü bir birliğin oluşması gibi yeni parametrelerle şekillendi. Ancak daha da önemlisi, teknolojik dönüşüm sayesinde, dünyamız, 1990'lardan bu yana çok değişti. Bilgisayarlar, internet teknolojileri, cep telefonları, uzaktan sistemler, dronlar ve sosyal medya, 21. yüzyılın başlarında sıradan özellikler haline geldi. 21. yüzyılın teknolojik ilerlemesi sayesinde, bu teknolojiler ve platformlar insanlar için daha rahat bir yaşam yaratırken, aynı zamanda bireyler, şirketler ve devletler için yeni riskler de doğurdu.

Bu dönüşüm, güvenliğin yalnızca askerî tehditlere indirgenemeyeceğini ortaya koymuştur. Kopenhag Okulu'nun güvenlikleştirme yaklaşımı bakımından siber tehditler; devletin egemenliği, ekonomik süreklilik, toplumsal düzen ve bireysel mahremiyet gibi farklı referans nesnelerini etkileyebilmektedir. Bununla birlikte, her teknik arıza veya suç faaliyeti doğrudan ulusal güvenlik tehdidi olarak nitelendirilmemelidir. Tehdidin ölçeği, etkisi, faili, hedef aldığı altyapının kritik niteliği ve kamu düzeni üzerindeki sonuçları birlikte değerlendirilmelidir. Bu ayrım, siber suç, siber casusluk, siber saldırı ve silahlı çatışma bağlamındaki siber operasyonların birbirine karıştırılmasını önlemek açısından önemlidir. Türkiye'nin politikaları da bu nedenle yalnızca savunma tedbirleriyle değil, tehdit sınıflandırması, kurumsal görev paylaşımı ve demokratik-hukuki denetim boyutlarıyla ele alınmalıdır.

1990'ların başından beri, bilgi, siyasi araçlar açısından önemi nedeniyle Uluslararası İlişkiler disiplininde de kilit bir rol oynamaktadır. Bilgi ve iletişim teknolojileri, günümüzde sanayileşmiş devletlerin birçok alanında baskın konumdadır.[28] Güvenliğin derinleşmesi ve genişlemesi, temelde güvenlik tehditlerinin çoğalmasıyla ilgilidir. Bu bağlamda, güvenlik, küreselleşme ve teknoloji

[28] Myriam Dunn Cavelty (2010), "Cyber Security", içinde (editör: J. Peter Burgess) *The Routledge Handbook of New Security Studies*, New York: Taylor & Francis Group, s. 159.

arasındaki ilişkiyi incelemek gereklidir. Küreselleşme ve teknolojinin yarattığı sınırların geçirgenliği ve akışkanlık, bireylere ve devlete yönelik tehditlerin sayısını da arttırmıştır.[29] 1990'lardan bu yana, küreselleşme olgusunun hızlanmasıyla birlikte, çok hızlı ve kaçınılmaz bir değişim süreci başlamıştır. Küreselleşme, güvenlik tehditlerinin farklılaşmasını o kadar kapsamlı bir şekilde çoğaltmıştır ki, güvenlik kavramının kendisinin yeniden değerlendirilmesi gerekmektedir. Organize suç, yasadışı göç, insan kaçakçılığı, uyuşturucu/silah kaçakçılığı ve kara para aklama gibi yeni tehditler, büyük uluslararası istikrarsızlaştırıcılar olarak ortaya çıkmıştır. Bu nedenle, geleneksel tehdit algıları ve bu unsurlarla mücadele yöntemleri, bu yeni tehlikelerle mücadelede yetersiz kalmıştır. Bu yetersizlik, yeni bir güvenlik tanımının yanı sıra, yeterli bir yanıt uygulamak için yeni araçlar gerektirmiştir.[30] Siber saldırıların artan oranı, ulus devletleri veya uluslararası aktörleri bu alanda hızla çalışmaya yöneltmiştir. Temel kritik altyapıların ve siber güvenliğin geliştirilmesi, ulusal çıkarlar için hayati önem taşımaktadır. Bu nedenle, her aktör, siber savaşa sadece savunma için değil, aynı zamanda saldırı yetenekleri oluşturmak için de önem vermeye başlamıştır. Son gelişmeler, siber savaşların 21. yüzyılda da bir gerçeklik olarak kalacağını göstermektedir.[31]

3. 11 Eylül Sonrası Siber Saldırılar ve Siber Güvenlik Girişimleri

Soğuk Savaş'tan sonra, küresel güvenlik ortamını derinden etkileyen ve şekillendiren en önemli olay, 11 Eylül 2001'deki ABD'ye yönelik terör saldırılarıydı. 11 Eylül'den önce, siber uzayın riskleri ve güvenlik sorunları yalnızca küçük bir uzman grubu tarafından tartışılan konular arasındaydı. O günden beri ise, siber dünya, birbirine giderek daha fazla bağımlı hale gelen toplumlar için ciddi riskler yaratmıştır. 11 Eylül'de El Kaide saldırılarıyla İkiz Kuleler'e giren uçaklar, Washington DC ve uluslararası sistemdeki güvenlik, tehditler ve gündem tanımlarını tamamen değiştirdi. Bu saldırılar sonucunda, Soğuk Savaş'tan sonra nispeten belirsizleşen ulusal güvenlik kavramı, birçok ülkenin öncelik listesinde yeniden en üst sıraya yerleşti. Terörle mücadele veya Başkan Bush'un ifadesiyle "*teröre karşı savaş*", yalnızca saldırılara maruz kalan ülkelerin hükümetlerinin değil, sistemdeki neredeyse tüm aktörlerin gündemine girdi ve ABD'nin

[29] Muharrem Aksu & Faruk Turhan (2012), "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik", *Uluslararası Alanya İşletme Fakültesi Dergisi*, 4(2), s. 71.
[30] Bilal Karabulut (2015), *Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek*, Ankara: Barış Kitabevi, s. 119.
[31] Ayhan Gücüyener (2016), "21. Yüzyılda 'Siber' Rekabet: Yeni Hedef Kritik Altyapılar mı?", Linkedin, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.linkedin.com/pulse/21-y%C3%BCzy%C4%B1lda-siber-rekabet-yeni-hedef-kritik-m%C4%B1-ayhan-gucuyener/.

liderliğinde hızla ivme kazandı.

Enkazın üzerindeki tozlar yatıştıktan hemen sonra, saldırıları gerçekleştiren teröristlerin internet üzerinden kendi aralarında iletişim kurdukları ve daha önce bu uçaklarla simülasyon çalışmaları yaptıkları anlaşıldı. Bu açıklama, internetin terörizm için kullanılabileceği fikrini güçlendirdi.[32] Örneğin, 11 Eylül (9/11) saldırganlarının hepsinin Hotmail hesapları vardı ve bu hesapları haberleşmek için kullandıkları düşünülüyordu. Ayrıca araştırmalar sonucu anlaşıldı ki, teröristler, El Kaide lideri Usame bin Ladin'in yardımcılarından birinin kayınbiraderi tarafından yönetilen bir internet sitesinin ziyaretçi defteri bölümüne bırakılan notlar aracılığıyla koordinasyon sağlamıştı.[33]

11 Eylül (9/11) sonrası yüksek gerilim döneminde, uluslararası arenada en çok tartışılan konulardan biri, varsayımsal olarak NATO üyesi ülkelerden birini felç edecek olan "*Dijital Felaket*" senaryosuydu. Terörist grupların siber saldırı olasılığı, olası bir "*Dijital Pearl Harbor*" beklentisini arttırdı. Ulus devletlerin ekonomik ve diğer kritik altyapılarının, siber sistemlerine yönelik saldırılar sonucunda yok edilebileceği düşünülüyordu.[34] Bu tür endişeler ulusal güvenlikle yakından ilişkili olduğundan, birçok ülke siber güvenlik stratejilerini ulusal güvenlik belgelerine eklemiş ve bunları düzenli olarak güncellemiştir. Örneğin, Siber Güvenlik Yasası, ABD'de 13 Kasım 2001'de kabul edildi. Bu durum, polisin mahkeme kararı olmaksızın telefon dinlemesi yapmasına veya elektronik gözetim kullanmasına olanak sağladı. Bu bağlamda, Savunma Bakanlığı tarafından terörizmle mücadele için geliştirilen "*Toplam Bilgi Farkındalığı*" (*Total Information Awareness*) planı, ülke genelinde uygulamaya konuldu.[35]

2007 yılında Estonya'ya yönelik siber saldırılar, Soğuk Savaş sonrası artan siber tehdidin açık bir örneğiydi. Sovyetler Birliği'nin çöküşünün ardından Rusya ve Estonya arasında sürekli bir gerginlik yaşandı. Estonya yetkililerinin 26 Nisan 2007'de Tallinn'deki bir meydandan Bronz Asker adlı Sovyet savaş anıtını kaldırmasıyla, bu iki ülke arasındaki ilişkiler iyice gerildi. Bu süreçte, büyük bir Rus azınlığı barındıran Estonya, üç hafta boyunca yoğun siber saldırılara maruz kaldı. Saldırılar, Estonya Cumhurbaşkanlığı ve parlamentosunu, siyasi partileri, devletin tüm

[32] Timothy L. Thomas (2003), "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters*, 33(1), s. 120.
[33] P. W. Singer & Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, s. 101.
[34] Lene Hansen & Helen Nissenbaum (2009), "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly,* 53(4), s. 1160.
[35] TUİÇ (2017), "Gözetim Politikaları ve Terörizm: 11 Eylül 2001", 04.01.2017, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.tuicakademi.org/gozetim-politikalari-terorizm-11-eylul-2001/.

Bakanlıklarını, ülkenin en ünlü üç medya kuruluşunu, en büyük bankasını ve iletişim şirketlerini hedef aldı. Siber saldırılar, Avrupa'nın en güçlü kablolu yayın ağına ve en üst düzey e-devlet uygulamasına sahip olan Estonya'da hayatı durma noktasına getirdi. Olay, NATO veya Avrupa Birliği (AB) tarafından "*siber savaş*" olarak nitelendirilmemiş; bunun yerine "*siber saldırı*" eylemleri olarak sınıflandırılmıştır. Önemli maddi hasar veya insanlara zarar verilmemesi nedeniyle, bu olay doğrudan bir savaş eylemi olarak kabul edilmemiştir. Bu bağlamda, yapanları belirlemenin zor olduğu siber saldırıları açık bir askeri eylem olarak tanımlamanın zor olduğu da açıkça belirtilmiştir.[36] Bu saldırının ardından, NATO ve Estonya arasında NATO İşbirliğine Dayalı Siber Savunma Mükemmeliyet Merkezi kurulmuştur.

Dahası, 2008 yılında Rusya ve Gürcistan arasındaki karşılıklı siyasi krizin bir sonucu olarak, Rusya, bu yıl içerisinde Gürcistan'a karşı bir siber saldırı başlattı. Rus siber savaşı, Gürcistan'ın hükümet web sitelerine ve ülkenin birçok ticari web sitesine karşı da kullanıldı. Bu sabotaj, interneti birkaç gün boyunca devre dışı bıraktı ve hatta elektrik kesintilerine yol açtı. Ancak Gürcistan'ın internet ağları çok gelişmiş olmadığı için siber saldırılar Estonya'da yaşanan kadar büyük hasara yol açmadı.

Yakın tarihte, muazzam bir etki yaratan bir başka büyük siber saldırı daha yaşandı. Stuxnet saldırısı adı verilen sabotaj eylemini, ABD, 2009 yılında İran'ın nükleer santrallerine yönelik olarak gerçekleştirdi. ABD yetkilileri saldırıların sorumluluğunu üstlenmese de, siyasi ve istihbari analizler ABD'nin bu olayda mutlak bir rolü olduğunu ortaya koydu.[37] Saldırı, 2010 yılında tespit edildi. İran'ın zenginleştirilmiş uranyum tesislerinde bir yıl içinde değiştirilen santrifüjlerin yüzde 10'unun doluluk oranına ulaşması, sistemde bir sorun olduğunu ortaya koydu. Bir yıllık bir çalışma, santrifüjlerdeki değişikliklerin aslında bir bilgisayar arızasından kaynaklandığını kanıtladı. Program o kadar güçlüydü ki, 100.000'den fazla bilgisayara bağlantı sağlıyordu.[38]

Son yıllarda, köktendinci terör örgütleri de sıklıkla siber yöntemler kullanmaktadır. Örneğin, IŞİD/DEAŞ terör örgütü, 2015 yılında ABD Merkez Komutanlığı'nın (CENTCOM) resmi Twitter

[36] James P. Farwell & Rafal Rohozinski (2011), "Stuxnet and the Future of Cyber War", *Survival,* 53(1), s. 32.
[37] Şener Çelik (2014), "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 15(1), s. 144.
[38] Kim Zetter (2011), "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History", *Wired*, 11.07.2011, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

ve YouTube hesaplarına siber saldırı düzenledi. Korsanlar, ele geçirdikleri hesaplardan şu mesajı paylaştılar: "*Amerikan askerleri, geliyoruz, arkanızı kollayın. Kişisel telefonlarınızı ve ailelerinizi biliyoruz*."[39] İddialara göre, bu saldırıları, kendilerine Siber Halifelik adını veren IŞİD bağlantılı bir grup organize etti. ABD medyasına göre, saldırı, IŞİD'in en başarılı bilgisayar sihirbazı olarak tanımlanan İngiliz bilgisayar korsanı Junaid Hussein (Abu Hussein El Britani) tarafından organize edildi.[40] Dahası, 2015 yılında, Fransa'da, IŞİD/DEAŞ, programları dünya çapında 200'den fazla ülkede yayınlanan küresel yayın kuruluşu *TV5 Monde*'a bir siber saldırı düzenledi. Kanalın internet sitelerini ele geçiren bilgisayar korsanları, Facebook ve Twitter hesapları, "*Siber cihatçılar*" adı altında "*Ben IŞİD'im*" mesajını yayınladı. Mesajlarında, teröristler, ayrıca, Fransa Cumhurbaşkanı François Hollande ve Fransız Ordusu'nu da tehdit ettiler.[41]

2019'da Sri Lanka'da IŞİD/DEAŞ tarafından gerçekleştirilen bombalı saldırının Bitcoin ile finanse edilmesi ve teröristler ile sempatizanlarının örgüte Bitcoin aracılığıyla para transferi yapması, siber terörizmin internetteki tehlikeli boyutunu ortaya koymaktadır. IŞİD/DEAŞ, fiziksel dünyada büyük bir darbe almış olsa da, son birkaç yıldır siber alanda giderek daha aktif hale gelmiştir.[42]

4. Türkiye'de Siber Güvenlik

Türkiye'de 86 milyonluk toplam nüfusun yüzde 92-93'lük çok büyük bir kısmı internet kullanmaktadır.[43] İnternet ve bilgisayar kullanımının artması, diğer devletler gibi Türkiye'de de birçok siber güvenlik riskini de beraberinde getirmektedir. Bu güvenlik riskleri arasında kritik altyapıların güvenliği, gizliliğin ihlali, bilgi bütünlüğünün veya erişilebilirliğinin bozulması, büyük ölçekli ekonomik zararlar, ulusal güvenlik açıkları veya kamu düzeninin bozulması yer

[39] *Reuters* (2015), "Apparent Islamic State backers hack U.S. military Twitter feed", 13.01.2015, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.reuters.com/article/us-cybersecurity-centcom-hack-idUSKBN0KL1UZ20150112/.

[40] *The Guardian* (2015), "Briton lead suspect after US Central Command's Twitter account is hacked", 14.01.2015, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.theguardian.com/us-news/2015/jan/14/briton-suspect-us-central-command-twitter-hack-junaid-hussain-tony-blair.

[4141] Ozan Örmeci & Eren Alper Yılmaz & Ahmet Emre Köker (2022), "Turkey's Cyber Security Policies", içinde (editörler: Hasret Çomak & Burak Şakir Şeker & Yaprak Civelek & Çağla Arslan Bozkuş) *Cyber Environment and International Politics*, Londra: TPLondon, s. 76.

[42] Emine Çelik (2019), "Siber Terörizm ve IŞİD-Bitcoin İlişkisi", *Ortadoğu Analiz*, 10(89), ss. 90-91.

