Nihat Ali Özcan[1]
Bölge Çalışmaları Program Danışmanı

Erol Başaran Bural[2]
Bölge Çalışmaları Program Danışmanı

DEĞERLENDİRME NOTU

BARIŞLA SAVAŞ ARASINDA YÖNÜNÜ KAYBETMEK: 72 SAATLİK HAZIRLIK ÇAĞRILARI

"Kişi kendinden bilir işi…"
Anonim

GİRİŞ

Savaşla barış arasında güvenliği nasıl tartışmalıyız? Bu soruya ışık tutan en iyi örneklerden biri, Fransa'da 11-12 Ekim 2026 tarihlerinde, yaklaşık 700 perakende satış noktasının endüstriyel soğutma sistemlerine yönelik yapılan siber saldırıdır. Saldırı, gıda tedarik zincirinde kopuşa ve paniğe yol açtı. Fransız Siber Krizler Koordinasyon Merkezi (Centre de coordination des crises cyber [C4], 2026, ss.1-3), eylemin İran Devrim Muhafızlarıyla bağlantılı *Shahid Kaveh* birimi tarafından yapıldığını iddia etti. Sanal araçlarla başlatılan bu müdahale; bir yandan ekonomik faaliyetlerin ve gündelik yaşamın kırılganlığını gözler önüne sererken, öte yandan ilan edilmemiş bir düşmanlığın en çarpıcı göstergelerinden biriydi. Bu örnek, savaş ilanı olmadan da sivil kritik altyapıların hedef alınabildiğini ve bu tür saldırıların gündelik yaşamı aksatabildiğini gösteriyor.

Avrupa'da yaşanan krizlerin, ne kadarının endemik sosyal, ekonomik, teknik nedenlerden, ne kadarının ise söz konusu kaosları fırsat alanı olarak gören aktörlerin planlı ve örtülü dış müdahalelerinden kaynaklandığı sorusu, son gelişmelerle birlikte gündemi daha fazla işgal edecek gibi görünüyor. Diplomasi ve müzakerenin çoğu zaman sorunları çözmekte yetersiz kalması, savaşların yüksek maliyeti ve uluslararası hukuk ile ahlakın, güçlü aktörlere getirdiği sınırlamalar, bu aktörleri yeni yöntemlere yöneltiyor. Teknolojinin demokratikleşmesi, toplumsal değişimin hızlanması ve

[1] https://www.tepav.org.tr/tr/ekibimiz/s/46
[2] https://www.tepav.org.tr/tr/ekibimiz/s/1528

Bu çalışmada ifade edilen bulgular, yorumlar, sonuçlar, öneriler ve görüşler tamamen yazar(lar)ına aittir. TEPAV'ın resmi görüşü değildir. © TEPAV, aksi belirtilmedikçe her hakkı saklıdır.

küreselleşme de söz konusu aktörlere sorumluluktan kaçmak için yeni imkanlar sunuyor. Dijital teknolojilerin ve yapay zekânın yaygınlaşması, bu teknolojilere erişim maliyetlerinin düşmesi ve toplumların teknolojik araçlara giderek daha bağımlı hâle gelmesi yeni kırılganlıklar yaratıyor. Bu gelişmeler, yukarıda sayılan diğer etkenlerle birlikte, küçük ve orta ölçekli devletlerin yanı sıra terör örgütleri, suç şebekeleri, özel şirketler ve bireyler gibi devlet dışı aktörlerin de küresel ölçekte asimetrik etki kapasitesini artırıyor.

Rusya-Ukrayna Savaşı, İran krizi, İsrail-Arap çatışmaları ve Arap Baharı deneyimi, bu gelişmelere doğrudan ya da dolaylı olarak taraf olan ülkelerde "halkların fikirlerini ve algılarını" şekillendirmenin, o ülkelerin kararlarını etkilemenin bir yolu olduğunu gösterdi. Üstelik internet, sosyal medya ve diğer teknolojik gelişmeler, bu hedefi hem genişletti hem de kolaylaştırdı. Bu etkiyi yaratmak için artık ne büyük bir sermayeye ve yatırıma ne de belirli bir mekâna ihtiyaç duyulmamaktadır.

Böylesine bir fırsat alanı elbette göz ardı edilemezdi. Aktörler, bir yandan bu fırsat alanından sistemli biçimde kendi amaçları doğrultusunda yararlanırken diğer yandan zayıf yönlerini güçlendirmenin de yollarını arıyorlar. Bu aktörlerin politik, ekonomik, toplumsal ve güvenlik amaçları doğrultusunda gerçekleştirecekleri müdahaleler, Batılı uluslararası ilişkiler ve istihbarat literatüründe "örtülü operasyon" (*covert action*) kavramı çerçevesinde tartışılmaktadır. Bu kapsamda örtülü operasyon (Johnson, 1989, ss.64-65), bir başka devletin siyasi, ekonomik veya güvenlik koşullarını etkilemek amacıyla, müdahaleyi gerçekleştiren aktörün kendi rolünü gizleyerek yürüttüğü faaliyetler olarak tanımlanmaktadır. Sovyetler Birliği ve mirasçısı Rusya, bu tür faaliyetleri "aktif tedbirler" (*active measure*) olarak adlandırmaktadır. Çin'in "Sınırsız Savaş" konsepti de, çatışmayı geleneksel askeri sınırların ötesine taşıyarak diplomatik, ekonomik, hukuki, teknolojik ve siber alanları da kapsar. İran ise benzer bir yaklaşımı "Yumuşak Savaş" olarak ifade etmektedir. Bu yaklaşımlar farklı adlarla anılsa da birçok alanda örtüşmektedir.

Bu çalışma, Avrupa ülkelerinin krizlere hazırlık çağrılarından hareketle savaş ile barış arasındaki gri alanda ortaya çıkan güvenlik risklerini ele almaktadır. Bu çerçevede örtülü operasyonların kavramsal ve tarihsel temellerini, kullanılan yöntemlerin birbirleriyle ilişkisini ve bu operasyonların gri alandaki rolünü incelemektedir.

1. 72 SAATLİK HAZIRLIK

Son aylarda Avrupa ülkeleri, olası krizlere hazırlık çağrılarında kısa süreli ancak yaygın hizmet kesintileri sırasında toplumsal yaşamın nasıl sürdürülebileceğine odaklanıyor. Örneğin Alman Hükümeti (BBK, 2025, ss.2-5), siber saldırı, dezenformasyon, sabotaj ve savaş dâhil çeşitli risklere karşı hanelerin en az 10 gün kendi kendine yetebilecek biçimde hazırlanmasını tavsiye etti. Fransa'da yayımlanan "*Tous Responsables*", yani "Hepimiz Sorumluyuz" rehberi, (SGDSN, 2025, ss.3-7) en az 72 saatlik hazırlığa ihtiyaç olduğunu vurguladı. Birleşik Krallık'ın "*Be Ready*", yani "Hazır Olalım" kampanyası ise (Cabinet Office, 2026) üç günlük temel ihtiyaç stokunu tavsiye etti. Bu belgelerdeki hazırlık süreleri ülkeden ülkeye değişiklik gösterse de aralarındaki farkı ülkelerin kendi risk değerlendirmeleri ve hane düzeyinde erişilebilir kaynaklar belirlemektedir.