[43] *Anadolu Ajansı* (2026), "Türkiye'de internet kullananların oranı bu yıl yüzde 92,3'e yükseldi", 05.09.2026, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.aa.com.tr/tr/bilim-teknoloji/turkiyede-internet-kullananlarin-orani-bu-yil-yuzde-92-3e-yukseldi/4018733.

almaktadır. Öte yandan, Türkiye'de mobil cihazların artması ve "*nesnelerin interneti*"nin gelişmesiyle birlikte tüm süreçlerin işleyişi siber alana girmiştir. Bu nedenle, siber alanın bu beklenmedik genişlemesi, onu her türlü saldırıya karşı savunmasız hale getirmiştir.

4.1. Türkiye'deki Siber Güvenlik Kurumları

Türkiye'de siber alanın kontrolü ve yönetimiyle ilgili temel kurum T.C. Cumhurbaşkanlığı'na bağlı olarak 2025 yılında kurulan Siber Güvenlik Başkanlığı'dır.[44] Siber Güvenlik Başkanlığı, Türkiye'nin siber uzaydaki millî güvenliğini ve dijital egemenliğini sağlamak amacıyla Cumhurbaşkanlığı'na bağlı olarak kurulan en üst düzey yetkili merciidir. 8 Ocak 2025 tarihinde 177 sayılı Cumhurbaşkanlığı kararnamesi ile kurulan kurum, halen Ümit Önal başkanlığında faaliyetlerine devam etmektedir.

4.1.1. Siber Güvenlik Başkanlığı

Resim 1. Siber Güvenlik Başkanlığı logosu

Kurum web sitesinden özetlemek gerekirse, T.C. Cumhurbaşkanlığı'na bağlı Siber Güvenlik Başkanlığı'nın temel görevleri şunlardır:

A-) Siber Güvenlik ve Tehdit Yönetimi

- ✓ **Politika ve Strateji Belirleme:** Siber Güvenlik Başkanlığı, ulusal siber güvenlik politika, strateji ve hedeflerini belirler, eylem planları hazırlar ve mevzuat çalışmalarını yürütür.
- ✓ **Kritik Altyapıların Korunması:** Siber Güvenlik Başkanlığı, kamu kurumlarının ve kritik

[44] T.C. Siber Güvenlik Başkanlığı, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://siberguvenlik.gov.tr/.

altyapıların siber tehditlere karşı korunması amacıyla izleme, analiz ve önleyici tedbir faaliyetlerini koordine eder.

- ✓ **Siber Tehdit İstihbaratı:** Siber Güvenlik Başkanlığı, siber tehdit aktörlerini ve küresel zafiyetleri takip ederek elde ettiği bulguları ilgili paydaşlarla paylaşır.
- ✓ **Olay Müdahale ve Koordinasyon:** Siber Güvenlik Başkanlığı, siber olayların tespiti, analizi ve müdahale kapasitesinin artırılması için ulusal düzeyde hazırlık seviyesini yükseltir. Siber Olaylara Müdahale Ekiplerinin (SOME) koordinasyonunu sağlar.
- ✓ **Denetim ve Gözetim:** Siber Güvenlik Başkanlığı, belirlenen standartların ve siber güvenlik düzenlemelerinin uygulanmasını denetler.

B-) Dijital Devlet ve Altyapı Güvenliği

- ✓ **E-Devlet Kapısı Yönetimi:** Siber Güvenlik Başkanlığı, E-Devlet altyapısının güvenli bir şekilde işletilmesini ve kamu hizmetlerinin kesintisiz sürdürülmesini sağlar.
- ✓ **Veri Güvenliği ve Bulut Stratejileri:** Siber Güvenlik Başkanlığı, Kamu Bulut Bilişim Stratejisi, Açık Devlet Verisi uygulamaları ve kamuda açık kaynak kodlu yazılım kullanımına yönelik standartları oluşturur.

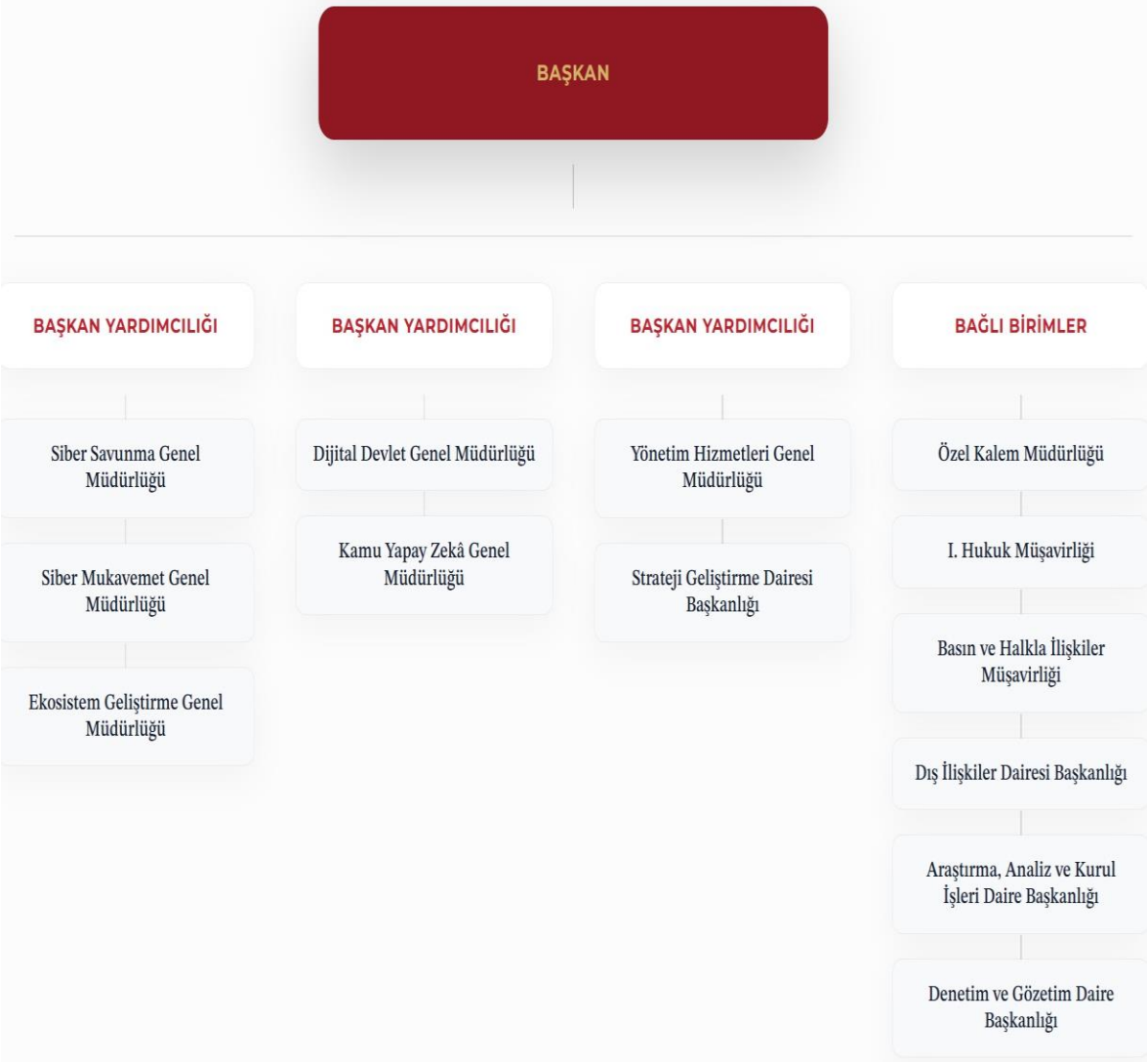
C-) Kamu Yapay Zekâsı ve Teknoloji Yönetimi

- ✓ **Güvenli Yapay Zekâ Kullanımı:** Siber Güvenlik Başkanlığı, kamuda yapay zekâ ve veri analitiği teknolojilerinin güvenli, sorumlu ve etik kurallara uygun olarak kullanılmasına yönelik düzenlemeler ve uygulamalar geliştirir.

Ç-) Ekosistem Geliştirme ve İş Birlikleri

- ✓ **Kapasite ve İnsan Kaynağı Geliştirme:** Siber Güvenlik Başkanlığı, Türkiye'nin ulusal siber güvenlik uzmanı ihtiyacını karşılamak üzere kapasite geliştirme süreçlerini ve personel istihdamını yönetir.
- ✓ **Ulusal ve Uluslararası İş Birliği:** Siber Güvenlik Başkanlığı, kamu, özel sektör, akademi ve uluslararası paydaşlar arasında bilgi paylaşım ağları kurarak siber güvenlik ekosistemini büyütür.

Resim 2. Siber Güvenlik Başkanlığı'nın kurumsal şeması



4.1.2. Diğer Kurumlar

Ancak yeni kurulan Siber Güvenlik Başkanlığı dışında da bu alanda faaliyet gösteren bazı önemli resmi kuruluşlar bulunmaktadır.

Resim 3. BTK logosu

Bilgi Teknolojileri ve İletişim Kurumu (BTK): BTK, Türkiye'de elektronik haberleşme, bilgi teknolojileri ve posta sektörlerini düzenleyen ve denetleyen bağımsız bir kamu otoritesidir. 2025 yılının başında T.C. Cumhurbaşkanlığı'na bağlı Siber Güvenlik Başkanlığı (SGB) kurulmadan önce, Türkiye'deki ulusal siber güvenlik süreçlerinin koordinasyonu ve operasyonel yönetimi ağırlıklı olarak Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yapılıyordu. SGB'nin kurulmasının ardından bu alandaki yetkilerini devreden BTK'nın şu andaki temel görev ve yetkileri şunlardır:

- ✓ **Sektörel Düzenleme ve Yetkilendirme:** Telekomünikasyon ve internet alanında faaliyet gösteren operatörlere ve işletmecilere lisans/yetki verir, pazar kurallarını belirler ve adil rekabeti korur.
- ✓ **Tüketici Hakları:** Abonelik sözleşmelerini, faturalandırma süreçlerini ve hizmet kalitesini denetler; tüketicilerden gelen şikâyetleri değerlendirir.
- ✓ **Frekans ve Altyapı Yönetimi:** Radyo frekanslarının tahsisini yapar, spektrum izleme ve yönetim faaliyetlerini yürütür.
- ✓ **IMEI Kayıt İşlemleri:** Cep telefonlarının kayıt altına alınması, IMEI sorgulama ve eşleştirme işlemlerini yönetir.
- ✓ **Alan Adı Yönetimi:** .tr uzantılı alan adlarının TRABİS sistemi üzerinden tahsis ve yönetim süreçlerini düzenler.

- ✓ **BTK Akademi:** 16 yaş ve üzeri herkese yazılım, siber güvenlik ve yapay zekâ gibi alanlarda ücretsiz çevrim içi eğitimler sunar.
- ✓ **Erişim Engelleme ve Güvenlik:** Güvenli internet hizmetlerini düzenler ve yasal mevzuat çerçevesinde internet sitelerine erişimin engellenmesi kararlarını uygular.

BTK USOM (Ulusal Siber Olaylara Müdahale Merkezi): Bilgi Teknolojileri ve İletişim Kurumu bünyesinde ülkenin siber güvenlik olaylarına müdahale ana merkezidir ve ulusal koordinasyonu yürütür. Temel görev ve faaliyetleri şöyledir:

- ✓ **Siber Tehdit İstihbaratı:** Ülke genelindeki siber saldırıları ve riskleri izler, zararlı bağlantıları (Zararlı Bağlantılar) raporlar.
- ✓ **Zafiyet Yönetimi:** Kritik altyapılardaki güvenlik açıklarını tespit ederek ilgili kurum ve kuruluşları uyarır.
- ✓ **SOME Koordinasyonu:** Kurumlar arası Siber Olaylara Müdahale Ekiplerinin (SOME) eş güdümünü sağlar ve SİP (SOME İletişim Platformu) üzerinden güvenli bilgi paylaşımı yürütür.
- ✓ **İhbar Süreçleri:** Vatandaşlardan ve kurumlardan gelen siber güvenlik ihbarlarını değerlendirir.

TÜBİTAK BİLGEM (Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi): Siber güvenlik ve kriptoloji alanında yerli Ar-Ge çözümleri ve ürünler (ör. Siper, Ulak) geliştiren temel araştırma merkezidir. BİLGEM, çatısı altında farklı uzmanlık alanlarına odaklanmış 6 stratejik enstitü barındırır:

1. **UEKAE:** Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü,
2. **BTE:** Bilişim Teknolojileri Enstitüsü,
3. **SGE:** Siber Güvenlik Enstitüsü,
4. **YTE:** Yazılım Teknolojileri Araştırma Enstitüsü,
5. **İLTAREN:** İleri Teknolojiler Araştırma Enstitüsü,
6. **YZE:** Yapay Zekâ Enstitüsü.

TSK Siber Savunma Komutanlığı: Türk Silahlı Kuvvetleri (TSK) bünyesindeki Siber Savunma Komutanlığı, TSK'nın dijital hudutlarını korumak ve askeri bilgi sistemlerinin güvenliğini sağlamakla görevlidir. Komutanlık, TSK Siber Savunma Merkezi (SİSAMER) aracılığıyla ülkede meydana gelen siber olaylara anında tepki vererek olası zararları ve kriz durumlarını en aza indirir. Ayrıca dışa bağımlılığı azaltmak amacıyla yerli ve milli siber güvenlik yazılımları geliştirir, entegre eder ve güncel tutar. Ek olarak, ulusal güvenliği hedef alan siber tehditleri önceden belirlemek için istihbarat ve güvenlik analizleri gerçekleştirir. Bunların yanı sıra, TSK'nın kritik iletişim altyapısını korumak ve savunma reflekslerini tek bir merkezden koordine etmekle yükümlüdür. Son olarak, yine SİSAMER'e bağlı Siber Savunma Harekât Merkezi aracılığıyla TSK ağlarına ve sistemlerine yönelik her türlü siber saldırıyı veya yetkisiz erişim girişimini kesintisiz takip eder.

Emniyet ve Jandarma Siber Suçlarla Mücadele Daire Başkanlıkları: Türkiye'deki temel yetkili kurum olan EGM Siber Suçlarla Mücadele Daire Başkanlığı'nın (ve Jandarma bünyesindeki muadilinin) ulusal çatı kuruluş olan T.C. Siber Güvenlik Başkanlığı'nın çalışmaları doğrultusunda belirlenen görev ve yetkileri şu şekildedir:

- Adli kolluk olarak doğrudan siber suçların tespiti, soruşturulması ve suçluların yakalanmasıyla görevlidirler.
- Bilişim sistemlerine hukuka aykırı girme (*hacking*), sistemleri engelleme/bozma, veri hırsızlığı, nitelikli internet dolandırıcılığı, yasadışı bahis ve siber zorbalık gibi suçları araştırırlar.
- Suç mahalli ya da şüphelilerden elde edilen bilgisayar, telefon, hard disk gibi bilişim sistemlerinde mahkeme kararıyla arama yapar, adli kopyalarını (imaj) alır, silinen verileri kurtarır ve raporlayarak adli makamlara sunarlar.
- İnternet ortamında açık kaynaklar üzerinden 7/24 önleyici izleme yapar; suç unsuru barındıran paylaşımları, siber tehditleri ve terör faaliyetlerini tespit ederler.
- Teknoloji bağımlılığı, güvenli internet kullanımı ve siber zorbalığa karşı toplumda farkındalık yaratmak amacıyla Siberay gibi projeler üzerinden eğitim ve bilgilendirme faaliyetleri yürütürler.
- Son olarak, sınır aşan siber suçlarla (uluslararası siber nitelikli dolandırıcılık gibi)

mücadele etmek için Europol, Interpol ve diğer ülkelerin siber polis birimleriyle ortak operasyonlar ve bilgi paylaşımı gerçekleştirirler.

Türkiye Siber Güvenlik Kümelenmesi: T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı öncülüğünde; kamu, özel sektör ve akademiyi bir araya getiren ekosistem platformudur.

Savunma ve Kamu Kaynaklı Şirketler: HAVELSAN, STM ve ASELSAN gibi kurumlar da ulusal siber savunma sistemleri ve operasyonel merkezler (SOC) kurmaktadır.

Kurumsal yapı bakımından temel mesele, kurumların sayısından çok görev ve sorumlulukların açık biçimde tanımlanması ve ortak bir müdahale zinciri içinde çalışabilmesidir. Siber Güvenlik Başkanlığı'nın strateji ve koordinasyon rolü ile BTK/USOM'un teknik izleme ve olay müdahalesi, kolluk birimlerinin adli soruşturma yetkileri, TÜBİTAK BİLGEM'in araştırma-geliştirme kapasitesi ve TSK'nın askerî ağlara ilişkin sorumlulukları birbirini tamamlayabilecek niteliktedir. Ancak bu çok aktörlü yapı, bilgi paylaşımında gecikme, mükerrer görevler veya kriz anında yetki belirsizliği risklerini de beraberinde getirebilir. Dolayısıyla, kurumsal etkinliğin değerlendirilmesinde ortak olay müdahale tatbikatları, bildirim süreleri, kritik altyapı sektörleriyle bilgi paylaşımı, personel yeterliliği ve olay sonrası öğrenme mekanizmaları gibi göstergeler önem taşımaktadır. Bu göstergelere ilişkin karşılaştırılabilir ve kamuya açık veriler bulunmadığı ölçüde, kurumsal kapasite ile fiilî performans arasında ayrım yapılmalıdır.

4.2. Ulusal Siber Güvenlik Stratejisi

Türkiye'nin ulusal siber güvenlik politikaları, en güncel olarak Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) çerçevesinde siber dayanıklılığı artırmayı ve yerli teknolojileri geliştirmeyi amaçlamaktadfir.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028), Türkiye'nin siber uzaydaki güvenliğini arttırmak, riskleri azaltmak ve yerli teknolojileri geliştirmek amacıyla 7 Eylül 2024 tarihli *Resmi Gazete* süreçleri sonrasında yürürlüğe girmiştir.

Temel Amaç ve Kapsam:

- Vizyon: Türkiye'nin siber dayanıklılığını en üst seviyeye çıkarmak ve uluslararası alanda güvenilir bir siber güvenlik ekosistemi oluşturmak.
- Koordinasyon: Çalışmalar Ulaştırma ve Altyapı Bakanlığı koordinasyonunda yürütülmektedir.

- Temel Yapı: Plan, 4 temel kavram (İnsan, Savunma, Caydırıcılık, İş Birliği) üzerine kurulmuştur.

Stratejik Bileşenler:

Belge, genel hatlarıyla şu ana unsurları içerir:

- 6 Stratejik Amaç: Siber dayanıklılık, proaktif siber savunma, insan odaklı yaklaşım, güvenli teknoloji kullanımı, yerli ve millî çözümler ile uluslararası iş birliği.
- 18 Hedef ve 61 Eylem Maddesi: Kritik altyapıların korunmasından siber farkındalığın artırılmasına kadar somut adımlar.
- İzleme ve Değerlendirme: Hedeflerin gerçekleşme oranları periyodik olarak raporlanmakta ve ilgili kamu kurum ile kuruluşlarının sorumlulukları takip edilmektedir.

4.3. Mevzuat

Türkiye'nin siber güvenlik alanındaki ana omurgasını, 19 Mart 2025 tarihinde yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu ve Cumhurbaşkanlığı bünyesinde kurulan T.C. Siber Güvenlik Başkanlığı Mevzuat rehberliği oluşturur.

Türkiye'deki siber güvenlik mevzuatı, başlıca şu temel kanun, kararname ve düzenlemelerden meydana gelir:

1. Ana Kanun ve Kurumsal Yapı:

- 7545 sayılı Siber Güvenlik Kanunu: Türkiye'nin siber uzaydaki milli gücünü korumak, siber güvenliği güçlendirmek ve Siber Güvenlik Başkanlığı ile Siber Güvenlik Kurulu'nu tesis eden temel ve bağlayıcı kanundur. Kamu kurumlarını, meslek örgütlerini, gerçek ve tüzel kişileri kapsar.
- Cumhurbaşkanlığı Kararnameleri: Siber Güvenlik Başkanlığı'nın teşkilat yapısını, görev, yetki ve sorumluluk alanlarını belirleyen ikincil üst düzey idari düzenlemeler.

2. Türk Ceza Kanunu (TCK) - Siber Suçlar:

- Madde 243 (Bilişim Sistemine Girme): Bir sisteme izinsiz girme veya kalma.
- Madde 244 (Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme): Bilişim sistemlerinin çalışmasını engelleme veya verileri bozma/silme.

- Madde 245 (Banka veya Kredi Kartlarının Kötüye Kullanılması): Kartların izinsiz kullanılması veya sahte üretilmesi.
- Madde 245/A (Yasak Cihaz veya Programlar): Siber saldırı araçlarının imal, ithal veya sevk edilmesi.

3. Bilgi ve İletişim Güvenliği Düzenlemeleri:

- Bilgi ve İletişim Güvenliği Rehberi: Kamu kurumları ve kritik altyapı işleten kritik sektörlerdeki firmalar için uyulması zorunlu teknik ve idari güvenlik standartlarını belirler.
- SOME (Siber Olaylara Müdahale Ekibi) Yönetmelikleri: Ulusal ve kurumsal düzeyde siber olay müdahale süreçlerini, koordinasyon esaslarını ve raporlama yükümlülüklerini düzenler.

4. Kişisel Verilerin Korunması ve Sektörel Mevzuat:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK): Kişisel verilerin hukuka aykırı işlenmesini önlemek ve veri güvenliğini sağlamak amacıyla veri sorumlularına teknik/idari tedbir alma zorunluluğu getirir.
- Sektörel Düzenlemeler: Bankacılık (BDDK düzenlemeleri), elektronik haberleşme (BTK yönetmelikleri) ve enerji piyasası gibi kritik altyapı sektörlerine özel siber güvenlik ve loglama standartları.

4.4. Türkiye'nin Siber Güvenlik Politikalarının Analitik Değerlendirmesi

Türkiye'nin siber güvenlik mimarisi, son 10 yılda strateji belgeleri, teknik müdahale birimleri ve mevzuat aracılığıyla aşamalı biçimde gelişmiş; 2025 yılında Siber Güvenlik Başkanlığı'nın kurulması ve 7545 sayılı Kanun'un kabul edilmesiyle daha merkezi bir yönetişim modeline yönelmiştir. Bu gelişme, siber güvenliğin yalnızca haberleşme ve bilişim sektörüne ait teknik bir konu olmaktan çıkarak ulusal güvenlik, kamu yönetimi ve dijital egemenlik başlıklarıyla birlikte ele alındığını göstermektedir. Bununla birlikte, merkezî koordinasyonun güçlendirilmesi tek başına etkili uygulamayı garanti etmez. Kurumların görev sınırlarının ikincil düzenlemelerle açıklığa kavuşturulması, bütçe ve uzman personel kapasitesinin sürdürülebilirliği ve kamu-özel sektör arasında güvenilir bilgi paylaşımının sağlanması gerekmektedir.

Kritik altyapıların korunması, politikanın başarısını sınayacak temel alanlardan biridir. Enerji,

finans, ulaştırma, sağlık, elektronik haberleşme ve kamu hizmetleri gibi sektörlerde dijital sistemlerin birbirine bağımlılığı, tek bir kurumda ortaya çıkan güvenlik açığının sektörler arası sonuçlar doğurabilmesine yol açmaktadır. Bu nedenle, yalnızca saldırıların önlenmesi değil, hizmetlerin kesinti sırasında sürdürülebilmesi, yedekleme ve kurtarma kapasitesi, tedarik zinciri güvenliği ve düzenli tatbikatlar da siber dayanıklılığın parçası olarak görülmelidir. Mevcut metinde sıralanan kurum ve mevzuat, bu hedefler için bir yönetişim zemini sunmaktadır; ancak etkinliğin kanıtlanması için sektör bazlı risk değerlendirmeleri ve ölçülebilir performans göstergelerinin düzenli yayımlanması gereklidir.

Siber caydırıcılık açısından Türkiye'nin karşı karşıya olduğu temel güçlükler, siber saldırıların kaynağını yüksek kesinlikle tespit etmenin (atıf) zorluğu, saldırıların farklı aktörler üzerinden yürütülebilmesi ve verilecek karşılığın hukuki-siyasi sınırlarıdır. Bu nedenle, caydırıcılık, yalnızca misilleme kapasitesine indirgenmemelidir. Güçlü savunma, hızlı toparlanma, saldırıların maliyetini artıran ulusal ve uluslararası koordinasyon, kamuoyuna doğru ve zamanında bilgilendirme ve hukuka uygun karşılık seçenekleri birlikte düşünülmelidir. Bu yaklaşım, siber saldırıların her durumda silahlı saldırı veya savaş eylemi sayılmaması gerektiği yönündeki uluslararası hukuk tartışmalarıyla da uyumludur.

Uluslararası iş birliği, Türkiye'nin NATO üyeliği ve sınır aşan siber tehditlerin niteliği nedeniyle ayrıca önem taşımaktadır. Siber olayların ulusal sınırları aşması, tehdit istihbaratının paylaşılmasını, ortak tatbikatları, teknik standartların uyumlaştırılmasını ve adli makamlar arasında iş birliğini gerekli kılmaktadır. NATO'nun siber savunmayı kolektif savunma ve dayanıklılık gündeminin parçası olarak ele alması, Türkiye açısından askerî ağların korunmasının yanı sıra sivil kritik altyapıların dayanıklılığı ve müttefiklerle birlikte çalışabilirlik bakımından da önemlidir. Bununla birlikte, uluslararası iş birliği ulusal kapasitenin ikamesi değildir; yerli araştırma-geliştirme, nitelikli insan kaynağı ve güvenilir tedarik zinciriyle desteklenmelidir.

Yerli siber güvenlik teknolojilerinin geliştirilmesi, dışa bağımlılığı azaltma ve stratejik özerklik açısından önemlidir. Ancak yerlilik tek başına güvenlik veya kalite göstergesi değildir. Ürünlerin bağımsız güvenlik testlerinden geçirilmesi, güncel tutulması, uluslararası standartlarla uyumlu olması ve yaşam döngüsü boyunca desteklenmesi gerekir. Benzer biçimde, uzman personel yetiştirme politikaları yalnızca kısa süreli eğitim programlarıyla sınırlı kalmamalı; üniversiteler, kamu kurumları ve özel sektör arasında sürdürülebilir araştırma ve istihdam kanalları

oluşturulmalıdır.

Son olarak, siber güvenlik politikalarının uygulanması temel haklar ve hukukun üstünlüğü ilkeleriyle birlikte değerlendirilmelidir. Güvenlik amacıyla alınan tedbirlerin kişisel verilerin korunması, ifade özgürlüğü, haberleşmenin gizliliği ve etkili başvuru yolları üzerindeki etkileri açık ve ölçülü olmalıdır. Bu çerçevede 7545 sayılı Kanun'un uygulaması, yetki ve denetim mekanizmalarının açıklığı ile idari işlemlere karşı hukuki güvenceler bakımından da izlenmelidir. Böylece siber güvenlik, yalnızca teknik kapasite veya devletin müdahale gücü olarak değil, demokratik meşruiyet ve toplumsal güven üreten bir kamu politikası olarak ele alınabilir.

Sonuç

2000'li yıllarda dijitalleşmenin hızlanmasıyla birlikte Türkiye'ye yönelik siber saldırılarda da artış yaşandı. Bu artış, yasal ve kurumsal önlemlerin alınmasını zorunlu kıldı. Bu bağlamda, daha önce yayımlanan Ulusal Siber Güvenlik Stratejisi, 2013-2014 Eylem Planı ve 2016-2019 Ulusal Siber Güvenlik Stratejileri, Türkiye'nin siber alanda nasıl hareket ettiğine katkıda bulunmuştur. Türkiye, 29 Aralık 2020 tarihinde 2020-2023 dönemini kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nı belirlemiştir. Yakın zamanda ise, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) kabul edilmiştir. Daha da önemlisi, önceden BTK'nın ilgilendiği siber güvenlik konusunu tek öncelikli işi yapan Siber Güvenlik Başkanlığı, 2025 yılı başlarında faaliyetlerine başlamıştır. Böylece, Türkiye, siber güvenliğini sağlamak için proaktif bir rol üstlenmeye ve gerekli mevzuat ve kurumları oluşturmaya başlamıştır.

Kilit kurumlar arasında koordineli politikalara rağmen, Türkiye, halen zaman zaman siber güvenlik alanında etkili bir oyuncu olarak ortaya çıkmakta zorlanmaktadır. Bu tarz siber saldırıları azaltabilmek için, Türkiye'nin, komşuları ve diğer devletlerle siyasi sorunlarını çözerek daha barışçıl ilişkiler kurmaya ve yine kendi içerisinde toplumsallaşan siyasi sorunları çözmek için yeni stratejiler uygulayarak militan grupların tehdidini etkisiz hale getirmeye çalışması akılcı olacaktır. Zira günümüzde hiçbir devlet kendi başına yüzde yüz korunaklı değildir; bu konuda uluslararası iş birliği ve uluslararası hukukun geliştirilmesi şarttır. Bu konuda da Birleşmiş Milletler'in ve üye devletlerin öncü rol üstlenmesi gerekmektedir.

KAYNAKÇA

- Aksu, Muharrem & Turhan, Faruk (2012), "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik", *Uluslararası Alanya İşletme Fakültesi Dergisi*, 4(2), ss. 69-80.
- *Anadolu Ajansı* (2026), "Türkiye'de internet kullananların oranı bu yıl yüzde 92,3'e yükseldi", 05.09.2026, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.aa.com.tr/tr/bilim-teknoloji/turkiyede-internet-kullananlarin-orani-bu-yil-yuzde-92-3e-yukseldi/4018733.
- Andress, Jason & Winterfield, Steve (2014), *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* Waltham, MA: Elsevier Inc.
- Carafano, James & Sayers, Eric (2008), "Building Cyber Security Leadership for the 21st Century", The Heritage Foundation, 16.12.2008, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.heritage.org/defense/report/building-cyber-security-leadership-the-21st-century.
- Cavelty, Myriam Dunn (2010), "Cyber Security", içinde (editör: J. Peter Burgess) *The Routledge Handbook of New Security Studies,* New York: Taylor & Francis Group, ss. 154-162.
- Clark, Richard A. & Knake, Robert K. (2011), *Siber Savaş*, Çeviri: Murat Erduran, İstanbul: İstanbul Kültür Üniversitesi Yayınları.
- Çakır, Hüseyin & Kılıç, M. Serkan (2014), *Güncel Tehdit Siber Suçlar,* Ankara: Seçkin Yayınları.
- Çelik, Emine (2019), "Siber Terörizm ve IŞİD-Bitcoin İlişkisi", *Ortadoğu Analiz*, 10(89), ss. 86-89.
- Çelik, Şener (2014), "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* 15(1), ss. 137-175.
- Farwell, James P. & Rohozinski, Rafal (2011), "Stuxnet and the Future of Cyber War", *Survival,* 53(1), ss. 23-40.
- Gücüyener, Ayhan (2016), "21. Yüzyılda 'Siber' Rekabet: Yeni Hedef Kritik Altyapılar mı?", Linkedin, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.linkedin.com/pulse/21-y%C3%BCzy%C4%B1lda-siber-rekabet-yeni-hedef-kritik-m%C4%B1-ayhan-gucuyener/.
- Hansen, Lene & Nissenbaum, Helen (2009), "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly,* 53(4), ss. 1155-1175.
- Hildreth, Steven A. (2001), "Cyberwarfare", CRS Report for Congress, 19.06.2001, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-014.pdf.
- Iasiello, Emilio (2014), "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security,* 7(1), Bahar 2014, ss. 54-67.
- Jalil, Shamsuddin Abdul (2003), "Countering Cyber Terrorism Effectively: Are We Ready to Rumble?", GIAC, Haziran 2003, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154.
- Karabulut, Bilal (2015), *Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden*

Düşünmek, Ankara: Barış Kitabevi.

- Karaosmanoğlu, Ali (2015), "Savunma Planlaması ve Stratejik Belirsizlik", *Bilge Strateji,* 7(12), ss. 23-45.

- Libicki, Martin C. (2009), *Cyber Deterrence and Cyberwar*, California: RAND Corporation.

- McCallion, Jane (2022), "What is cyber warfare?", ITPro, 20.05.2022, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.itpro.com/security/28170/what-is-cyber-warfare.

- Merriam-Webster, "Cyber", Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.merriam-webster.com/dictionary/cyber.