Bu nedenle kamuoyunda sıkça gündeme gelen "üç günlük stok" önerisi, bir güvenlik standardı değildir. Bu süre, kamu hizmetlerinin geçici olarak kesintiye uğrayabileceği senaryolarda bireylerin ilk müdahale sürecini daha güvenli atlatmasını amaçlayan asgari bir tedbir süresi olarak okunmalıdır. Acil durum müdahalesindeki asli sorumluluğu devlet kurumları

sürdürmektedir. Bireysel hazırlık ise bu hizmetlere yönelebilecek ani talep baskısının yönetilmesini kolaylaştıran tamamlayıcı bir kapasite sunmaktadır.

Almanya, Fransa ve Birleşik Krallık'a benzer biçimde Hollanda Hükümeti de (NCTV, 2025, ss.2-6) vatandaşlarına 72 saatlik hazırlık çağrısı yaptı. Hollanda, "ülkenin savaşta olmamakla birlikte bütünüyle barış koşullarında da bulunmadığını" belirtti. Belçika (Belçika Ulusal Kriz Merkezi, 2026) ile Polonya (Polonya İçişleri ve İdare Bakanlığı, 2025, ss.20-22) da benzer şekilde hane dayanıklılığının artırılması gerektiğini ifade etti. İsveç (MSB, 2024, ss.3, 6, 15) ve Norveç (DSB, t.y.) en az bir haftalık hazırlık önerirken, Danimarka (Danish Emergency Management Agency, 2024) ve Finlandiya (Suomi, 2026) üç günlük temel hazırlıkla yetindi. Bu ulusal adımlara koşut olarak Avrupa Komisyonu, Mart 2025'te açıkladığı "Hazırlık Birliği Stratejisi" (*Preparedness Union Strategy*) ile AB genelinde en az 72 saatlik bireysel hazırlığı ve kritik kamu hizmetlerinin dayanıklılığını gündeme taşıdı (Avrupa Komisyonu, 2025, ss.1-2).

Avrupa hükümetlerinin bu çağrıları yalnızca konvansiyonel savaş tehdidinden kaynaklanmamakta, doğal afet, salgın, teknik arıza ve insan kaynaklı saldırılar gibi çok boyutlu riskleri de kapsamaktadır. Uyarıların ortak noktası, elektrik, su, haberleşme, ulaşım ve gıda tedarikinde yaşanabilecek olası kesintilerin toplum üzerindeki yıkıcı etkisini en aza indirmektir. Avrupa Birliği Konseyinin Mart 2026 tarihli değerlendirmesi de sabotaj, siber faaliyetler, seçimlere müdahale ve dezenformasyonun eş güdümlü biçimde kullanılabildiğine, özellikle Rusya kaynaklı hibrit tehditlerin yarattığı risklere dikkat çekmiştir (Avrupa Birliği Konseyi, 2026, ss.2-5).

Özellikle, enerji ve haberleşme kesintileri, etkilenen sektörün sınırlarını aşabilen geniş çaplı sonuçlar doğurmaktadır. Fransa'daki "siber sabotaj" vakalarında da görüldüğü üzere, kritik altyapılar hedef alındığında ödeme sistemleri, lojistik ağlar ve hastaneler gibi hayati yapıların tamamı domino etkisiyle eş zamanlı olarak işlevsiz hâle gelebilmektedir. Söz konusu hazırlık stratejileri, yalnızca bir tehdidin ortaya çıkma olasılığıyla değil, gerçekleşmesi hâlinde farklı sektörlerin bundan zincirleme biçimde nasıl etkileneceğiyle de yakından ilgilidir. Avrupa'daki kurumsal açıklamaların güvenlik bakımından bir diğer önemli yönü, doğrudan sıcak bir askerî çatışma yaşanmadan da geniş çaplı olağanüstü durumların ortaya çıkabileceğini kabul etmeleri ve risk yönetimini merkezi yönetimle sınırlı tutmayıp birey/vatandaş düzeyine kadar yaymalarıdır.

Avrupa'da güvenlik kaygıları yükselirken, Fransa'da hayat pahalılığı, ücret politikaları, eğitim ve kamu hizmetleriyle ilgili örtülü operasyonların tekniklerinden biri olan geniş katılımlı protestolar da yaşandı. Fransız İçişleri Bakanlığının (2026) açıkladığı verilere göre 17 Ekim'de yaklaşık 550.000, 5 Kasım'da ise 575.000 kişi bu gösterilere katıldı. Ne var ki bu protestolar ile siber sabotaj arasındaki bağ henüz kanıtlanamıştır. İnkar edilebilir örtülü operasyon ihtimalinin siber ortamla sınırlı olmadığını gösteren bir başka gelişme, Polonya'nın Wola Krobowska bölgesindeki Starlink uydu haberleşme istasyonuna 23 Eylül 2026 tarihinde düzenlenen sabotajdır. Polonya İç Güvenlik Ajansı (Agencja Bezpieczeństwa Wewnętrznego, 2026), yangının kasıtlı çıkarıldığını, iki şüphelinin Almanya'da yakalandığını ve soruşturmanın yabancı bir istihbarat servisi yararına hareket edildiği şüphesini de kapsadığını açıkladı. Alman basınında (Deutsche Welle, 2026), saldırının Türkiye'de faaliyet gösteren "Daltonlar" adlı organize suç örgütü tarafından gerçekleştirildiği ve faillerin Rus istihbaratı adına hareket etmiş olabileceği öne sürüldü.

Avrupa güvenlik ortamının psikolojik boyutunu görünür kılan bir başka örnek, 11-12 Kasım 2026 tarihlerinde okullara gönderilen bomba ihbarlarıdır. İtalya'da 11 Kasım'da yaklaşık 6.300 okula, ertesi gün ise 3.778 okula tehdit mesajları ulaştı. İskoçya, Kuzey İrlanda ve İrlanda

Cumhuriyeti'nde de çok sayıda eğitim kurumu benzer mesajlar aldı. Fransa'da yayılan benzer e-postalar nedeniyle, bazı eğitim kurumları güvenlik amacıyla boşaltıldı (Sky News, 2026). Gerçek bir patlayıcı bulunmasa bile bu tür ihbarlar eğitim hizmetlerinin aksamasına, kamu güvenliği birimlerinin meşgul edilmesine ve toplumda korku ortamı oluşmasına yol açtı (Amante, 2026; Sky News, 2026). Bununla birlikte ihbarların tek bir merkezden yönetildiği ya da yabancı bir devlet tarafından organize edildiği de kesinleşmemiştir. Fransa Cumhurbaşkanı Emmanuel Macron da yabancı güçlere sorumluluk atfetmek için yeterli kanıt bulunmadığını açıklamıştır (Sözcü, 2026). Reuters'ın (2026b) haberine göre ise Norveçli enerji şirketi Equinor, 17 Kasım 2026'da bazı bilgi teknolojisi sistemlerini hedef alan bir siber saldırı tespit ettiğini, önlem aldığını ve enerji üretiminde kesinti gözlemediğini duyurdu.

Avrupa'nın yanı sıra ABD'de yaşanan teknik arızalar da temel hizmetlerdeki aksamaların, bir saldırı söz konusu olmadan da, sektörler arasında nasıl yayılabildiğini gösteriyor. Microsoft'un 12 Kasım 2026'da başlayan hizmet kesintisi, Outlook, Teams ve diğer Microsoft uygulamalarına erişimi önemli ölçüde aksattı. Reuters'ın (2026c) aktardığına göre şirket, sorunu ağ kapasitesi ve sunucu altyapısındaki teknik işlemlerle ilişkilendirdi; kötü niyetli bir siber faaliyete ilişkin bulgu açıklamadı. Bu örnek, ortak dijital hizmet sağlayıcılarına bağımlılığın, kamusal ve özel faaliyetlerde geniş ölçekli aksamalara yol açabileceğini gösterdi.