- Örmeci, Ozan & Yılmaz, Eren Alper & Köker, Ahmet Emre (2022), "Turkey's Cyber Security Policies", içinde (editörler: Hasret Çomak & Burak Şakir Şeker & Yaprak Civelek & Çağla Arslan Bozkuş) *Cyber Environment and International Politics,* Londra: TPLondon, ss. 67-91.

- Republic of Turkey Ministry of Transport Maritime Affairs, and Communications, *2016-2019 National Cyber Security Strategy,* Erişim Tarihi: 04.10.2026, Erişim Adresi: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusalsibereng.pdf.

- *Reuters* (2015), "Apparent Islamic State backers hack U.S. military Twitter feed", 13.01.2015, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.reuters.com/article/us-cybersecurity-centcom-hack-idUSKBN0KL1UZ20150112/.

- Singer, P. W. & Friedman, Allan (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know,* Oxford: Oxford University Press.

- Şenol, Mustafa (2020), "Türkiye'nin Ulusal Siber Güvenlik Strateji ve Politikalarının Olusturulması Çerçevesinde Caydırıcılık", Doktora Tezi, İstanbul Teknik Üniversitesi, İstanbul, Türkiye.

- T.C. Siber Güvenlik Başkanlığı, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://siberguvenlik.gov.tr/.

- *The Guardian* (2015), "Briton lead suspect after US Central Command's Twitter account is hacked", 14.01.2015, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.theguardian.com/us-news/2015/jan/14/briton-suspect-us-central-command-twitter-hack-junaid-hussain-tony-blair.

- Thomas, Timothy L. (2003), "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters,* 33(1), ss. 114-122.

- TUİÇ (2017), "Gözetim Politikaları ve Terörizm: 11 Eylül 2001", 04.01.2017, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.tuicakademi.org/gozetim-politikalari-terorizm-11-eylul-2001/.

- Turhan, Oğuzhan (2006), "Bilgisayar Ağları İle İlgili Suçlar", Planlama Uzmanlığı Tezi, DPT Müsteşarlığı, Ankara, Türkiye.

- Ulaşanoğlu, M. Emin & Yılmaz, Ramazan & Tekin, M. Alper (2010), *Bilgi Güvenliği: Riskler ve Öneriler*, Ankara: Bilgi Teknolojileri ve İletişim Kurumu (BTK).

- UNTerm, "Cyber space", Erişim Tarihi: 04.10.2026, Erişim Adresi: https://unterm.un.org/unterm2/en/.
- Yayla, Mehmet (2014), "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", *Hacettepe Hukuk Fakültesi Dergisi*, 4(2), ss. 181-200.
- Zetter, Kim (2011), "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History", *Wired*, 11.07.2011, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

MULTIDIMENSIONAL HUMAN SECURITY AMONG OLDER MUSLIM MIGRANTS IN EUROPE: VULNERABILITY, DISCRIMINATION AND PROTECTION

Cemal YILMAZ[1]

Abstract: This article examines multidimensional human security among older Muslim migrants in Europe through an integrated framework connecting ageing, migration history, religious identity and institutional protection. Drawing on human security theory and intersectionality, the study addresses the limitations of approaches that examine discrimination, socioeconomic vulnerability, healthcare inequalities and institutional representation separately. Methodologically, it combines a critical integrative literature review, conceptual analysis and historically contextualised documentary examination. The article proposes five interconnected dimensions of human security: physical security; psychosocial security; health and care security; housing and economic security; and cultural, religious and institutional security. The analysis suggests that insecurity is shaped not by ageing, migration background or religious identity alone, but by interactions between individual circumstances, structural inequalities and access to protective resources. Particular attention is devoted to institutional representation, examined through the historical experiences of the Turkish-Islamic Elderly Union (Turks-Islamitische Ouderen Bond, TISBO, founded in 1993) and the Netherlands Islamic Elderly Union (NISBO, founded in 1995) in the Netherlands. These cases illustrate how migrant organisations sought to address housing needs, facilitate access to welfare services and strengthen collective representation, while also highlighting questions of institutional effectiveness and sustainability. The article contributes a population-sensitive conceptual framework in which institutional protection operates both as a distinct security dimension and as a cross-cutting mechanism.

Keywords: *Human security, Older Muslim migrants, Ageing and migration, Intersectional age discrimination, Institutional protection.*

Makale Geliş Tarihi: 30.10.2026

Makale Kabul Tarihi: 16.11.2026

[1] Dr., Independent Researcher.
Email: gerostudies@gmail.com.
ORCID: https://orcid.org/0000-0002-6315-9372.

AVRUPA'DAKİ YAŞLI MÜSLÜMAN GÖÇMENLER ARASINDA ÇOK BOYUTLU İNSAN GÜVENLİĞİ: KIRILGANLIK, AYRIMCILIK VE KORUMA

Öz: Bu makale, yaşlanma, göç geçmişi, dini kimlik ve kurumsal korumayı birbirine bağlayan bütünleşik bir çerçeve aracılığıyla Avrupa'daki yaşlı Müslüman göçmenler arasında çok boyutlu insan güvenliğini inceliyor. İnsan güvenliği teorisi ve kesişimsellikten yararlanan çalışma, ayrımcılığı, sosyoekonomik kırılganlığı, sağlık hizmetlerindeki eşitsizlikleri ve kurumsal temsili ayrı ayrı inceleyen yaklaşımların sınırlılıklarını ele alıyor. Metodolojik olarak, eleştirel bütünleştirici bir literatür taraması, kavramsal analiz ve tarihsel bağlamda belgesel incelemeyi birleştiriyor. Makale, insan güvenliğinin beş birbirine bağlı boyutunu öneriyor: fiziksel güvenlik; psikososyal güvenlik; sağlık ve bakım güvenliği; barınma ve ekonomik güvenlik; ve kültürel, dini ve kurumsal güvenlik. Analiz, güvensizliğin yalnızca yaşlanma, göç geçmişi veya dini kimlik tarafından değil, bireysel koşullar, yapısal eşitsizlikler ve koruyucu kaynaklara erişim arasındaki etkileşimler tarafından şekillendirildiğini öne sürüyor. Bu çalışmada, özellikle Hollanda'daki Türk-İslam Yaşlılar Sendikası (TISBO, 1993) ve Hollanda İslam Yaşlılar Sendikasının (NISBO, 1995) tarihsel deneyimleri üzerinden kurumsal temsile özel önem verilmektedir. Bu örnekler, göçmen örgütlerinin konut ihtiyaçlarını karşılama, sosyal hizmetlere erişimi kolaylaştırma ve kolektif temsili güçlendirme çabalarını gösterirken, kurumsal etkinlik ve sürdürülebilirlik konularını da vurgulamaktadır. Makale, kurumsal korumanın hem ayrı bir güvenlik boyutu hem de kesişen bir mekanizma olarak işlev gördüğü, nüfusa duyarlı kavramsal bir çerçeve sunmaktadır.

Anahtar Kelimeler: *İnsan güvenliği, Yaşlı Müslüman göçmenler, Yaşlanma ve göç, Kesişimsel yaş ayrımcılığı, Kurumsal koruma.*

DOI: 10.5281/zenodo.24281733

Introduction

Human security provides a people-centred framework for examining threats to well-being, dignity and fundamental rights beyond conventional concerns with state and territorial security. The United Nations Development Programme identified seven interconnected dimensions of human security[2], while United Nations General Assembly Resolution 66/290 subsequently emphasised its comprehensive, context-specific and prevention-oriented character.[3] This perspective is particularly relevant to populations whose security is shaped by overlapping social, economic, health-related and institutional conditions.

Population ageing and international migration have created new challenges for European welfare systems. Migrants who arrived during earlier periods of labour recruitment and family reunification are increasingly entering later life, often with circumstances shaped by employment histories, socioeconomic resources, language proficiency, family relationships and access to public services.[4] These conditions vary considerably between individuals and communities, requiring approaches that recognise diversity rather than treating older migrants as a homogeneous vulnerable population. Older Muslim migrants represent a particularly relevant population for examining the intersection of ageing, migration history, religious identity and institutional protection. Their experiences may reflect both challenges associated with later life and inequalities linked to ethnic or religious minority status. However, Muslim identity does not necessarily imply shared cultural practices, socioeconomic circumstances or experiences of discrimination. Understanding insecurity therefore requires attention to individual differences and the institutional contexts in which ageing occurs.[5]

European research demonstrates the broader significance of discrimination affecting Muslim populations. The European Union Agency for Fundamental Rights, drawing on a survey of 9,604 Muslims in thirteen EU Member States, reported that 47 per cent had experienced racial

[2] UNDP (1994), *Human Development Report 1994*, New York: UNDP (United Nations Development Programme), Date of Accession: 01.09.2026 from https://hdr.undp.org/content/human-development-report-1994.
[3] UN General Assembly (2012), "Follow-up to Paragraph 143 on Human Security of the 2005 World Summit Outcome", A/RES/66/290, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/n11/476/22/pdf/n1147622.pdf.
[4] NISBO (1998), "Ontluikende diversiteit in het lokale ouderenbeleid, Een discussienotitie over knelpunten en oplossingsstrategieen", Rotterdam: Zenodo; WVC (1993), "Address by the Minister of Welfare, Health and Cultural Affairs, Ms. Hedy d'Ancona, at the national presentation meeting of the Turkish-Islamic Elderly Union (TISBO)", Zenodo.
[5] Cemal Yılmaz (2026), "The First European Housing Project for Older Turkish Migrants in Haarlem, the Netherlands, and Its Lasting Legacies (1993–2008)", SocArXiv, Date of Accession: 01.09.2026 from osf.io/preprints/socarxiv/fc4aq_v1.

discrimination during the preceding five years and 27 per cent had experienced racist harassment.[6] These findings establish an important context for examining minority-related insecurity, although the survey was not specifically designed to represent older Muslim migrants.

Age-related security concerns also extend to healthcare accessibility, long-term care, financial resources, housing conditions, social connectedness and the preservation of valued cultural and religious practices.[7] Research on older Turkish and Moroccan migrants in the Netherlands, for example, has examined healthcare utilisation across countries of residence and origin, demonstrating the importance of understanding service use within transnational and institutional contexts.[8] Such studies provide valuable evidence concerning specific aspects of migrant ageing but do not necessarily explain how different forms of insecurity interact. Existing scholarship on migrant ageing, healthcare inequalities, discrimination and social participation has frequently examined these issues through separate disciplinary perspectives. Although these contributions are valuable, a more integrated framework is needed to examine how age, migration background, religious identification and institutional conditions may jointly shape security in later life.

This article addresses that challenge by proposing five interrelated dimensions of human security among older Muslim migrants in Europe: physical security; psychosocial security; health and care security; housing and economic security; and cultural, religious and institutional security. Drawing on human security theory and intersectionality, the framework examines vulnerability and protection across individual, community and institutional levels. Particular attention is given to institutional representation as a potentially important mechanism of protection. The historical experiences of the Turkish-Islamic Elderly Union (Turks-Islamitische Ouderen Bond, TISBO)[9], founded in the Netherlands in 1993, and the Netherlands Islamic Elderly Union (Nederlandse Islamitische Bond voor Ouderen, NISBO)[10], founded in 1995,

---

[6] FRA (2024), *Being Muslim in the EU: Experiences of Muslims*, European Union Agency for Fundamental Rights, Date of Accession: 01.09.2026 from https://fra.europa.eu/en/publication/2024/being-muslim-eu?utm.
[7] Dirk Kloosterboer & Berna Yılmaz (1999), "NISBO Beleidsvisie: Een gemiste kans? Oudere migranten in het grotestedenbeleid", Rotterdam: Zenodo.
[8] Aydın Şekercan & Marieke B Snijder & RJG Peters & Karien Stronks (2018), "Gaat zorggebruik in het land van herkomst onder oudere Turkse en Marokkaanse migranten gepaard met minder zorggebruik in Nederland? Een combinatie van HELIUS-data met Achmea registratiedata", *Tijdschrift voor Gerontologie en Geriatrie*, 49(6), pp. 253–262.
[9] TISBO (1994), "Handleiding TISBO Afdelingen (1993-1996) - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond", Zenodo.
[10] NISBO (1995), *Founding Statutes of the Netherlands Islamic Elderly Union*, Amsterdam: Netherlands Islamic Elderly Union.

provide illustrative examples of collective efforts to address the needs of ageing migrant populations. These cases are examined as historically situated institutional experiences rather than representative models of migrant organisations throughout Europe.

The central research question is: How do ageing, migration background, religious identity and institutional conditions interact to shape multidimensional human security among older Muslim migrants in Europe, and what forms of protection can address their overlapping vulnerabilities?

Methodologically, the study combines a critical integrative literature review, conceptual analysis and historically contextualised documentary examination, drawing on established approaches to interdisciplinary evidence synthesis and qualitative document analysis.[11] It makes three contributions: developing a population-sensitive human security framework; integrating intersecting forms of vulnerability and protection; and identifying institutional representation as both a distinct security concern and a mechanism connecting the five dimensions.

The article thereby seeks to advance an integrated understanding of security in later migrant life and inform further research on inclusive ageing policies, equitable services and institutional protection.

1. Theoretical Framework: Human Security, Ageing and Intersectionality

1.1. Human Security as a People-Centred Concept

Human security shifts analytical attention from the protection of states and territories towards the safety, well-being and dignity of individuals. The United Nations Development Programme identified seven interconnected dimensions of human security: economic, food, health, environmental, personal, community and political security.[12] This framework extends the meaning of security beyond protection against violence to encompass the conditions necessary for human development and fundamental rights.

United Nations General Assembly Resolution 66/290 subsequently defined human security as a people-centred, comprehensive, context-specific and prevention-oriented approach. It emphasised the complementary principles of protection and empowerment, recognising the primary responsibility of governments alongside the contributions of individuals, communities

[11] Hannah Snyder (2019), "Literature review as a research methodology: An overview and guidelines", *Journal of Business Research*, 104, pp. 333–339; Robin Whittemore & Kathleen Knafl (2005), "The integrative review: updated methodology", *Journal of Advanced Nursing*, 52(5), pp. 546–553.
[12] UNDP (1994), *Human Development Report 1994*.

and civil society.[13] Contemporary security scholarship encompasses different levels of analysis, ranging from state-centred strategic concerns to individual welfare and social protection. Örmeci (2024), in his analysis of Türkiye's multidimensional foreign policy, illustrates the continuing relevance of geopolitical interests, international relations and strategic considerations in state-level analysis.[14] While addressing a different analytical domain, this perspective provides a useful contrast with human security, which directs attention towards individuals and the conditions affecting their everyday lives. This contrast helps clarify the analytical shift from state-centred security concerns to the everyday vulnerabilities and protection needs of older Muslim migrants in Europe.

These principles provide a relevant foundation for examining security in later migrant life. Older migrants may encounter interconnected challenges involving healthcare, housing, income, discrimination and institutional accessibility. Human security offers an integrated perspective through which these conditions can be analysed without reducing insecurity to either individual vulnerability or physical threats.

1.2. Ageing, Migration and the Accumulation of Vulnerabilities

Ageing is shaped by biological, social, economic and institutional processes that develop across the life course. For migrants, employment histories, pension entitlements, language proficiency, transnational family relationships and access to public services may influence the resources available in later life. The World Health Organization conceptualises healthy ageing in terms of functional ability, emphasising the interaction between individual capacities and supportive environments.[15] This perspective is particularly relevant to migrant populations because well-being depends not only on personal health but also on the accessibility and responsiveness of social and institutional arrangements. A life-course approach further highlights how earlier socioeconomic circumstances may influence later-life security. Employment conditions, educational opportunities, housing histories and participation in social protection systems can contribute to cumulative advantages or disadvantages. However, these processes are neither uniform nor necessarily irreversible.

---

[13] UN General Assembly (2012), "Follow-up to Paragraph 143 on Human Security of the 2005 World Summit Outcome", A/RES/66/290, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/n11/476/22/pdf/n1147622.pdf.

[14] Ozan Örmeci (2024), "Türkiye's New Multi-Dimensional Foreign Policy", *Russian Law Journal*, 12(2), pp. 86–99.

[15] WHO (2015), *World Report on Ageing and Health*, Geneva, Date of Accession: 01.09.2026 from https://www.who.int/publications/i/item/9789241565042?utm.