ABD Federal Havacılık İdaresinin 13 Kasım 2026'da yaşadığı iletişim altyapısı arızası, ülke çapında geçici olarak uçşların durdurulmasna neden oldu. Reuters'ın haberinde (2026d), arızanın eski sistemlerle yeni ağ donanımı arasındaki uyumsuzluklarla ilişkilendirildiği, arızadan etkilenen hava ulaşımında üç güne yayılan çok sayıda iptal yaşandığı ve yetkililerin olayı siber saldırı olarak tanımlamadığı bildirildi. ABD'deki kesinti dizisi 16-17 Kasım'da farklı sektörlerde devam etti. Associated Press'in (2026) haberine göre 16 Kasım'da JPMorgan Chase'in işlem sistemindeki yazılım sorunu, bazı bankalar arası ödemeleri ve "Zelle" üzerinden gerçekleştirilen işlemleri geciktirdi. Reuters'ın (2026c) haberinde aynı gün United Airlines'ın uçuş operasyonlarında teknik aksamalar yaşandığı belirtildi.

Dijital hizmet kesintileri Apple'ın 10 Kasım'da iCloud ve kullanıcı hesabı hizmetlerinde yaşadığı erişim sorunlarıyla da gündeme geldi (Miller, 2026). Haberlere göre (Reuters, 2026a) şirketin 17 Kasım'da Apple Pay ve iCloud dâhil bazı hizmetlerinde ortaya çıkan yeni kesintiler kurum içi bir güncellemeden kaynaklandı. Şirket bunun bir siber saldırı olmadığını bildirdi. Bu olaylarla aynı gün ABD Ulusal Güvenlik Ajansının (*National Security Agency*-NSA) NSANet adlı kurum içi gizli haberleşme ağında da kesinti meydana geldi. Yayımlanan bir başka habere göre (Toropin ve Tucker, 2026) NSA açıklamasında, sorunun rutin bakım sırasında oluştuğu ve kritik görev kabiliyetlerinin işlerliğini koruduğu belirtildi. ABD Ulusal İstihbarat Direktörü Jay Clayton (Murray ve Deliso, 2026) söz konusu kesintilerde koordineli bir siber saldırı veya devlet destekli bir faaliyet işareti görülmediğini açıkladı. Dışişleri Bakanı Marco Rubio da olayların birbirinden farklı teknik nedenlere dayandığını belirtti.

Batılı ülkelerde son günlerde meydana gelen bu olaylar birlikte değerlendirildiğinde "72 saatlik hazırlık" çağrılarının anlamı daha açık hâle gelmektedir. Devletler, doğal afet ve teknik arızaların yanı sıra kasıtlı sabotaj, iletişim kesintisi, psikolojik baskı ve dezenformasyonun bir arada veya art arda ortaya çıkabileceği senaryolara da hazırlanmaya çalışmaktadır. Olası failin ve yönlendiricinin kim olduğu, eylemin hangi siyasi amaca hizmet ettiği ve farklı olaylar arasında kanıtlanabilir bir koordinasyon bulunup bulunmadığı ise asıl güvenlik sorusudur. Bu nedenle Avrupa'daki hazırlık politikaları, örtülü operasyonların araçlarını ve sınırlarını inceleyen kavramsal tartışmadan bağımsız düşünülemez. ABD Federal İletişim Komisyonunun (Federal Communications Commission [FCC], 2026), 17 Kasım 2026 tarihinde ülke genelinde

radyo ve televizyon yayınlarını kısa süreliğine keserek gerçekleştirdiği acil durum uyarı sistemi testi de devletlerin olası krizlerde toplumu bilgilendirme ve iletişim kapasitesini korumaya yönelik hazırlıklarının bir örneğidir. Dolayısıyla modern sivil hazırlık politikaları, krizleri tetikleyen veya derinleştiren ve faillerine makul inkâr edilebilirlik alanı sunan örtülü operasyonların araçlarını, sınırlarını ve yöntemlerini inceleyen kavramsal tartışmadan bağımsız düşünülemez.

2. ÖRTÜLÜ OPERASYONLAR: İNKAR EDİLEBİLİRLİK VE YÖNTEMLER

Devletler arasındaki rekabet, yalnızca diplomatik ilişkiler, ekonomik yaptırımlar veya doğrudan askerî güç kullanımı üzerinden yürümez. Barış koşullarında dahi devletler, rakiplerinin siyasi karar alma süreçlerini, ekonomik faaliyetlerini ve toplumsal dengelerini açık ya da örtülü araçlarla etkilemeye çalışır. George F. Kennan (1948, ss.668-669), 4 Mayıs 1948 tarihli değerlendirmesinde propaganda, ekonomik tedbirler, gizli siyasi destek ve yeraltı hareketlerinin teşvik edilmesini, savaş eşiğinin altında yürütülen siyasi mücadelenin (*political warfare*) araçları arasında sayar. Bu mücadele, Kennan'a göre hem açık hem de örtülü yöntemleri kapsamaktadır.

Bu çerçevede örtülü operasyonlar, bir devletin başka bir ülkedeki siyasi, ekonomik veya askerî koşulları kendi çıkarları doğrultusunda etkilemeyi amaçladığı faaliyetlerdir. Ancak burada devlet, müdahaledeki rolünü gizlemeyi ya da resmen üstlenmemeyi hedefler. Örtülü operasyonu belirleyen şey, yürütülen faaliyetin mutlaka gizli kalması değil, faaliyetin arkasındaki gerçek sorumlunun kimliğinin gizlenmesi, meydana gelen olayın gri alanda bırakılmasıdır. ABD Ulusal Güvenlik Konseyinin 1948 yılında yayımladığı NSC 10/2 direktifi (National Security Council [NSC], 1948), propaganda, ekonomik mücadele, sabotaj ve direniş hareketlerine desteği bu kapsamda değerlendirmiş, operasyonların gerektiğinde inkâr edilebilir biçimde yürütülmesini öngörmüştür.

Örtülü operasyonların diplomasi ile doğrudan askerî müdahale arasında bir "üçüncü seçenek" (Johnson, 2022, ss.4-6) olarak görülmesi, devletlerin dış politika hedeflerine ulaşmak için başvurduğu araçların ne kadar çeşitli olduğunu ortaya koyar. Ne var ki bu operasyonlar yalnızca barış dönemine özgü değildir, savaş öncesinde, sırasında ve sonrasında da uygulanabilir. Askerî harekâtın hazırlayıcısı ya da destekleyicisi olabildiği gibi doğrudan çatışmanın yerine de geçebilir. Galtung'un (1969, s.183) negatif ve pozitif barış ayrımı, silahlı çatışmanın bulunmamasının devletler arasındaki mücadelenin bittiği anlamına gelmediğini de gösterir.

Uygulanan yöntemlerin niteliği, örtülü operasyonları farklı alt disiplinlere ayırır. Johnson (2022, ss.19-39), geleneksel örtülü operasyonları propaganda, siyasi, ekonomik ve paramiliter faaliyetler üzerinden inceler. Dijital teknolojilerin gelişmesi ve bilgi sistemlerinin kritik altyapıların işleyişinde belirleyici hâle gelmesi ise bilgi savaşının ayrıca ele alınmasını gerekli kılmıştır. Bu çalışmada ekonomik faaliyetler, siyasi müdahalenin bir unsuru olarak değerlendirilmekte ve örtülü operasyonlar propaganda, politik aktivite, paramiliter faaliyetler ile bilgi savaşı başlıkları altında dört temel grupta incelenmektedir.