For older Muslim migrants, such circumstances may intersect with experiences associated with ethnic or religious minority status. Nevertheless, neither migration background nor religious identification should be regarded as an inherent source of vulnerability. Individual resources, family support, community networks and institutional protections may substantially modify experiences of insecurity. Vulnerability is therefore understood here as a context-dependent condition arising from relationships between individual circumstances and social structures, rather than as a fixed characteristic of older Muslim migrants.[16]

1.3. Intersectionality and Multidimensional Insecurity

Intersectionality provides a theoretical basis for examining how different social positions and structural inequalities interact. Crenshaw (2013) developed the concept to challenge approaches that treated race and gender as independent categories of discrimination, demonstrating that their intersection could produce distinctive experiences of disadvantage.[17] Applied to older Muslim migrants, intersectionality draws attention to the combined influence of age, migration history, gender, socioeconomic position, religious identification and institutional context. These factors do not necessarily operate independently or produce identical consequences across individuals. For example, an older migrant woman with limited financial resources and restricted proficiency in the language of her country of residence may experience healthcare barriers differently from someone with greater economic resources and institutional familiarity. Experiences of discrimination may further influence access, but their effects depend on individual circumstances and national contexts.[18]

Intersectionality therefore complements human security by identifying how overlapping social positions and structural conditions shape exposure to threats and access to protection. In the present study, it functions as a cross-cutting analytical perspective rather than an additional security dimension.

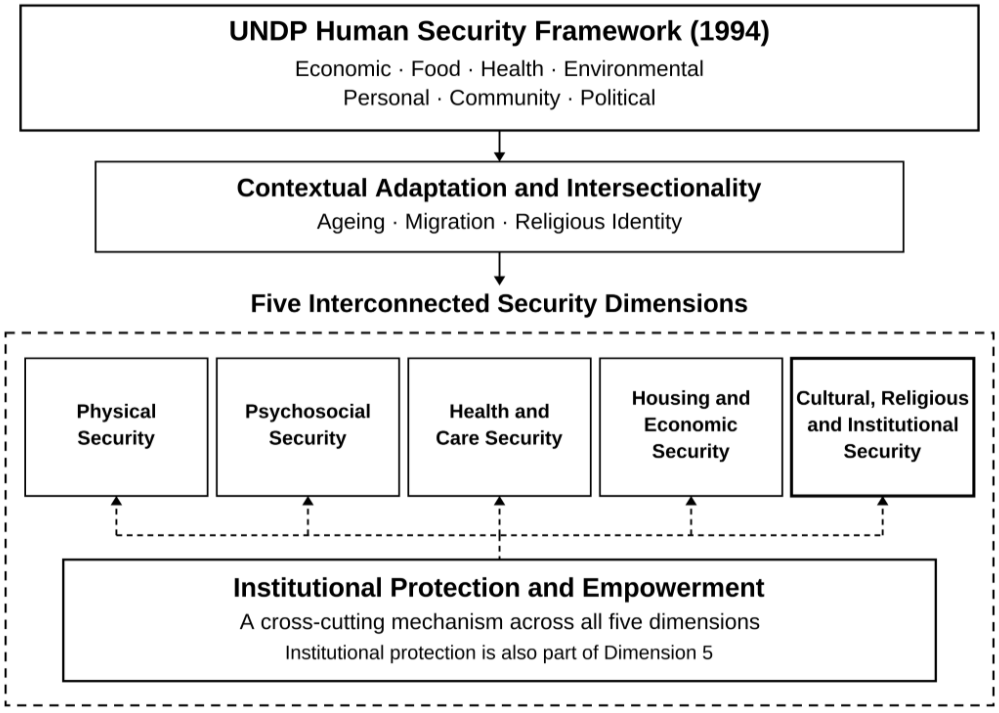
1.4. A Five-Dimensional Framework of Human Security

Building on the UNDP framework, this article proposes five interconnected dimensions adapted to the circumstances of older Muslim migrants in Europe. The model reorganises relevant

[16] D. Kloosterboer & B. Yılmaz (1997), *De leefsituatie van moslimouderen in Rotterdam*, Nederlandse Islamitische Bond voor Ouderen (NISBO), URL: https://books.google.com.tr/books?id=_XOnGwAACAAJ.
[17] Kimberlé Crenshaw (2013), "Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics", in (eds. by Karen J. Maschke) *Feminist Legal Theories*, London: Routledge, pp. 23–51.
[18] NISBO (2001), "NISBO-ouderenadviseurs, Rapport 2001: Belangrijke schakel in een integraal, toegankelijk en vraaggestuurd voorzieningenaanbod", Rotterdam: Zenodo.

elements of the original seven dimensions to give greater analytical visibility to ageing-related needs, psychosocial conditions, care accessibility and institutional representation. **Figure I** illustrates how the seven dimensions of the UNDP human security framework are conceptually reorganised through the perspectives of ageing, migration and intersectionality into five interconnected dimensions adapted to older Muslim migrants in Europe.

Figure I. Conceptual framework of multidimensional human security among older Muslim migrants in Europe



Source: Author's conceptual synthesis drawing on UNDP (1994), Crenshaw (2013), and WHO (2015). Institutional protection operates both within the fifth dimension and as a cross-cutting mechanism across the framework.

The five dimensions are:

1. Physical security: Protection against violence, harassment, intimidation and threats to personal safety, including racism, xenophobia and anti-Muslim hostility.
2. Psychosocial security: Emotional well-being, social connectedness, belonging, autonomy and protection against exclusion and isolation.
3. Health and care security: Equitable access to healthcare, long-term care and social support, including effective communication and culturally responsive provision.

4. Housing and economic security: Adequate and accessible accommodation, financial stability, pension-related resources and the material conditions necessary for independent living.
5. Cultural, religious and institutional security: The ability to maintain valued identities and practices, exercise fundamental rights, access institutions and participate in collective representation.

These dimensions are analytically distinguishable but not mutually exclusive. Economic insecurity may affect housing and health, while experiences of discrimination may influence physical safety, psychosocial well-being and institutional trust. The model is intended as a conceptual framework for organising interdisciplinary evidence and identifying potential relationships between vulnerability and protection. It does not constitute a validated measurement instrument, nor does it assume that the identified conditions affect all older Muslim migrants equally.

1.5. Institutional Protection and Empowerment

Institutional protection occupies a distinctive position within the proposed framework. It forms part of the fifth dimension while also influencing the conditions under which the other four dimensions are secured. The distinction between protection and empowerment is particularly important. Protection concerns the responsibilities of public institutions to safeguard rights and respond to threats, while empowerment involves enabling individuals and communities to participate in decisions affecting their lives.[19] Migrant organisations may contribute to both processes by identifying unmet needs, facilitating access to services, communicating with public authorities and advocating for inclusive policies. Their effectiveness, however, depends on organisational resources, accountability, institutional relationships and the continuity of their activities. The historical experiences of the Turkish-Islamic Elderly Union (TISBO) and the Netherlands Islamic Elderly Union (Nederlandse Islamitische Bond voor Ouderen, NISBO) provide relevant Dutch examples of collective representation and institutional engagement. Their activities and limitations are examined in Section 4.

The proposed framework thus conceptualises human security as a dynamic relationship between individual resources, social environments and institutional structures. Its principal

[19] UN General Assembly (2012), "Follow-up to Paragraph 143 on Human Security of the 2005 World Summit Outcome", A/RES/66/290, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/n11/476/22/pdf/n1147622.pdf.

contribution lies in integrating interconnected security concerns while recognising both the diversity of older migrant populations and the importance of effective institutional protection.

2. Methodology and Scope

2.1. Research Design

This study employs a critical integrative literature review, conceptual analysis and historical documentary examination to investigate multidimensional human security among older Muslim migrants in Europe. It draws on human security studies, gerontology, migration research, sociology of religion, public health and social policy. Integrative reviews enable the synthesis of evidence across disciplinary and methodological boundaries. They can also support theoretical development when research objectives, source selection and analytical procedures are clearly articulated.[20] Unlike systematic reviews or meta-analyses, the present study seeks to develop an interpretive synthesis rather than establish pooled estimates or causal effects.

The research combines three components: a critical examination of academic and institutional literature, the development of a five-dimensional human security framework, and a historically contextualised analysis of selected migrant organisations in the Netherlands. Together, these approaches connect contemporary research with documented institutional experiences.

2.2. Geographical and Population Scope

The study focuses on Europe, particularly the Netherlands, Germany, Belgium, France and the United Kingdom, where established migrant populations provide relevant contexts for examining ageing, religious diversity and social protection. The principal population consists of older people with Muslim backgrounds who have experienced international migration and entered later life in European societies. An age threshold of 60 years and above serves as a working reference, while recognising that statistical sources and individual studies may employ different thresholds, frequently 65 years or above. Studies involving people approaching later life are included where analytically relevant.

The term older Muslim migrants is used as a heterogeneous analytical category, encompassing differences in migration history, religious identification, gender, socioeconomic circumstances and length of residence. Research concerning broader Muslim populations or older migrants of

[20] Arzu Toker (2022), "Bir araştırma metodolojisi olarak sistematik literatür incelemesi: Meta-sentez yöntemi", *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 22(2), pp. 313–340; Ayşe Yıldız (2022), "Bir araştırma metodolojisi olarak sistematik literatür taramasına genel bakış", *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 22(2), pp. 367–386.

unspecified religious backgrounds is considered where relevant, but its findings are distinguished from evidence directly concerning older Muslim migrants.

2.3. Literature Identification and Source Selection

The review examines scholarship on human security, migrant ageing, discrimination, psychosocial well-being, healthcare, long-term care, housing, economic conditions and institutional representation. Sources include peer-reviewed publications, scholarly books and reports from recognised international, European and national institutions, particularly the United Nations, World Health Organization, European Union Agency for Fundamental Rights and relevant research organisations. Literature identification is organised around combinations of concepts relating to ageing, migration, Muslim communities, vulnerability, discrimination, social protection, care accessibility and collective representation.

Selection is guided by conceptual relevance, methodological transparency, population characteristics, geographical applicability and contribution to the research question. The assessment considers study design, sample composition, age thresholds, geographical coverage and stated limitations. The review is selective and interpretive rather than exhaustive. Particular priority is given to studies directly addressing older Muslim migrants or ageing populations with comparable migration backgrounds in European contexts. Where population-specific evidence is limited, studies concerning broader migrant and Muslim populations are included for contextual and analytical purposes, without assuming that their findings apply equally to older Muslim migrants. Sources with only tangential relevance to the research question are not used as primary evidence for the proposed framework. Historical archival documents are selected on the basis of their institutional provenance, thematic relevance and contribution to understanding collective protection and representation.

2.4. Analytical Framework and Evidence Synthesis

The synthesis follows the five dimensions developed in Section 1: physical security, psychosocial security, health and care security, housing and economic security, and cultural, religious and institutional security.

Evidence is examined at three interconnected levels:

1. Individual: Health, functional ability, economic resources, language proficiency and migration experience.

2. Social and community: Family relationships, social networks, community participation and cultural or religious support.
3. Institutional and structural: Welfare policies, healthcare systems, service accessibility, discrimination safeguards and collective representation.

An intersectional perspective is applied across these levels to examine how age, gender, migration history, socioeconomic position and religious identification may interact with institutional conditions. The analysis distinguishes documented vulnerabilities, plausible mechanisms of insecurity and potential protective resources. Empirical findings are separated from conceptual interpretations and policy recommendations, with particular attention to differences in evidence quality and population coverage.

2.5. Historical Documentary Analysis: TISBO and NISBO

The study incorporates a historically contextualised examination of two Dutch migrant organisations: the Turkish-Islamic Elderly Union (Turks-Islamitische Ouderen Bond, TISBO), founded on 5 July 1993, and the Netherlands Islamic Elderly Union (Nederlandse Islamitische Bond voor Ouderen, NISBO), founded on 5 July 1995. These organisations were selected because their documented objectives and activities addressed housing, welfare access, social participation, advisory services and institutional representation—concerns directly relevant to the proposed human security framework. The documentary material includes organisational working plans, project proposals, research reports, policy documents and selected institutional correspondence. Relevant primary sources include "*Woonwensen Turkse Ouderen*"[21], "*Turkse ouderen: Drie woonprogramma's*"[22], TISBO's working plan and project documents[23], and NISBO's policy and elderly advisory publications.[24] Several documents are preserved in historical archival editions deposited in Zenodo. The analysis considers documentary provenance, organisational objectives, historical context and relationships with public authorities. It distinguishes proposed initiatives from documented implementation and

[21] ACB & TISBO (1994), "Woonwensen Turkse Ouderen 1994 - Een samenvatting en vergelijk van de resultaten van negen monitorgesprekken met Turkse ouderen te Haarlem", Zenodo.
[22] Van der Lingen Adviseurs & ACB/RCB & TISBO (1994), "Programma's van eisen voor woonprojecten voor Turkse ouderen in Haarlem, 1994", Zenodo.
[23] TISBO (1995), "TISBO Werkplan 1995 - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond", Zenodo; TISBO (1995), "TISBO Projecten 1995 - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond", Zenodo.
[24] NISBO (2001), "NISBO-ouderenadviseurs, Rapport 2001: Belangrijke schakel in een integraal, toegankelijk en vraaggestuurd voorzieningenaanbod".

measurable outcomes, avoiding the assumption that institutional intentions necessarily produced effective protection.

TISBO and NISBO are treated as historically situated Dutch examples. Their relevance lies in illustrating the development, functions and limitations of collective institutional protection.

2.6. Research Limitations

The study has several limitations. First, available research does not consistently distinguish older Muslim migrants from broader ethnic minority, migrant or Muslim populations, restricting the availability of directly applicable evidence. Differences in national welfare systems, migration histories and age classifications also limit cross-country comparability.

Second, the integrative review is selective and interpretive rather than systematic. It cannot establish representative prevalence estimates, determine causal relationships or claim comprehensive coverage of the literature.

Third, the proposed five-dimensional framework is a conceptual synthesis rather than an empirically validated measurement instrument. Its dimensions and relationships require further investigation through population-specific and comparative research.

These limitations define the study's contribution as an interdisciplinary conceptual synthesis supported by selected empirical research and historical institutional evidence.[25]

3. Five Dimensions of Human Security among Older Muslim Migrants in Europe

3.1. Physical Security: Discrimination, Harassment and Personal Safety

Physical security concerns protection against violence, harassment, intimidation and threats to personal safety. For older Muslim migrants, these risks may intersect with age-related circumstances, migration background and experiences of ethnic or religious discrimination. The European Union Agency for Fundamental Rights, surveying 9,604 Muslims across thirteen EU Member States, reported that 47 per cent had experienced racial discrimination during the preceding five years, 27 per cent racist harassment and 4 per cent racist violence. Only 12 per cent of respondents experiencing racist harassment reported their most recent incident to an official body.[26]

[25] Sait Gürbüz & Faruk Şahin (2014), *Sosyal Bilimlerde Araştırma Yöntemleri*, Ankara: Seçkin Yayıncılık, pp. 74–82.
[26] FRA (2024), *Being Muslim in the EU: Experiences of Muslims*.

These findings highlight the relevance of discrimination to personal safety and institutional protection. However, the survey was not designed specifically for older Muslim migrants, and its percentages cannot be interpreted as prevalence estimates for this population. Ageing may introduce additional considerations. Mobility limitations, chronic health conditions, restricted transportation options and dependence on local facilities can potentially influence how older individuals experience threats or intimidation. Such relationships require age-specific empirical investigation rather than assumptions based on religious or migrant status. Physical insecurity may also affect psychosocial well-being, mobility and confidence in public institutions. Consequently, relevant protective measures include accessible reporting procedures, effective anti-discrimination enforcement, equitable police protection and age-sensitive community safety policies.

3.2. Psychosocial Security: Loneliness, Exclusion and Belonging

Psychosocial security encompasses emotional well-being, social connectedness, autonomy and belonging. Its significance extends beyond the frequency of interpersonal contact to include relationship quality, perceived control, socioeconomic circumstances and experiences of exclusion. Van Tilburg and Fokkema (2021), drawing on the Longitudinal Aging Study Amsterdam, examined loneliness among 176 Moroccan-born and 235 Turkish-born participants aged 55–66, compared with 292 Dutch participants.[27] The migrant groups reported greater loneliness despite relatively frequent social contacts. Differences in social participation, income satisfaction, perceived control and depressive symptoms explained more than half of the observed loneliness gap. These findings demonstrate that loneliness cannot be addressed solely by increasing social contacts. Socioeconomic circumstances, autonomy and meaningful participation are also relevant.[28] Transnational relationships add another dimension. Tezcan (2018), drawing on forty interviews with older Turkish migrants in Germany, examined circular migration between Germany and Türkiye and its relationship with healthcare, family responsibilities and intergenerational negotiations.[29] Decisions concerning residence and care

[27] Theo G. Van Tilburg & Tineke Fokkema (2021), "Stronger feelings of loneliness among Moroccan and Turkish older adults in the Netherlands: in search for an explanation", *European Journal of Ageing*, 18(3), pp., pp. 311–322.
[28] Cansu Taşcı (2024), "Türk Emek Göçmenlerinin Ulusötesi Yaşlanma Deneyimleri", *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 41(2), pp. 383–406.
[29] Tolga Tezcan (2018), "On the move in search of health and care: Circular migration and family conflict amongst older Turkish immigrants in Germany", *Journal of Aging Studies*, 46, pp. 82–92.

reflected both perceived differences between national healthcare systems and changing family circumstances.[30]

Such findings suggest that transnational networks may provide support while also involving competing expectations and practical challenges. Their implications vary across individuals and should not be generalised to all older Muslim migrants. Experiences of discrimination may additionally influence belonging and institutional trust, although their relationship with loneliness requires further population-specific research. Psychosocial protection therefore involves supportive relationships, accessible participation opportunities and policies addressing socioeconomic exclusion. Effective interventions should consider relationship quality, autonomy and individual preferences alongside social contact.

3.3. Health and Care Security: Access, Communication and Culturally Responsive Services

Health and care security concerns equitable access to healthcare, long-term care and social support. Among older migrants, access may be shaped by communication, socioeconomic resources, institutional familiarity, family relationships and continuity of care. Research from the Netherlands illustrates these interactions. Pot, Keijzer, and de Bot (2018), studying thirty-nine older Turkish women, found that limited Dutch-language proficiency did not automatically imply poorer well-being. The consequences depended partly on social support and access to assistance with communication. Language barriers became more consequential where such resources were insufficient.[31]

Şekercan et al. (2018) examined healthcare utilisation among older Turkish and Moroccan migrants in the Netherlands, including medical services obtained in their countries of origin.[32] Their findings did not support the assumption that healthcare use abroad necessarily corresponded to reduced healthcare utilisation in the Netherlands.

Similarly, Tezcan (2018) demonstrated that older Turkish circular migrants negotiated care across Germany and Türkiye, with decisions shaped by healthcare arrangements, family relationships and individual preferences. Long-term care research provides further evidence of

[30] NISBO (1998), "Ontluikende diversiteit in het lokale ouderenbeleid, Een discussienotitie over knelpunten en oplossingsstrategieen".
[31] Anna Pot & Merel Keijzer & Kees de Bot (2018), "De taalbarrière bij oudere Turkse vrouwen nader onderzocht", *Tijdschrift voor Gerontologie en Geriatrie,* 49(6), pp. 274–282.
[32] Aydın Şekercan & Marieke B Snijder & RJG Peters & Karien Stronks (2018), "Gaat zorggebruik in het land van herkomst onder oudere Turkse en Marokkaanse migranten gepaard met minder zorggebruik in Nederland? Een combinatie van HELIUS-data met Achmea registratiedata", pp. 253–262.

institutional differences. Conkova and van den Broek (2025), analysing Dutch administrative data covering 2016–2022, identified variations in formal care utilisation across older migrant populations.[33] Moroccan and Turkish older adults were comparatively less likely to use residential care and more likely to use personal care budgets. Such differences require examination of service arrangements, preferences and accessibility rather than automatic interpretation as unmet needs.

In Belgium, Ahaddour, Van Den Branden, and Broeckaert (2016) identified linguistic, financial, informational and cultural or religious considerations affecting access to institutional elderly care among Moroccan and Turkish migrants.[34] Berdai Chaouni et al. (2020) further illustrated the complexity of dementia care arrangements among Moroccan migrant families, involving interactions between informal caregivers, professional services and transnational networks.[35] Extending this discussion, Berdai Chaouni (2026) argues that equitable dementia care for older migrants requires attention to structural inequalities and institutional practices alongside cultural responsiveness.

Evidence from the United Kingdom similarly identifies communication, family expectations and service responsiveness as relevant concerns among Bangladeshi, Pakistani and White British social care users.[36]

In France, Bettayeb et al. (2023) examined sixty-seven older former migrant workers living in a Marseille migrant hostel, documenting chronic health conditions, socioeconomic difficulties and limitations in preventive healthcare access.[37] Although religious identity was not the study's defining analytical category, its findings contribute to understanding health insecurity among ageing labour migrants.

---

[33] Nina Conkova & Thijs van den Broek (2025), "Long-term care use among older migrants in the Netherlands: What to expect in the next decade?", *Journal of Aging & Social Policy*, 37(5), pp. 875–891.
[34] Chaïma Ahaddour & Stef Van Den Branden & Bert Broeckaert (2016), "Institutional Elderly Care Services and Moroccan and Turkish Migrants in Belgium: A Literature Review", *Journal of Immigrant and Minority Health*, 18(5), pp. 1216–1227.
[35] Saloua Berdai Chaouni & An-Sofie Smetcoren & Liesbeth De Donder (2020), "Caring for migrant older Moroccans with dementia in Belgium as a complex and dynamic transnational network of informal and professional care: A qualitative study", *International Journal of Nursing Studies*, 101, 103413.
[36] Margaret Blake & Alison Bowes & Valdeep Gill & Fatima Husain & Ghazala Mir (2017), "A collaborative exploration of the reasons for lower satisfaction with services among Bangladeshi and Pakistani social care users", *Health & Social Care in the Community*, 25(3), pp. 1090–1099.
[37] Leila Bettayeb & Yannick Jaffré & Jacques Chiaroni & Yassine Ennomany & Patrick Villani & Anne-Laure Couderc (2023), "Accès aux soins d'une population d'anciens travailleurs immigrés vivant en foyer", *Santé Publique*, 35(5), pp. 13–17.

Collectively, these studies show that health and care security depends on more than formal service availability. Accessible communication, continuity of care, socioeconomic conditions, institutional responsiveness and individual autonomy are also important. Potential protective measures include professional interpretation, accessible health information, inclusive care planning and equitable long-term care arrangements. Their effectiveness should be evaluated through service accessibility, patient experiences, continuity of care and relevant health outcomes.

3.4. Housing and Economic Security: Adequate Living Conditions and Financial Independence

Housing and economic security encompass stable income, adequate accommodation and the material resources necessary for independent living. Among older migrants, these conditions may reflect employment histories, pension entitlements, household composition and housing market inequalities. The Organisation for Economic Co-operation and Development and European Commission reported that 26 per cent of immigrants aged 65 and above in the European Union lived in relative poverty, compared with 19 per cent of native-born older adults.[38] These figures demonstrate broader economic inequalities among older immigrants but do not provide estimates specifically for older Muslim migrants. Housing conditions may compound financial insecurity. Affordability, accessibility, residential stability and proximity to healthcare and community facilities can influence independence and well-being.

The FRA (2024) also reported racial discrimination affecting access to housing among Muslim respondents.[39] Approximately 35 per cent of those seeking to rent or purchase accommodation during the relevant survey period reported discriminatory experiences. This evidence concerns the wider surveyed Muslim population rather than older migrants specifically. Bettayeb et al. (2023) provide an additional perspective through their study of older former migrant workers residing in accommodation originally designed for labour migrants.[40] Their findings illustrate the relationship between ageing, socioeconomic disadvantage, housing circumstances and healthcare accessibility. From a human security perspective, adequate housing involves more than physical shelter. Residential arrangements may affect mobility, family relationships, social

[38] OECD & European Commission (2023), *Indicators of Immigrant Integration 2023: Settling In*, OECD Publishing.
[39] FRA (2024), *Being Muslim in the EU: Experiences of Muslims*.
[40] Leila Bettayeb & Yannick Jaffré & Jacques Chiaroni & Yassine Ennomany & Patrick Villani & Anne-Laure Couderc (2023), "Accès aux soins d'une population d'anciens travailleurs immigrés vivant en foyer", pp. 13–17.

participation, access to care and opportunities to maintain valued cultural or religious practices. Collective housing initiatives and age-appropriate residential programmes may help address these concerns when they respond to documented needs and respect individual choice. Their contribution should be evaluated through affordability, accessibility, resident autonomy and actual outcomes.

3.5. Cultural, Religious and Institutional Security: Identity, Rights and Collective Protection

Cultural, religious and institutional security concerns the ability to maintain valued identities and practices, exercise fundamental rights, access public institutions and participate in collective representation. For older Muslim migrants, cultural and religious practices may provide continuity, belonging and support. Their significance varies according to personal beliefs, migration experiences, family relationships and individual preferences. Muslim identity therefore should not be treated as implying uniform religious observance or identical expectations concerning care. Kevern et al. (2023), examining seven family caregivers within a British Pakistani Muslim community, found that religious faith could provide support in dementia caregiving, while certain community expectations and limited dementia awareness could complicate access to external assistance.[41] The study illustrates the potentially varied roles of religion in care, although its small qualitative sample limits generalisation.

Belgian research similarly identifies the relevance of cultural and religious considerations in institutional elderly care.[42] However, culturally responsive services alone may be insufficient when structural inequalities and institutional barriers remain unaddressed.[43] Institutional security therefore extends beyond recognition of cultural or religious preferences. It also includes equitable access to legal protection, administrative procedures, public services and mechanisms for addressing discrimination.

The FRA (2024) reported that only 6 per cent of respondents who had experienced discrimination during the preceding year reported the incident or made a complaint. Although these findings do not establish reporting patterns among older Muslim migrants specifically,

[41] Peter Kevern & Dawn Lawrence & Nargis Nazir & Anna Tsaroucha (2023), "Religious Influences on the Experience of Family Carers of People with Dementia in a British Pakistani Muslim Community", *Healthcare*, 11(1), 120.
[42] Chaïma Ahaddour & Stef Van Den Branden & Bert Broeckaert (2016), "Institutional Elderly Care Services and Moroccan and Turkish Migrants in Belgium: A Literature Review", pp. 1216–1227.
[43] Saloua Berdai Chaouni (2026), "Toward equitable dementia care for older migrants: a new conceptual framework", *International Journal of Ageing and Later Life*, 19(2), pp. 247–279.

they underscore the wider importance of accessible complaint procedures and institutional accountability. Older migrants may encounter additional difficulties in exercising rights where communication barriers, health-related limitations or limited familiarity with administrative systems affect access to assistance. Collective representation constitutes a further protective mechanism. Migrant organisations may identify unmet needs, communicate concerns to public authorities, facilitate access to services and advocate for more inclusive policies. Their contribution nevertheless depends on accountability, institutional relationships and demonstrable activities rather than organisational identity alone.

The historical experiences of TISBO and NISBO in the Netherlands provide relevant examples of attempts to develop such mechanisms.[44] Their activities and institutional limitations are examined in Section 4.

Cultural, religious and institutional security thus encompasses both individual autonomy and the practical conditions necessary to exercise rights, participate in decision-making and obtain institutional protection.

3.6. Interconnections between the Five Dimensions

The five dimensions are interconnected, with insecurity in one domain potentially influencing conditions in another. Economic disadvantage may restrict housing choices; unsuitable accommodation may complicate healthcare access; communication barriers may limit service utilisation; and discrimination may affect both personal safety and institutional trust. The reviewed evidence illustrates these relationships across different contexts. Dutch research highlights the association between loneliness and socioeconomic conditions; German studies demonstrate the interaction of transnational mobility, healthcare and family relationships; Belgian and British research identifies barriers within care systems; and French findings connect ageing, residential conditions and health needs.

These studies do not establish a uniform causal model applicable to all older Muslim migrants in Europe. Rather, they support an analytical approach that examines vulnerability and protection across individual, social and institutional levels while recognising differences between populations and national contexts. Institutional arrangements are particularly

[44] NISBO (2002), "NISBO-Werkplan 2002: Institutioneel jaarwerkplan en beleidsdocument", Rotterdam: Zenodo; TISBO (1995), "TISBO Projecten 1995 - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond"; Van der Lingen Adviseurs & ACB/RCB & TISBO (1994), "Programma's van eisen voor woonprojecten voor Turkse ouderen in Haarlem, 1994".

significant because public policies, accessible services, anti-discrimination measures and collective representation may influence several dimensions simultaneously.

The following section examines these protective mechanisms through governmental responsibilities, civil society participation and the historically situated experiences of TISBO and NISBO in the Netherlands.

4. Institutional Protection and Representation: Government Policies, Civil Society and the Historical Experiences of TISBO and NISBO

4.1. Government Policies and Institutional Responsibilities

Institutional protection is essential to human security because the effective exercise of rights depends not only on legal entitlements but also on accessible and accountable public institutions. For older migrants, this encompasses healthcare, social protection, housing, anti-discrimination measures and opportunities to participate in decisions affecting their lives. The United Nations human security framework assigns governments primary responsibility for protection while recognising the complementary role of community participation and empowerment.[45] The Madrid International Plan of Action on Ageing similarly emphasises older persons' inclusion, participation and well-being.[46] Within Europe, the continuing review of this framework has reinforced the importance of civil society engagement in ageing policy.[47]

International attention to older persons' rights has also intensified. In 2025, the United Nations Human Rights Council adopted Resolution 58/13, establishing an intergovernmental process to develop a legally binding instrument concerning the human rights of older persons. Resolution 60/11 subsequently addressed their continuing promotion and protection.[48]

National political environments also influence the institutional context in which migrant populations exercise their rights and seek representation. Examining the 2017 German federal elections, Örmeci (2018) analyses the political position of the Social Democratic Party (SPD), including its approach to Türkiye and Turkish communities in Germany. Although the study

[45]UN General Assembly (2012), "Follow-up to Paragraph 143 on Human Security of the 2005 World Summit Outcome", A/RES/66/290, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/n11/476/22/pdf/n1147622.pdf.
[46] UN (2002), "Report of the Second World Assembly on Ageing, Madrid 2002", A/CONF.197/9, United Nations, Date of Accession: 01.09.2026 from https://docs.un.org/en/A/CONF.197/9.
[47] UNECE (2026), *Strengthening the Voice of Older Persons: Civil Society's Role in the MIPAA Review Process*, United Nations Economic Commission for Europe.
[48] UN (2025), "Resolution Adopted by the Human Rights Council", A/HRC/RES/60/11, United Nations Human Rights Council, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/g25/170/83/pdf/g2517083.pdf.

does not specifically address older Muslim migrants, it provides relevant political context for understanding how questions concerning migrant communities are situated within national political debates. Such political environments constitute an important background for examining institutional inclusion, participation and representation.[49]

For older Muslim migrants, these developments are relevant because formal protections may coexist with practical barriers arising from language, socioeconomic inequalities, discrimination or limited institutional familiarity. Research on ageing and health among migrants in Europe likewise identifies the importance of addressing inequalities through accessible and responsive public systems.[50] Institutional protection therefore requires translating recognised rights into effective access, accountability and meaningful participation.

4.2. Civil Society and Community-Based Protection

Civil society organisations may act as intermediaries between older migrant populations and public authorities by identifying unmet needs, disseminating information, facilitating service access and communicating collective concerns. Their contribution involves both protection and empowerment. Community-based knowledge can help institutions understand migration histories, communication needs and barriers to participation, while representative activities may strengthen the capacity of older migrants to influence public decisions. However, community organisations cannot substitute for governmental responsibilities. Their effectiveness depends on resources, professional capacity, accountability and institutional cooperation. Representation must also be evaluated through actual engagement with the people concerned rather than assumed from shared ethnic or religious identity.

The development of migrant organisations in the Netherlands during the 1990s provides relevant historical material for examining these functions. TISBO and NISBO illustrate two related approaches: community-specific organisation and broader representation across ethnic and national backgrounds.

[49] Ozan Örmeci (2018), "2017 Almanya Federal Seçimleri ve SPD'nin Türkiye ile İlişkilere ve Almanya'daki Türklere Bakışı", *EURO Politika*, 01.10.2018, pp. 201–230.
[50] Dirk Kloosterboer & Berna Yılmaz (1997), *De leefsituatie van moslimouderen in Rotterdam*, Nederlandse Islamitische Bond voor Ouderen (NISBO); Dirk Kloosterboer & Berna Yılmaz (1999), "NISBO Beleidsvisie: Een gemiste kans? Oudere migranten in het grotestedenbeleid".