Örtülü faaliyetlerin hedefi yalnızca askerî bir tesis, devlet kurumu, siyasetçi veya bilgi sistemi değildir. Bu araçların nihai siyasi etkisi çoğu zaman toplumun algısına, güven duygusuna, gündelik tercihlerine ve yöneticiler üzerindeki baskısına yönelir. Propaganda kanaatleri, ekonomik müdahale geçim koşullarını, sabotaj kamu hizmetlerini, paramiliter faaliyet ise güvenlik algısını etkileyebilir. Dolayısıyla farklı yöntemleri birleştiren ortak nokta, halkın

davranışlarını ve bu davranışların siyasi karar alma süreçleri üzerindeki etkisini değiştirme potansiyelidir.

Propaganda

Propaganda, bir topluluğun düşüncelerini (Jowett & O'Donnell, 2019, ss.7-9), duygularını, inançlarını ve davranışlarını belirli bir amaç doğrultusunda etkilemek veya değiştirmek üzere bilginin sistemli biçimde üretilmesi, seçilmesi ve çeşitli iletişim araçlarıyla yayılmasıdır. Örtülü operasyonların en eski ve görece düşük maliyetli yöntemlerinden biri olan propaganda, hedef toplumda yeni düşünceler oluşturmayı amaçlayabileceği gibi mevcut kanaatleri güçlendirmeye, kuşkuları artırmaya veya belirli siyasi tercihlere yönlendirmeye de hizmet edebilir.

Propagandanın temel özelliği (Jowett & O'Donnell, 2019, ss.4-9), mutlaka yanlış bilgiye dayanması değildir. Gerçek olayların belirli yönlerinin öne çıkarılması, bazı bilgilerin görmezden gelinmesi ya da doğru bilgilerin hedef kitlenin duygusal tepkilerini artıracak biçimde sunulması da propaganda kapsamında değerlendirilebilir. Dolayısıyla propaganda yalnızca bilgi aktarmayı değil, bilginin hedef toplum tarafından nasıl algılanacağını da etkilemeyi hedefler. Kullanılan bilginin niteliği ve kaynağın açıklığı bakımından propaganda faaliyetleri beyaz, gri ve kara propaganda olmak üzere üçe ayrılmaktadır.

Kaynağı açıkça bilinen ve genel olarak doğrulanabilir bilgilere dayanan propaganda türü (Kennan, 1948, ss.668-669; Johnson, 2022, ss.19-22; Jowett & O'Donnell, 2019, ss.20-21), beyaz propagandadır. Bu yöntemde gerçek olaylar, belgeler ve açıklamalar belirli bir siyasi görüşü destekleyecek şekilde kullanılır. Soğuk Savaş döneminde ABD'nin Sovyet yönetiminin açıklamalarıyla çelişen bilgileri kamuoyuna ulaştırmaya çalışması ve sansürlenen yayınları desteklemesi, bu yaklaşımın örnekleri arasında sayılabilir. Kaynağını gizlemediği için tek başına örtülü operasyon niteliği taşımayan beyaz propaganda, daha geniş bir siyasi mücadele stratejisinin parçası olabilmektedir.

Gri propagandada ise (Jowett & O'Donnell, 2019, ss.24-28) bilginin kaynağı belirsizdir. Gerçek destekleyici gizlenir veya doğruluk kolaylıkla teyit edilemez. Bir devletin, başka bir ülkenin akademisyenlerine, gazetecilerine ya da kanaat önderlerine kendi politikalarını destekleyen içerikler hazırlatması ve bu ilişkiyi kamuoyundan gizlemesi buna örnek gösterilebilir. Bu yöntemde her zaman tamamen yanlış bilgi üretilmesi gerekmez, çoğu zaman gerçek bilgiler seçici biçimde kullanılarak belirli bir siyasi görüşün bağımsız kaynaklarca desteklendiği izlenimi yaratılır. Gri propagandanın etkisi, mesajı hazırlayan veya finanse eden gerçek aktörün bilinmemesinden doğar.

Bilginin kaynağının kasıtlı olarak yanlış gösterildiği (U.S. Department of State, 1981, ss.1-3; Jowett & O'Donnell, 2019, ss.21-24; Rid, 2020), sahte belgelerin, uydurma haberlerin veya aldatıcı kimliklerin kullanıldığı faaliyetler ise kara propaganda kapsamındadır. Bu yöntemde propaganda mesajı, gerçekte onu hazırlamayan bir kişi, kurum veya devlete aitmiş gibi sunulabilir. Soğuk Savaş döneminde Sovyetler Birliği'nin sahte belgeler, paravan yayınlar ve etki ajanları aracılığıyla yürüttüğü faaliyetler, kara propagandanın tarihsel örnekleri arasındadır. Kara propagandayı gri propagandadan ayıran nokta, kaynağın gizlenmesinin ötesinde mesajın başka bir kaynaktan geliyormuş gibi gösterilmesidir.

Propaganda faaliyetlerinde kullanılan önemli yöntemlerden biri de dezenformasyondur. Kasıtlı biçimde yanlış veya yanıltıcı bilginin üretilmesi ve dolaşıma sokulması anlamına gelen dezenformasyon; sahte haberler, değiştirilmiş görüntüler, uydurma belgeler ve gerçek bilgilerin yanıltıcı bağlamlarda kullanılması yoluyla gerçekleştirilebilir. Ancak propaganda ile

dezenformasyon eş anlamlı değildir: propaganda doğru bilgilere dayanabildiği hâlde dezenformasyonda belirleyici olan, kasıtlı yanıltma unsurudur. Rid (2020), Sovyet aktif tedbirlerinin yalnızca sahte bilgi üretmekten ibaret olmadığını, gerçek olayların manipüle edilmesi, kaynakların gizlenmesi ve toplumsal ayrışmaların derinleştirilmesi gibi yöntemleri de kapsadığını göstermektedir.

Propagandanın sonuçları (Johnson, 2022, ss.19-39; Jowett & O'Donnell, 2019) çoğu zaman kısa sürede ortaya çıkmaz. Toplumların yerleşmiş inançlarını değiştirmek zaman alabildiği gibi, propaganda sonucunda oluşan tutum değişikliklerini diğer siyasi ve ekonomik gelişmelerden ayırmak da güçtür. Bu nedenle propagandanın başarısı yalnızca yayımlanan içerik sayısı veya ulaşılan kişi miktarıyla ölçülemez. Asıl ölçüt, hedef kitlenin düşünce ve davranışlarında amaçlanan değişikliğin gerçekleşip gerçekleşmediğidir. Propaganda tek başına kullanılabildiği gibi diplomatik girişimleri, ekonomik politikaları ve diğer örtülü operasyon faaliyetlerini destekleyen tamamlayıcı bir araç olarak da işlev görebilmektedir.

Politik Faaliyetler

Bir devletin başka bir ülkenin siyasi karar alma mekanizmalarını (Johnson, 2022, ss.19-21), yöneticilerini, siyasi partilerini veya toplumsal hareketlerini etkilemek amacıyla yürüttüğü örtülü faaliyetler politik aktivite kapsamındadır. Bu faaliyetler, propagandadan farklı olarak yalnızca düşünce ve kanaatlerin değiştirilmesiyle sınırlı kalmaz. Seçim süreçlerinin etkilenmesi, siyasi partilerin veya adayların desteklenmesi, toplumsal hareketlerin yönlendirilmesi ve hükümetler üzerinde baskı oluşturulması gibi doğrudan siyasi sonuçlar hedeflenir.

Hedef ülkede tercih edilen siyasi adaylara (Johnson, 2022, ss.19-20) veya partilere gizli finansman, danışmanlık, medya desteği ve örgütsel yardım sağlanması, örtülü siyasi müdahalelerin en bilinen yöntemlerinden biridir. Bunun yanında etki ajanları ve aracı kuruluşlar kullanılarak karar vericilere ulaşılması, kamuoyu üzerinde etkili kişilerin belirli politikaları desteklemeye yönlendirilmesi ya da toplumsal hareketlerin dolaylı biçimde teşvik edilmesi de bu kapsamda değerlendirilebilir. Bu faaliyetlerde operasyonun örtülü niteliğini belirleyen temel unsur, müdahaleyi gerçekleştiren devlet ile desteklenen aktör arasındaki ilişkinin gizlenmesidir.

Örtülü siyasi müdahalelerin tarihsel örneklerinden biri, 1953'te İran Başbakanı Muhammed Musaddık'ın devrilmesidir. Yayımlanan gizliliği kaldırılmış CIA belgeleri (National Security Archive, 2013) ABD ve Birleşik Krallık bağlantılı gizli müdahalenin rolünü ortaya koymaktadır. Dönemin operasyonu uzun yıllar sonra diplomatik ve ahlaki tartışmaların konusu olmaya devam etmiş, ABD Başkanı Barack Obama (2009) da 4 Haziran 2009 tarihli Kahire konuşmasında, ülkesinin demokratik yollarla seçilmiş İran hükümetinin devrilmesinde rol oynadığını kabul etmiştir.

Benzer bir örnek, 1960'ta bağımsızlığına kavuşan Kongo'nun ilk başbakanı Patrice Lumumba'nın iktidardan uzaklaştırılması sürecidir. ABD Dışişleri Bakanlığı Tarih Ofisinin yayımladığı resmî kayıtlar (U.S. Department of State, Office of the Historian, t.y.-b), Washington'un Lumumba'yı devre dışı bırakmak amacıyla siyasi aktörlere gizli destek sağladığını ve CIA bünyesinde suikast planları geliştirildiğini göstermektedir. Lumumba 17 Ocak 1961'de Kongolu rakipleri tarafından öldürülmüştür.

Küba'da Fidel Castro'nun devrilmesini hedefleyen girişimler ise siyasi müdahale ile paramiliter faaliyetler arasındaki geçişkenliğin bir örneğidir. ABD Senatosunun Church Komitesi raporu (U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1975, ss.71-72), 1960–1965 arasında Castro'yu öldürmeye yönelik CIA bağlantılı en az sekiz ayrı plan için somut kanıt bulunduğunu bildirmiştir. Bunların bir kısmı

planlama safhasını aşmamış, bazıları ise suç dünyasından aracılar veya farklı sabotaj araçları kullanma girişimlerine dönüşmüştür. Bu belgelerin sonradan kamuoyuna açılması, başarısız kalsa bile örtülü operasyonların uzun yıllar sonra siyasi hesap verebilirlik, hukuki meşruiyet ve etik sorumluluk tartışmalarını yeniden başlatabileceğini göstermektedir.

Siyasi müdahalelerin önemli bir bileşeni de ekonomik faaliyetlerdir. İşçi hareketleri (NSC, 1948, ss.713-715; Johnson, 2022, ss.19-20), grevler, üretim kesintileri, finansal istikrarsızlık ve tedarik zincirlerindeki aksamalar, belirli koşullarda siyasi baskı oluşturmak amacıyla kullanılabilir. Hedef ülkenin ekonomik faaliyetlerinin gizlice sekteye uğratılması, sahte para yoluyla ekonomik güvenin sarsılması veya kritik üretim ve dağıtım sistemlerine müdahale edilmesi, siyasi sonuç yaratmayı amaçlayan ekonomik örtülü faaliyetlere örnek gösterilebilir.

Ekonomik örtülü faaliyetlerin etkileri, doğrudan hedef alınan kurum veya sektörle sınırlı kalmayabilir. Enerji, ulaşım, haberleşme ve üretim altyapılarında ortaya çıkan kesintiler ekonomik hayatın diğer alanlarına yayılarak hükümetlere yönelik toplumsal memnuniyetsizliği artırabilir. Bu nedenle ekonomik araçlar kimi zaman doğrudan maddi kayıp yaratmaktan çok, hedef ülkenin yönetim kapasitesine ve siyasi meşruiyetine duyulan güveni zayıflatmak için kullanılabilmektedir.

Siyasi faaliyetlerin yürütülme biçimini dijital teknolojiler de değiştirmiştir. 2016 ABD başkanlık seçimlerinde Donald Trump'ın seçim kampanyasının Facebook'un (Federal Trade Commission [FTC], 2019; Broussard & Weintraub, 2021, ss.1-3) hedefli reklamcılık imkânlarından ve Cambridge Analytica adlı veri analiz şirketinin hizmetlerinden yararlanması, bunun dikkat çekici örneklerinden biridir. Bu olay, dijital ortamda elde edilen kişisel bilgilerin siyasi tercihleri etkilemek amacıyla nasıl kullanılabildiğini göstermesi bakımından son derece önemlidir.

ABD Senatosu İstihbarat Komitesinin incelemesi de (U.S. Senate Select Committee on Intelligence, 2019, ss.3-5) Rusya bağlantılı Internet Research Agency'nin 2016 seçimlerinde sahte sosyal medya kimlikleri ve hedefli içerikler kullanarak Hillary Clinton'ın seçim şansını azaltmayı ve Trump'ı desteklemeyi amaçlayan ayrı bir etki kampanyası yürüttüğünü ortaya koymuştur. İki örnek birlikte değerlendirildiğinde, dijital platformların hem açık siyasi kampanyalara hem de kaynağı gizlenen dış müdahale faaliyetlerine imkân tanıdığı görülür.

Paramiliter Faaliyetler

Örtülü operasyonların doğrudan fiziksel güç kullanımıyla en fazla ilişkili alt disiplini paramiliter faaliyetlerdir. Silahlı grupların desteklenmesi, gerilla gruplarına eğitim, teçhizat ve lojistik yardım sağlanması, sabotaj ve belirli koşullarda rejim değiştirmeye yönelik girişimler bu faaliyetler kapsamındadır. Temel özelliği, müdahaleyi gerçekleştiren devletin düzenli askerî birliklerini açık biçimde kullanmadan başka bir ülkedeki gelişmeleri etkilemeye çalışmasıdır (Johnson, 2022, ss.19-39). Bu yöntemde çoğunlukla yerel silahlı gruplar, direniş hareketleri veya vekil aktörler kullanılır; böylece müdahaleci devlet, doğrudan askerî çatışmaya girmeden hedef ülke üzerinde baskı oluşturabilir. Ne var ki vekil aktörler üzerinden yürütülen faaliyetlerde önemli sorunlar da çıkabilmektedir.