4.3. TISBO and NISBO: Historical Experiences of Institutional Representation in the Netherlands

4.3.1. TISBO: From Community Needs to Organised Representation

The Turks-Islamitische Ouderen Bond (TISBO), established on 5 July 1993, developed initiatives addressing the housing, welfare and social participation needs of older Turkish migrants in the Netherlands. A prominent example was the Bizim Ev housing initiative in Haarlem. Contemporary research and planning documents, including Woonwensen Turkse Ouderen and Turkse ouderen: Drie woonprogramma's, examined residential preferences and translated identified needs into differentiated housing proposals.[51]

The initiative illustrates how housing concerns could become matters of organised representation, involving migrant communities, housing professionals and public authorities. In human security terms, it connected residential needs with autonomy, social participation and institutional engagement. TISBO's activities extended beyond housing. Its Werkplan 1995 and Projecten 1995 identified initiatives concerning elderly advisory services, information provision, older Turkish women and the exchange of knowledge and experience.[52]

These documents demonstrate a multidimensional approach to identifying older migrants' needs. Nevertheless, proposed programmes must be distinguished from completed activities and demonstrated outcomes. TISBO's historical significance lies particularly in its efforts to organise community concerns and develop institutional responses.

4.3.2. NISBO: Towards Broader Institutional Representation

The Netherlands Islamic Elderly Union (Nederlandse Islamitische Bond voor Ouderen, NISBO), founded on 5 July 1995, extended institutional representation beyond a single ethnic or national community. Its development included parliamentary recognition on 7 December 1995, followed by public funding beginning in January 1996. These milestones are relevant to

[51] ACB & TISBO (1994), "Woonwensen Turkse Ouderen 1994 - Een samenvatting en vergelijk van de resultaten van negen monitorgesprekken met Turkse ouderen te Haarlem"; ACB/RCB (1995), *Oud worden in Haarlem – Een onderzoek naar de zorgbehoeften van Turkse en Marokkaanse ouderen in Haarlem*, 30132 – Archief van het Amsterdams Centrum Buitenlanders, Date of Accession: 01.09.2026 from https://archief.amsterdam/archives/pdf/30132.ead.pdf; Van der Lingen Adviseurs & ACB/RCB & TISBO (1994), "Programma's van eisen voor woonprojecten voor Turkse ouderen in Haarlem, 1994".

[52] TISBO (1995), "TISBO Projecten 1995 - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond"; TISBO (1995), "TISBO Werkplan 1995 - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond".

understanding the relationship between community initiative, governmental recognition and institutional support.

NISBO subsequently addressed ageing, social welfare, institutional accessibility and public policy. Its response to research by the Dutch Social and Cultural Planning Office demonstrates engagement with debates concerning older ethnic minority populations.[53] The organisation also examined the position of older migrants within Dutch urban policy. Its 1999 report "*Een gemiste kans? Oudere migranten in het grotestedenbeleid"* considered policy developments in Amsterdam, The Hague, Haarlem, Rotterdam and Utrecht, questioning whether older migrants' needs were adequately recognised and incorporated into policy objectives and evaluation procedures.[54] This intervention illustrates an important dimension of institutional security: the difference between formal inclusion in general welfare policies and the effective recognition of population-specific circumstances. NISBO's broader organisational approach sought to connect community representation with governmental policy processes, while its elderly advisory activities offered a more direct mechanism for facilitating access to existing services.

4.3.3. Elderly Advisory Services as Institutional Protection

NISBO's ouderenadviseurs programmes provide a concrete example of institutional intermediation. Its reports from 1999 and 2001 describe advisory arrangements addressing income, healthcare, housing, social services and participation among older Turkish and Moroccan migrants. The 1999 report documented 697 registered requests for advice between January and May 1998, providing evidence of the recorded volume of enquiries handled during that period.[55] This figure concerns requests rather than distinct beneficiaries or successful interventions. The 2001 report describes further operational arrangements, including individual guidance, consultation registration, mediation, cooperation with welfare providers and assistance procedures. It identifies consultation locations in Amsterdam, Haarlem, Rotterdam, Zaandam, Utrecht and The Hague. These records are important because they document advisory practices rather than organisational intentions alone.

[53] NISBO (1998), "Enkele kanttekeningen bij het SCP-rapport "De eerste generatie in de derde levensfase"", Rotterdam: Zenodo.
[54] Dirk Kloosterboer & Berna Yılmaz (1999), "NISBO Beleidsvisie: Een gemiste kans? Oudere migranten in het grotestedenbeleid".
[55] NISBO (1999), "NISBO-ouderenadviseurs, Rapport 1999: Belangrijke schakel in een integraal, toegankelijk en vraaggestuurd voorzieningenaanbod", Rotterdam: Zenodo.

Within the human security framework, elderly advisers can be understood as potential instruments of protection and empowerment. They may help individuals navigate administrative procedures, obtain information, communicate with service providers and exercise social rights. The advisory model also illustrates how a community organisation can connect several security dimensions without directly delivering every service. Its potential contribution spans healthcare, income, housing and social participation. However, the available documentation does not establish the long-term effectiveness of these services. Such an assessment would require additional evidence concerning beneficiaries, referrals, completed interventions and subsequent outcomes.

4.3.4. Historical Significance and Institutional Limitations

The experiences of TISBO and NISBO demonstrate different but related forms of collective organisation. TISBO focused on identifying and articulating the needs of older Turkish migrants, while NISBO sought broader representation and engagement with welfare and governmental institutions. Their historical contributions can be differentiated into identifying needs, developing proposals, obtaining institutional recognition, implementing advisory arrangements and participating in policy discussions. These achievements should not be conflated. Recognition does not automatically establish effective service provision, and documented activities do not necessarily demonstrate improved individual security. The eventual discontinuation of both organisations raises questions about financial sustainability, institutional continuity and the preservation of organisational knowledge. Their experiences nevertheless provide historically grounded evidence of attempts to strengthen collective protection in the Netherlands. They do not establish the current state of representation among older Muslim migrants throughout Europe, which requires separate contemporary investigation.

4.4. Institutional Gaps and Contemporary Protection Challenges

The historical cases highlight questions relevant to contemporary institutional protection. Universal welfare systems may provide formal entitlements without ensuring equitable access for people facing communication difficulties, socioeconomic disadvantage or discrimination. Fragmented responsibilities across healthcare, housing, municipalities and welfare institutions may create additional obstacles when multiple needs arise simultaneously.[56] Representation also requires attention to differences within migrant populations. Older women, people living

[56] Maria Kristiansen & Oliver Razum & Hürrem Tezcan-Güntekin & Allan Krasnik (2016), "Aging and health among migrants in a European perspective", *Public Health Reviews*, 37(1), 20, pp. 1-14.

alone, individuals with disabilities and those with limited resources may encounter distinct barriers to participation. International human rights developments reinforce the importance of meaningful participation, non-discrimination and institutional accountability.[57]

The TISBO and NISBO experiences suggest that effective protection requires more than the establishment of community organisations. It also depends on cooperation with public institutions, continuity of accessible services, demonstrable engagement and sustainable mechanisms of representation.

4.5. Towards an Integrated Institutional Protection Framework

The preceding analysis identifies four principles for strengthening institutional protection within a multidimensional human security approach.

- First, equal accessibility requires translating formal rights into practical access to services, information and protection mechanisms.
- Second, meaningful participation involves older migrants in identifying needs, designing programmes and evaluating policies.
- Third, institutional coordination connects governmental agencies, healthcare providers, housing organisations and civil society to reduce fragmented responses.
- Fourth, organisational sustainability requires attention to institutional resources, accountability, continuity of representation and preservation of knowledge.

The historical examples illustrate the relevance of these principles. TISBO's housing activities demonstrate the mobilisation of residential needs into organised proposals, while NISBO's advisory and policy initiatives show how community representation may facilitate engagement with welfare systems. These experiences support the conceptual proposition that institutional protection operates both as a distinct component of human security and as a mechanism potentially influencing its other dimensions. Effective protection ultimately requires combining governmental responsibility, accessible services and opportunities for older migrants to participate as rights-bearing members of society.

[57] UN (2025), "Resolution Adopted by the Human Rights Council", A/HRC/RES/60/11, United Nations Human Rights Council, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/g25/170/83/pdf/g2517083.pdf.

5. Discussion: Towards an Integrated Human Security Framework

5.1. From Individual Vulnerability to Multidimensional Human Security

The preceding analysis indicates that human security among older Muslim migrants cannot be adequately understood by examining ageing, migration background, religious identity or socioeconomic conditions independently. These factors interact within social and institutional environments, producing different patterns of vulnerability and protection. Research on migrant ageing has identified relationships between health, socioeconomic resources and access to institutional support.[58] However, evidence concerning migrant ageing and religious discrimination often derives from different populations and research traditions. Integrating these perspectives therefore requires analytical caution.

The five-dimensional framework developed in this article builds on the people-centred approach of the United Nations Development Programme[59] and its subsequent articulation through protection and empowerment principles.[60] It examines security across physical, psychosocial, health and care, housing and economic, and cultural, religious and institutional dimensions. Its central proposition is that vulnerability emerges through interactions between personal circumstances, structural conditions and available protective resources. Age, migration history and Muslim identity are therefore not treated as inherent indicators of insecurity. This interpretation shifts attention from categorising vulnerable populations towards identifying the mechanisms through which insecurity develops and the conditions under which protection becomes effective.

5.2. The Interaction between Vulnerability and Discrimination

An important implication of the framework is that socioeconomic disadvantage and discrimination may interact rather than operate as independent sources of insecurity. European evidence documents substantial experiences of racial discrimination among Muslim populations,[61] while comparative data indicate higher poverty rates among older immigrants

[58] Maria Kristiansen & Oliver Razum & Hürrem Tezcan-Güntekin & Allan Krasnik (2016), "Aging and health among migrants in a European perspective"; Cemal Yılmaz (2026), "Islamic University of Rotterdam: From Interfaith Dialogue to Pluralistic Cooperation", *International Journal of Humanities and Social Science*, (16), pp. 279–298.
[59] UNDP (1994), *Human Development Report 1994*.
[60] UN General Assembly (2012), "Follow-up to Paragraph 143 on Human Security of the 2005 World Summit Outcome", A/RES/66/290, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/n11/476/22/pdf/n1147622.pdf.
[61] FRA (2024), *Being Muslim in the EU: Experiences of Muslims.*

than among their native-born counterparts in the European Union.[62] Although these findings concern different populations, they establish relevant contexts for examining potentially overlapping inequalities.

Intersectionality provides an analytical perspective for understanding such relationships. Following Crenshaw (2013), disadvantage is examined through interactions between social positions and structural conditions rather than as the simple accumulation of separate characteristics.[63] For example, limited financial resources may restrict housing options, while discriminatory practices can create additional barriers. Similarly, language-related difficulties may affect healthcare access when professional interpretation or institutional assistance is unavailable. These relationships represent plausible mechanisms rather than established causal pathways among older Muslim migrants. Their significance depends on national contexts, individual resources and available support.

Research on equitable dementia care among older migrants in Belgium similarly highlights the importance of structural inequalities alongside cultural considerations (Berdai Chaouni, 2026). Although focused on dementia care, this perspective supports examining institutional conditions rather than attributing disadvantage primarily to cultural differences. Within the proposed framework, discrimination is therefore understood as a potential cross-cutting mechanism affecting several dimensions of human security, including institutional trust, service accessibility and social participation.

5.3. Institutional Protection as a Cross-Cutting Mechanism

A distinguishing feature of the proposed framework is its conceptualisation of institutional protection as both a component of the fifth security dimension and a mechanism potentially influencing the other four. Institutional security encompasses access to rights, cultural and religious autonomy, representation and protection against exclusion. At the same time, governmental policies, public services and institutional practices influence physical safety, healthcare, housing, economic resources and psychosocial well-being. This interpretation

[62] OECD & European Commission (2023), *Indicators of Immigrant Integration 2023: Settling In*.
[63] Kimberlé Crenshaw (2013), "Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics", pp. 23–51.

reflects the human security principles of protection and empowerment, which combine governmental responsibility with meaningful participation by individuals and communities.[64]

The historical experiences of TISBO and NISBO provide illustrations of institutional intermediation. TISBO's involvement in the Bizim Ev housing initiative demonstrates how identified residential needs were translated into research, organised proposals and engagement with public authorities.[65] NISBO's elderly advisory reports document arrangements intended to assist older migrants with welfare institutions, healthcare, housing and administrative procedures.[66] These activities illustrate how community organisations may connect individual needs with institutional responses. However, the historical documents do not establish the long-term effectiveness of all initiatives or their transferability to other European contexts. Institutional protection is consequently understood as a relationship involving governmental responsibility, accessible services, accountable civil society organisations and the agency of older migrants themselves.

5.4. Proposed Integrated Human Security Model

The proposed model combines three analytical levels with three elements through which vulnerability and protection can be examined. The individual level includes health, functional ability, economic resources, language proficiency and migration experience. The social and community level encompasses family relationships, social networks, neighbourhood environments, cultural and religious participation, and collective support. The institutional and structural level addresses welfare arrangements, healthcare systems, housing policies, anti-discrimination safeguards and representation.

Across these levels, the model distinguishes:

- Conditions of vulnerability: Circumstances that may increase exposure to insecurity, such as inadequate resources, poor health or social isolation.

[64] UN (2025), "Resolution Adopted by the Human Rights Council", A/HRC/RES/60/11, United Nations Human Rights Council, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/g25/170/83/pdf/g2517083.pdf.

[65] TISBO (1995), "TISBO Projecten 1995 - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond"; TISBO (1995), "TISBO Werkplan 1995 - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond"; Van der Lingen Adviseurs & ACB/RCB & TISBO (1994), "Programma's van eisen voor woonprojecten voor Turkse ouderen in Haarlem, 1994".

[66] NISBO (1999), "NISBO-ouderenadviseurs, Rapport 1999: Belangrijke schakel in een integraal, toegankelijk en vraaggestuurd voorzieningenaanbod"; NISBO (2001), "NISBO-ouderenadviseurs, Rapport 2001: Belangrijke schakel in een integraal, toegankelijk en vraaggestuurd voorzieningenaanbod".

- Mechanisms of insecurity: Processes through which disadvantage may develop or intensify, including discrimination, inaccessible services and insufficient institutional coordination.
- Protective arrangements: Individual, social and institutional resources capable of preventing or mitigating adverse consequences.

This distinction is important because vulnerability does not necessarily produce insecurity. Its consequences depend partly on the availability and effectiveness of protection. For example, limited proficiency in the language of residence may create communication difficulties, but accessible interpretation and appropriate assistance can reduce their consequences. Likewise, financial disadvantage may constrain housing choices, while effective social protection may improve residential stability. The model consequently proposes that security outcomes are shaped by interactions between exposure, institutional conditions and protective resources rather than determined by individual characteristics alone. It also generates three propositions for future investigation: overlapping vulnerabilities may produce different outcomes across institutional contexts; accessible protection may moderate their consequences; and the effectiveness of representation may depend more on participation, accountability and service accessibility than on formal organisational recognition. These propositions remain theoretical and require empirical testing.

5.5. Implications for Research and Policy Development

The integrated framework suggests several directions for further research. Population-specific studies should distinguish older Muslim migrants from broader migrant and Muslim populations while recognising internal differences in gender, socioeconomic position, religious identification and migration history. Comparative European research should examine how national welfare arrangements, healthcare systems, housing policies and anti-discrimination mechanisms influence security. Longitudinal and mixed-methods designs may be particularly useful for investigating relationships between the five dimensions over time. Institutional protection also requires empirical assessment through indicators of accessibility, participation, service outcomes and organisational sustainability. Formal recognition or the existence of community organisations cannot alone demonstrate effective protection.

For policy development, the framework suggests combining universal rights with context-sensitive implementation. Equal legal entitlements may not ensure equitable access where communication barriers, administrative procedures or discriminatory practices restrict their

practical exercise. These priorities are consistent with the World Health Organization's UN Decade of Healthy Ageing (2021–2030), which emphasises age-friendly environments, combating ageism, integrated person-centred care and access to long-term care.[67]

The five-dimensional framework may therefore serve as a preliminary structure for identifying unmet needs and examining whether policies address interconnected forms of insecurity. Its practical application, however, requires empirical evaluation and participation by older migrants themselves.