Devlet dışı aktörlerin paramiliter faaliyetlerinin devletler arasındaki stratejik rekabetle kesişebileceğine ilişkin kayda değer bir örnek, 5 Ağustos 2008 tarihinde Bakü-Tiflis-Ceyhan (Özcan, 2008) petrol boru hattına yönelik saldırıdır. PKK'nın sorumluluğunu üstlendiği saldırının, Rusya'nın Gürcistan'a yönelik askerî müdahalesinden yalnızca iki gün önce gerçekleşmesi dikkat çekicidir. Nitekim İngiltere Avam Kamarası Savunma Komitesi (2009,

para. 64) de saldırının gerçek failleri ve bölgesel enerji rekabetiyle olası bağlantıları hakkındaki farklı değerlendirmelere yer vermiştir.

Diğer örtülü operasyon türlerine göre paramiliter faaliyetler daha yüksek maliyet ve risk taşıyabilir. Propaganda veya sınırlı siyasi müdahaleler zaman içinde fark edilmeden sürdürülebilirken, silahlı faaliyetlerin sonuçlarını gizlemek çoğu zaman daha güçtür. Dolayısıyla operasyonun gizli hazırlanması, ortaya çıkan askerî ve siyasi sonuçların da gizli kalacağı anlamına gelmez. 1961 yılında ABD'nin desteklediği Kübalı sürgünlerin Domuzlar Körfezi çıkarmasının (U.S. Department of State, Office of the Historian, t.y.-a) başarısızlıkla sonuçlanması, örtülü paramiliter faaliyetlerin kontrol edilemeyen sonuçlarına ilişkin önemli bir tarihsel örnektir. Paramiliter faaliyetlerin kapsamı, silahlı çatışmanın doğrudan desteklenmesinden ibaret değildir. Müttefik unsurların eğitilmesi, özel operasyon kapasitesinin geliştirilmesi ve belirli personelin tehlikeli bölgelerden tahliyesi de bu alanda kullanılan kabiliyetlerle ilişkili olabilir.

Bilgi Savaşı

Dijital teknolojilerin gelişmesiyle siber alan, örtülü operasyonların önemli bir faaliyet alanı hâline gelmiştir. Bu çerçevede bilgi savaşı, bir aktörün rakibinin bilgiye erişimini, bilgiyi işlemesini, karar alma süreçlerini ve kamuoyu üzerindeki etkisini değiştirmek amacıyla yürüttüğü faaliyetleri kapsar. Örtülü operasyonlar bağlamında ise özellikle bilgisayar sistemlerine ve dijital verilere müdahale edilmesi, bilgilerin değiştirilmesi veya silinmesi, kritik sistemlerin çalışmasının engellenmesi ve dijital ortamda gizli etki faaliyetleri yürütülmesi öne çıkar.

Bilgi savaşını geleneksel örtülü operasyonlardan ayıran yön, hedef üzerinde fiziksel olarak bulunmadan da sonuç yaratılabilmesidir. Bir ülkenin enerji, haberleşme, ulaşım, sağlık veya finans sistemlerine yönelik siber müdahaleler yalnızca dijital verileri etkilemekle kalmaz, kamu hizmetlerinin kesintiye uğramasına, ekonomik kayıplara ve kritik altyapıların fiziksel işleyişinin ve toplumsal düzenin bozulmasına da yol açabilir. Böylece bilgi sistemleri üzerinden yürütülen bir operasyon, siyasi ve ekonomik sonuçların yanı sıra doğrudan fiziksel etkiler de yaratabilmektedir. Teknik sistemlere müdahalenin yanı sıra bilgi savaşı, dijital propaganda ve dezenformasyon faaliyetlerini de kapsar. Sosyal medya platformları, sahte hesaplar, otomatik içerik üretimi ve hedefli reklamcılık yöntemleri, belirli toplumsal gruplara kısa sürede ulaşılmasını mümkün kılmıştır. Devlet dışı aktörlerin bu alanda kazandıkları kapasitenin çarpıcı örneklerinden biri Irak Şam İslam Devletidir (IŞİD). Birleşmiş Milletler Güvenlik Konseyinin (2015, ss.7-8) raporuna göre IŞİD, sosyal medya ağlarını propaganda, militan temini, finansman ve faaliyetlerinin duyurulması amacıyla sistematik biçimde kullanmıştır. IŞİD örneği, dijital teknolojilerin devlet dışı aktörlere de ulusal sınırları aşabilen psikolojik etki ve toplumsal yönlendirme kapasitesi kazandırdığını göstermektedir.

Devletler arasında dijital asimetriye ilişkin dikkat çekici örneklerden biri, 2014'te Sony Pictures Entertainment'a yönelik saldırıdır. Kuzey Kore lideri Kim Jong-un'a yönelik kurgusal bir suikastı konu alan "*The Interview*" adlı sinema filminin gösterimi öncesinde Sony'nin sistemlerine sızılmş, ticari belgeler ve kişisel veriler çalınmış, çok sayıda bilgisayar kullanılamaz hâle gelmiş ve şirket faaliyetleri aksatılmıştır. ABD Federal Soruşturma Bürosunun (Federal Bureau of Investigation [FBI], 2014) açıklaması, saldırının sorumluluğunu Kuzey Kore hükümetine atfetmiştir.

Bu açıdan bilgi savaşı, diğer üç alt disiplinin yerini alan bağımsız bir mücadele biçimi olarak görülmemelidir. Aksine dijital ortam, propaganda faaliyetlerinin yayılmasını hızlandırır, siyasi

müdahalelere yeni imkânlar sunar ve ekonomik veya paramiliter operasyonların etkilerini artırabilir. Örneğin kritik bir altyapıya yönelik siber müdahale sonucunda hizmet kesintisi yaşanırken, aynı olay hakkında yürütülen dezenformasyon kampanyası toplumda paniğin artmasına ve kamu kurumlarına duyulan güvenin zayıflamasına yol açabilir. Bu nedenle bilgi savaşı, örtülü operasyonların hem ayrı bir faaliyet alanı hem de geleneksel yöntemleri destekleyen önemli bir unsurudur.

Sonuç olarak propaganda, politik ve paramiliter faaliyetler ile bilgi savaşı, örtülü operasyonların farklı ancak birbirini tamamlayabilen araçlarıdır. Bu araçların birlikte ya da birbirini izleyen aşamalar hâlinde kullanılması, devletlere doğrudan askerî çatışmaya başvurmadan rakiplerinin siyasi, ekonomik ve toplumsal yapıları üzerinde etki oluşturma imkânı sunar. Dijital teknolojiler bu mücadele biçimlerinin temel amaçlarını değiştirmemiş; ancak uygulanma yöntemlerini ve yaratabilecekleri sonuçların ölçeğini genişletmiştir. Dolayısıyla örtülü operasyonların günümüzdeki önemi, yalnızca gizli faaliyet yürütme kapasitesinden değil, geleneksel ve dijital araçların aynı stratejik hedef doğrultusunda kullanılabilmesinden kaynaklanmaktadır.

3. ÖRTÜLÜ OPERASYONLARDA BAŞARI KRİTERLERİ, GİZLİLİĞİN SINIRLARI, İTİBAR RİSKİ VE ASİMETRİK ETKİ

Tüm bunların yanı sıra, örtülü yöntemlerin kullanımı yalnızca devletler arasındaki rekabetle sınırlı değildir. Devletler, sahip oldukları siyasal rejimin niteliğine, hukuki sınırlamalara ve demokratik denetim mekanizmalarının etkinliğine bağlı olarak, istihbarat ve örtülü kapasitelerini farklı ölçülerde iç siyasi rekabeti yönlendirmek, muhalefeti baskılamak veya kamuoyunun siyasi tercihlerini etkilemek amacıyla da kullanabilmektedir.

Öte yandan örtülü operasyonların başarıya ulaşması (Johnson, 2022, ss.252-254) hiçbir zaman garanti edilemez. Planlama hataları, yerel aktörlerin beklenmeyen davranışları, istihbarat yanılgıları veya hedef ülkenin güvenlik birimlerince operasyonun açığa çıkarılması başarısızlığa yol açabilir. Operasyonun ifşa edilmesi özellikle, müdahaleyi gerçekleştiren devletin yalnızca hedef ülkeyle ilişkilerini değil, kendi kamuoyu ve müttefikleri nezdindeki güvenilirliğini de zedeleyebilir. Bu yüzden gizliliğin korunması operasyonun yürütülmesinde önemli olmakla birlikte tek başına başarı ölçütü değildir; daha belirleyici olan, elde edilen sonucun devletin uzun vadeli siyasi hedeflerine katkı sağlayıp sağlamadığıdır.

Örneğin CIA Eski Baş Tarihçisi David Robarge (2018, 23:52-25:43), kamuya açıklanmış yaklaşık 50 CIA örtülü operasyonunun yarısından fazlasının başarısız olduğunu ifade etmektedir. Robarge'a göre silahlı müdahalelerin sonuçları ve kullanılan araçlar, faaliyetin arkasındaki devletin belirlenmesini kolaylaştırabildiğinden paramiliter faaliyetlerde başarısızlık oranı daha yüksektir. Sorumluluğun gizlenmesinin görece daha kolay olduğu propaganda ve siyasi etki faaliyetlerinde ise başarı daha yüksek olabilmektedir.

Robarge (2018, 26:01-28:43) ayrıca örtülü operasyonların başarısını değerlendirirken yalnızca kısa vadede hedeflenen siyasi sonuca ulaşılıp ulaşılmadığına bakmanın yeterli olmadığını, kazanımların uzun vadede korunmasının da önem taşıdığını belirtmektedir. Nitekim Robarge, 1953'te İran Başbakanı Muhammed Musaddık'ın devrilmesini ve Şah'ın yeniden iktidara dönmesini kısa vadeli bir başarı saymakla birlikte, 1979 İran Devriminin bu başarının uzun vadeli sonuçlarını tartışmalı hâle getirdiğini vurgulamaktadır.

Gizlilik, örtülü bir operasyonun sonsuza dek bilinmeyeceği anlamına gelmez. Sorumluluk operasyonun ilk aşamasında gizlenebilse bile arşiv belgelerinin açılması, soruşturmalar, tanıklıklar, itiraflar, teknik izler veya siyasi açıklamalar gerçeği yıllar sonra ortaya çıkarabilir.

Musaddık, Lumumba ve Castro vakaları, geçmiş müdahalelerin yeni kuşaklar bakımından da devletlerin meşruiyetinin, uluslararası itibarının ve yönetimlerin rejim güvenliği algısının sorgulanmasına neden olabildiğini göstermektedir. Gizliliğin ortadan kalkması yalnızca eylemi gerçekleştiren devletin diplomatik ilişkilerini değil, kendi kamuoyunda hesap verebilirliğini ve yönetimin ahlaki sınırlarını da gündeme taşır. Dolayısıyla bir operasyonun kısa vadeli başarısı, ileride doğurabileceği etik, hukuki ve siyasi maliyetlerden bağımsız değerlendirilemez.

Örtülü bir müdahalenin hedefi olunduğunu açıklamak da özellikle küresel güçler açısından kolay değildir. Dışarıdan etkilenmeye açık olunduğunun kabulü, devletin caydırıcılığına, kurumsal yeterliliğine ve güvenlik kurumlarına duyulan toplumsal güvene ilişkin tartışmalar doğurabilir. Bu nedenle hedef devlet, bazı olaylarda ihtiyatlı bir açıklama dili seçebilir.

Soğuk Savaş döneminde geniş ölçekli örtülü operasyonlar büyük ölçüde ABD ve Sovyetler Birliği gibi süper güçlerin istihbarat, finansman ve küresel erişim kapasiteleriyle özdeşleşmiştir. İletişim altyapısına, yazılım araçlarına, veri kaynaklarına ve küresel ağlara erişim günümüzde kolaylaştıkça ve teknoloji demokratikleştikçe, devletler, devlet destekli gruplar, suç örgütleri ve diğer devlet dışı aktörler farklı ölçeklerde etki yaratabilecek araçlara ulaşabilmektedir. Aktör ve yöntem yelpazesini genişleten bu dönüşüm, faillerin belirlenmesini, niyetin anlaşılmasını ve etkinin ölçülmesini güçleştirmektedir.

Bu tablo, modern devletlerin teknolojiyle ilişkisinde önemli bir paradoksa işaret eder. Dijital teknolojilerin demokratikleşmesi, ekonomik ve idari kapasiteyi güçlendirirken bu teknolojilere duyulan bağımlılık yeni saldırı yüzeyleri ve zincirleme kesinti riskleri üretmektedir. Ayrıca saldırının maliyeti ile hedefte ortaya çıkan zarar arasında her zaman doğrusal bir ilişki yoktur. Asimetrik etkinin farklı bir örneğini oluşturan Sony vakasının yanı sıra ABD'de Kasım 2026' da ortaya çıkan teknik kesintiler, aynı kırılganlığın kötü niyetli bir fail bulunmadan da görünür olabileceğini göstermektedir. Bu yüzden asıl ayrım, olayın yarattığı zararın büyüklüğünde değil müdahalenin niteliği, failin kimliği ve kanıtlanabilir siyasi amaçta aranmalıdır.

SONUÇ

Uluslararası rekabet yalnızca doğrudan askerî çatışmalarla değil, siyasi müdahale, propaganda, sabotaj, ekonomik baskı ve siber saldırılar aracılığıyla da kesintisiz biçimde devam etmektedir. Devletler savaşın beraberinde getireceği askerî, ekonomik ve siyasi maliyetlerden kaçınmak ister; ancak rakipleriyle yaşadıkları sorunları her zaman diplomasi yoluyla çözemezler. Yine de doğrudan savaşa başvurmadan hasım devlete maliyet yüklemek, onun hareket serbestisini sınırlamak ve siyasi tercihlerini etkilemek isterler. İşte bu noktada örtülü operasyonlar, diplomasi ile açık askerî güç kullanımı arasında bir üçüncü seçenek olarak önem kazanmaktadır.

Örtülü operasyonlar kendi başlarına hedeflenen siyasi veya stratejik sonuçları üretebildikleri gibi bazı durumlarda nihai sonuca doğrudan ulaşmaktan ziyade daha sonraki siyasi veya askerî girişimler için harekât ortamını şekillendirmeyi de amaçlayabilmektedir. Hedef ülkenin ekonomik kapasitesinin zayıflatılması, toplumsal güvenin aşındırılması ve karar alma süreçlerinin baskı altına alınması, böyle bir hazırlık sürecinin unsurları olabilmektedir.