5.6. Theoretical Contribution and Future Directions

The principal contribution of this article is the integration of five human security dimensions within the intersecting contexts of ageing, migration and religious identity. Three features distinguish the proposed approach.

- First, a life-course perspective connects later-life security with migration histories, employment experiences, socioeconomic resources and changing social relationships.
- Second, intersectionality provides a means of examining how age, gender, migration background, religious identification and institutional conditions may interact in shaping security.
- Third, institutional protection and representation are conceptualised simultaneously as a distinct component of human security and as a cross-cutting mechanism influencing the other dimensions.

This contribution builds on, rather than replaces, existing scholarship concerning migrant ageing, structural inequalities and equitable care.[68]

The framework remains conceptual and does not establish statistically independent dimensions or causal relationships. Future studies should therefore develop population-sensitive indicators, examine its applicability across European settings and evaluate protective mechanisms through comparative empirical research. Such research should involve older Muslim migrants as active

[67] WHO (2021), *Decade of Healthy Ageing: Baseline report*, World Health Organization.
[68] Saloua Berdai Chaouni (2026), "Toward equitable dementia care for older migrants: a new conceptual framework", pp. 247–279; Semra Çamuka & Ercan Gön & Uğur Çoban (2021), "Yoksulluk Kiskacindaki Afrika'da Tarim Politikalarinin Geliştirilmesinde Selem'in Rolü", *Africania*, 1(2), pp. 16–27; Maria Kristiansen & Oliver Razum & Hürrem Tezcan-Güntekin & Allan Krasnik (2016), "Aging and health among migrants in a European perspective".

participants in defining security concerns, assessing institutional responses and identifying appropriate forms of protection.

The framework ultimately offers a basis for analysing human security not merely through exposure to disadvantage but through the relationships between structural conditions, institutional responsibilities and individual and collective agency.

Conclusion and Policy Implications

This article has examined multidimensional human security among older Muslim migrants in Europe through an integrated framework connecting ageing, migration history, religious identity and institutional conditions. Drawing on interdisciplinary scholarship and selected historical evidence, it has identified five interrelated dimensions: physical security, psychosocial security, health and care security, housing and economic security, and cultural, religious and institutional security.

The analysis suggests that insecurity cannot be attributed to ageing, migration background or Muslim identity alone. Rather, it may emerge through interactions between individual circumstances, socioeconomic inequalities, discrimination and the accessibility of protective institutions. These relationships vary across individuals and national contexts, making it essential to avoid treating older Muslim migrants as a homogeneous or inherently vulnerable population.

The article's principal theoretical contribution lies in adapting human security to the circumstances of later migrant life while incorporating intersectionality and institutional representation. Institutional protection emerges both as a distinct component of security and as a cross-cutting mechanism potentially influencing access to healthcare, housing, social participation and fundamental rights.

The historical experiences of TISBO and NISBO in the Netherlands illustrate how migrant organisations sought to translate identified needs into collective advocacy, housing initiatives, advisory services and policy engagement. Their experiences also highlight the importance of distinguishing institutional recognition and documented activities from demonstrated outcomes and long-term sustainability.

Several policy implications follow from this analysis. First, European ageing and social protection policies should combine universal entitlements with practical measures addressing inequalities in access. Second, healthcare, housing and welfare institutions should strengthen

communication accessibility, equitable treatment and coordination across services. Third, older migrants should participate meaningfully in identifying needs, developing programmes and evaluating institutional responses. Fourth, cooperation between public authorities and accountable community organisations should support accessible and sustainable protection without transferring governmental responsibilities to civil society.

Future research should investigate the proposed dimensions through population-specific, comparative and longitudinal studies. Particular attention is needed to the relationships between discrimination, socioeconomic circumstances, institutional accessibility and measurable security outcomes. The framework itself also requires empirical testing before being employed as a validated assessment instrument.

Ultimately, protecting human security among older Muslim migrants involves more than responding to individual vulnerabilities. It requires institutional environments in which dignity, autonomy, equal rights and meaningful participation can be maintained throughout later life. By connecting these concerns within a multidimensional framework, the article offers a conceptual foundation for more inclusive ageing research and policies in European societies.

BIBLIOGRAPHY

- ACB & TISBO (1994), "Woonwensen Turkse Ouderen 1994 - Een samenvatting en vergelijk van de resultaten van negen monitorgesprekken met Turkse ouderen te Haarlem", Zenodo. DOI: https://doi.org/10.5281/zenodo.23449620.
- ACB/RCB (1995), *Oud worden in Haarlem – Een onderzoek naar de zorgbehoeften van Turkse en Marokkaanse ouderen in Haarlem*, 30132 – Archief van het Amsterdams Centrum Buitenlanders, Date of Accession: 01.09.2026 from https://archief.amsterdam/archives/pdf/30132.ead.pdf.
- Ahaddour, Chaïma & Van Den Branden, Stef & Broeckaert, Bert (2016), "Institutional Elderly Care Services and Moroccan and Turkish Migrants in Belgium: A Literature Review", *Journal of Immigrant and Minority Health*, 18(5), pp. 1216–1227. DOI: https://doi.org/10.1007/s10903-015-0247-4.
- Berdai Chaouni, Saloua (2026), "Toward equitable dementia care for older migrants: a new conceptual framework", *International Journal of Ageing and Later Life*, 19(2), pp. 247–279. DOI: https://doi.org/10.3384/ijal.1652-8670.5679.
- Berdai Chaouni, Saloua & Smetcoren, An-Sofie & De Donder, Liesbeth (2020), "Caring for migrant older Moroccans with dementia in Belgium as a complex and dynamic transnational network of informal and professional care: A qualitative study", *International Journal of Nursing Studies*, 101, 103413. DOI: https://doi.org/10.1016/j.ijnurstu.2019.103413.
- Bettayeb, Leila & Jaffré, Yannick & Chiaroni, Jacques & Ennomany, Yassine & Villani, Patrick & Couderc, Anne-Laure (2023), "Accès aux soins d'une population d'anciens travailleurs immigrés vivant en foyer", *Santé Publique*, 35(5), pp. 13–17. DOI: https://doi.org/10.3917/spub.235.0013.
- Blake, Margaret & Bowes, Alison & Gill, Valdeep & Husain, Fatima & Mir, Ghazala (2017), "A collaborative exploration of the reasons for lower satisfaction with services among Bangladeshi and Pakistani social care users", *Health & Social Care in the Community*, 25(3), pp. 1090–1099. DOI: https://doi.org/10.1111/hsc.12411.
- Çamuka, Semra & Gön, Ercan & Çoban, Uğur (2021), "Yoksulluk Kiskacindaki Afrika'da Tarim Politikalarinin Geliştirilmesinde Selem'in Rolü", *Africania*, 1(2), pp. 16–27.

- Conkova, Nina & Van den Broek, Thijs (2025), "Long-term care use among older migrants in the Netherlands: What to expect in the next decade?", *Journal of Aging & Social Policy*, 37(5), pp. 875–891. DOI: https://doi.org/10.1080/08959420.2024.2384195.
- Crenshaw, Kimberlé (2013), "Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics", in (eds. by Karen J. Maschke) *Feminist Legal Theories*, London: Routledge, pp. 23–51.
- FRA (2024), *Being Muslim in the EU: Experiences of Muslims*, European Union Agency for Fundamental Rights, Date of Accession: 01.09.2026 from https://fra.europa.eu/en/publication/2024/being-muslim-eu?utm.
- Gürbüz, Sait & Şahin, Faruk (2014), *Sosyal Bilimlerde Araştırma Yöntemleri*, Ankara: Seçkin Yayıncılık.
- Kevern, Peter & Lawrence, Dawn & Nazir, Nargis & Tsaroucha, Anna (2023), "Religious Influences on the Experience of Family Carers of People with Dementia in a British Pakistani Muslim Community", *Healthcare*, 11(1), 120. DOI: https://doi.org/10.3390/healthcare11010120.
- Kloosterboer, Dirk & Yılmaz, Berna (1997), *De leefsituatie van moslimouderen in Rotterdam*, Nederlandse Islamitische Bond voor Ouderen (NISBO), Date of Accession: 01.09.2026 from https://books.google.com.tr/books?id=_XOnGwAACAAJ.
- Kloosterboer, Dirk & Yılmaz, Berna (1999), "NISBO Beleidsvisie: Een gemiste kans? Oudere migranten in het grotestedenbeleid", Rotterdam: Zenodo. DOI: https://doi.org/10.5281/zenodo.23639876.
- Kristiansen, Maria & Razum, Oliver & Tezcan-Güntekin, Hürrem & Krasnik, Allan (2016), "Aging and health among migrants in a European perspective", *Public Health Reviews*, 37(1), 20, pp. 1-14. DOI: https://doi.org/10.1186/s40985-016-0036-1.
- NISBO (1995), *Founding Statutes of the Netherlands Islamic Elderly Union*, Amsterdam: Netherlands Islamic Elderly Union.

- NISBO (1998), "Ontluikende diversiteit in het lokale ouderenbeleid, Een discussienotitie over knelpunten en oplossingsstrategieen", Rotterdam: Zenodo. DOI: https://doi.org/10.5281/zenodo.23638590.
- NISBO (1998), "Enkele kanttekeningen bij het SCP-rapport "De eerste generatie in de derde levensfase"", Rotterdam: Zenodo. DOI: https://doi.org/10.5281/zenodo.23637681.
- NISBO (1999), "NISBO-ouderenadviseurs, Rapport 1999: Belangrijke schakel in een integraal, toegankelijk en vraaggestuurd voorzieningenaanbod", Rotterdam: Zenodo. DOI: https://doi.org/10.5281/zenodo.23641808.
- NISBO (2001), "NISBO-ouderenadviseurs, Rapport 2001: Belangrijke schakel in een integraal, toegankelijk en vraaggestuurd voorzieningenaanbod", Rotterdam: Zenodo. DOI: https://doi.org/10.5281/zenodo.23642218.
- NISBO (2002), "NISBO-Werkplan 2002: Institutioneel jaarwerkplan en beleidsdocument", Rotterdam: Zenodo. DOI: https://doi.org/10.5281/zenodo.23647115.
- OECD & European Commission (2023), *Indicators of Immigrant Integration 2023: Settling In*, OECD Publishing. DOI: https://doi.org/10.1787/1d5020a6-en.
- Örmeci, Ozan (2018), "2017 Almanya Federal Seçimleri ve SPD'nin Türkiye ile İlişkilere ve Almanya'daki Türklere Bakışı", *EURO Politika*, 01.10.2018, pp. 201–230, IZ: https://izlik.org/JA36PM87UB.
- Örmeci, Ozan (2024), "Türkiye's New Multi-Dimensional Foreign Policy", *Russian Law Journal*, 12(2), pp. 86–99.
- Pot, Anna & Keijzer, Merel & de Bot, Kees (2018), "De taalbarrière bij oudere Turkse vrouwen nader onderzocht", *Tijdschrift voor Gerontologie en Geriatrie*, 49(6), pp. 274–282. DOI: https://doi.org/10.1007/s12439-018-0270-8.
- Şekercan, Aydın & Snijder, Marieke B & Peters, RJG & Stronks, Karien (2018), "Gaat zorggebruik in het land van herkomst onder oudere Turkse en Marokkaanse migranten gepaard met minder zorggebruik in Nederland? Een combinatie van HELIUS-data met Achmea registratiedata", *Tijdschrift voor Gerontologie en Geriatrie*, 49(6), pp. 253–262. DOI: https://doi.org/10.1007/s12439-018-0272-6.

- Snyder, Hannah (2019), "Literature review as a research methodology: An overview and guidelines", *Journal of Business Research*, 104, pp. 333–339. DOI: https://doi.org/10.1016/j.jbusres.2019.07.039.
- Taşcı, Cansu (2024), "Türk Emek Göçmenlerinin Ulusötesi Yaşlanma Deneyimleri", *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 41(2), pp. 383–406. DOI: https://doi.org/10.32600/huefd.1344567.
- Tezcan, Tolga (2018), "On the move in search of health and care: Circular migration and family conflict amongst older Turkish immigrants in Germany", *Journal of Aging Studies*, 46, pp. 82–92. DOI: https://doi.org/10.1016/j.jaging.2018.07.001.
- TISBO (1994), "Handleiding TISBO Afdelingen (1993-1996) - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond", Zenodo. DOI: https://doi.org/10.5281/zenodo.23454461.
- TISBO (1995), "TISBO Projecten 1995 - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond", Zenodo. DOI: https://doi.org/10.5281/zenodo.23483148.
- TISBO (1995), "TISBO Werkplan 1995 - Origineel historisch archiefdocument van de Turks-Islamitische Ouderen Bond", Zenodo. DOI: https://doi.org/10.5281/zenodo.23481800.
- Toker, Arzu (2022), "Bir araştırma metodolojisi olarak sistematik literatür incelemesi: Meta-sentez yöntemi", *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 22(2), pp. 313–340. DOI: https://doi.org/10.18037/ausbd.1227360.
- UN (2002), "Report of the Second World Assembly on Ageing, Madrid 2002", A/CONF.197/9, United Nations, Date of Accession: 01.09.2026 from https://docs.un.org/en/A/CONF.197/9.
- UN (2025), "Resolution Adopted by the Human Rights Council", A/HRC/RES/60/11, United Nations Human Rights Council, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/g25/170/83/pdf/g2517083.pdf.
- UN General Assembly (2012), "Follow-up to Paragraph 143 on Human Security of the 2005 World Summit Outcome", A/RES/66/290, Date of Accession: 01.09.2026 from https://documents.un.org/doc/undoc/gen/n11/476/22/pdf/n1147622.pdf.

- UNDP (1994), *Human Development Report 1994*, New York: UNDP (United Nations Development Programme), Date of Accession: 01.09.2026 from https://hdr.undp.org/content/human-development-report-1994.
- UNECE (2026), *Strengthening the Voice of Older Persons: Civil Society's Role in the MIPAA Review Process*, United Nations Economic Commission for Europe.
- Van der Lingen Adviseurs & ACB/RCB & TISBO (1994), "Programma's van eisen voor woonprojecten voor Turkse ouderen in Haarlem, 1994", Zenodo. DOI: https://doi.org/10.5281/zenodo.23457221.
- Van Tilburg, Theo G. & Fokkema, Tineke (2021), "Stronger feelings of loneliness among Moroccan and Turkish older adults in the Netherlands: in search for an explanation", *European Journal of Ageing*, 18(3), pp. 311–322. DOI: https://doi.org/10.1007/s10433-020-00562-x.
- Whittemore, Robin & Knafl, Kathleen (2005), "The integrative review: updated methodology", *Journal of Advanced Nursing*, 52(5), pp. 546–553, DOI: https://doi.org/10.1111/j.1365-2648.2005.03621.x.
- WHO (2015), *World Report on Ageing and Health*, Geneva, Date of Accession: 01.09.2026 from https://www.who.int/publications/i/item/9789241565042?utm.
- WHO (2021), *Decade of Healthy Ageing: Baseline report*, World Health Organization.
- WVC (1993), "Address by the Minister of Welfare, Health and Cultural Affairs, Ms. Hedy d'Ancona, at the national presentation meeting of the Turkish-Islamic Elderly Union (TISBO)", Zenodo. DOI: https://doi.org/10.5281/zenodo.23504075.
- Yılmaz, Cemal (2026), "The First European Housing Project for Older Turkish Migrants in Haarlem, the Netherlands, and Its Lasting Legacies (1993–2008)", SocArXiv, Date of Accession: 01.09.2026 from https://doi.org/10.5281/zenodo.23797990.
- Yıldız, Ayşe (2022), "Bir araştırma metodolojisi olarak sistematik literatür taramasına genel bakış", *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 22(2), pp. 367–386. DOI: https://doi.org/10.18037/ausbd.1227366.

- Yılmaz, Cemal (2026), "Islamic University of Rotterdam: From Interfaith Dialogue to Pluralistic Cooperation", *International Journal of Humanities and Social Science*, (16), pp. 279–298. DOI: https://doi.org/10.30845/ijhss.v16p24.