Örtülü operasyonların etkinliği, sahip olunan istihbarat veya operasyonel kapasiteye olduğu kadar bu kapasitenin tutarlı bir ulusal politika çerçevesinde kullanılmasına da bağlıdır. Nitekim Cormac ve Van Puyvelde (2025, s.17), devletlerin örtülü operasyonlara yaklaşımlarının jeopolitik konumları, stratejik kültürleri, iç siyasi dinamikleri ve yönetim biçimleri arasındaki etkileşimle şekillendiğini ileri sürmektedir. Bu çerçevede, gerek örtülü operasyonların yürütülmesi gerekse diğer devletlerin bu tür faaliyetlerine karşı koyulması, farklı araç ve

tedbirlerin ortak siyasi ve stratejik hedefler doğrultusunda koordineli ve gerektiğinde eş zamanlı kullanılmasını gerektirmektedir.

Örtülü operasyonların temel tarihsel hedefleri büyük ölçüde aynı kalmış, buna karşılık modern dijital teknolojiler bu faaliyetlerin etki ölçeğini, hızını ve hedef toplumların gündelik yaşamı üzerindeki sonuçlarını önemli ölçüde artırmıştır. Fransa'da Ekim 2026'da soğutma sistemlerine yönelik gerçekleştirilen sabotaj, kritik altyapılara yönelik siber-fiziksel müdahalelerin geniş çaplı ekonomik ve toplumsal sonuçlar yaratabileceğini göstermiştir. Fransa'nın ilgili kurumlarınca yayımlanan raporda saldırının İran Devrim Muhafızlarıyla bağlantılı siber birimlere atfedilmesi, bu faaliyetlerin devletler arası rekabetle ilişkisini ortaya koyan güncel bir örnektir.

Avrupa ülkelerinin güvenlik ve istihbarat kurumları, karşı karşıya kaldıkları sabotaj, dezenformasyon, siyasi müdahale ve siber saldırıların tekil olaylardan ibaret olmayabileceğinin farkındadır. Avrupa Birliği Konseyi'nin bu faaliyetleri eş güdümlü ve uzun süreli hibrit kampanyaların parçası olarak değerlendirilmesi bu farkındalığa işaret etmektedir. Bununla birlikte Avrupa'nın resmî açıklamalarında çoğunlukla "örtülü operasyon" yerine "hibrit tehdit", "sabotaj" veya "yabancı müdahale" kavramlarının kullanılması da dikkat çekmektedir. Bu tercih, çoğınlukla hedef alınan ülkelerin mağduriyetlerini itirafta zorlanmalarından kaynaklanmaktadır. Ancak kullanılan terminoloji ne olursa olsun, Avrupa ülkelerinin bu faaliyetlerin hem kendi siyasi, ekonomik ve toplumsal kapasitelerini zayıflatabileceğini hem de daha kapsamlı müdahaleler öncesinde harekât ortamını şekillendirmek amacıyla kullanılabileceğini dikkate aldıkları anlaşılmaktadır.

Avrupa'nın hazırlık politikaları da bu tehdit algısından bağımsız değildir. Avrupa ülkeleri, kritik altyapılarındaki kırılganlıkların ve temel hizmetlerde yaşanabilecek kesintilerin yaratacağı sonuçların farkında olarak vatandaşlarını bilinçlendirmeye ve bireysel hazırlık düzeylerini artırmaya çalışmaktadır. Avrupa'nın 72 saatlik ve daha uzun süreli hazırlık önerileri tek bir tehdide yönelik değildir; doğal afet, teknik arıza, salgın, sabotaj ve savaş gibi farklı riskleri kapsayan "tüm tehlikelere karşı" (*all-hazards*) dayanıklılık yaklaşımını yansıtmaktadır. Bu yaklaşım, devletlerin yalnızca saldırıları önlemeye değil, önlenemeyen saldırılar karşısında toplumun günlük yaşamını sürdürebilmesine de önem verdiğini göstermektedir.

Dijital sistemlere yönelik müdahalelerin oluşturduğu risklerin azaltılmasında teknolojik bağımlılığın yönetilmesi, yazılım ve donanım tedarikinde çeşitlilik, sistemlerin yedeklenmesi ve yerli teknik kapasitenin geliştirilmesi önem taşımaktadır. Bununla birlikte toplumsal dayanıklılığın örtülü operasyonlara karşı güçlendirilmesi yalnızca devlet kurumlarının güvenlik kapasitesinin artırılmasına bağlı değildir. Toplumun karşı karşıya bulunduğu tehditler konusunda bilinçlendirilmesi de bu sürecin bir parçasıdır. Devletlerin, örtülü operasyonların siber saldırılar, dezenformasyon, sabotaj, ekonomik müdahaleler ve toplumsal ayrışmaları derinleştirmeye yönelik faaliyetler gibi farklı biçimlerde ortaya çıkabileceği konusunda kamuoyunu bilgilendirmesi önemlidir.

Doğrudan bir askerî çatışmanın yaşanmaması, devletlerin birbirlerine karşı mücadele etmekten vazgeçtikleri anlamına gelmez. Bu nedenle geleceğe yönelik risk değerlendirmeleri yalnızca gerçekleşebilecek saldırılara değil, bu saldırıların ekonomik, siyasi ve toplumsal sonuçlarına ve daha kapsamlı bir müdahalenin hazırlayıcısı olma ihtimaline de odaklanmalıdır. Çalışmanın başında sorulan "Savaşla barış arasında güvenliği nasıl tartışmalıyız?" sorusuna verilecek yanıt, güvenliğin sadece savaşın varlığı ya da yokluğuyla değerlendirilemeyeceğidir. Askerî çatışmaların doğrudan yaşanmadığı dönemlerde bile devletler arasındaki mücadele; örtülü operasyonlar, siyasi müdahaleler, propaganda, ekonomik baskı, sabotaj ve bilgi savaşları üzerinden sürebilir.

Avrupa devletlerinin en az 72 saatlik hazırlık tavsiyeleri, gelişmiş risk değerlendirme kapasitesinin topluma dönük görünür bir sonucudur. Devletler, elektrik, haberleşme, ulaşım, ödeme ve tedarik sistemlerinin birbirine bağımlılığından doğan zayıflıkları, hangi açıkları giderebildiklerini ve hangilerinin tümüyle ortadan kaldırılamayacağını kendi risk analizleri çerçevesinde değerlendirmektedir. Bütün risklerin sıfırlanamayacağı gerçeği, kamu hizmetlerinin kriz anında mutlaka ve kesintisiz işleyeceği varsayımını da sınırlamaktadır. Bu nedenle 72 saat uyarısı, yalnızca bireysel stok tavsiyesi değil, olası hasarın büyüklüğünü azaltmayı amaçlayan toplumsal hazırlık politikasının bir unsurudur.

Bu çağrılar gelecekteki bir saldırının tarihinin önceden bilindiğini değil; hükümetlerin öngördükleri riskleri gizlemek yerine vatandaşlarla paylaşarak “olası sonuçların farkındayız ve hazırlanmanız için sizi önceden bilgilendiriyoruz” mesajı verdiğini göstermektedir. Riskin ne zaman ve hangi biçimde gerçekleşeceği belirsiz olduğu için kamuoyunda bugünden farkındalık oluşturmak, güvenilir bilgi ve erken uyarı mekanizmaları kurmak, temel ihtiyaçlar için sınırlı bir özerklik sağlamak ve kamu kurumlarının müdahale kapasitesini desteklemek önem kazanmaktadır. Sonuç olarak, 72 saat yaklaşımının temel anlamı, bütün açıkları kapatma iddiası değil, kapatılamayan açıkların yol açabileceği toplumsal zararı hazırlıklar sayesinde sınırlama iradesidir.

KAYNAKÇA

Agencja Bezpieczeństwa Wewnętrznego. (2026, 16 Ekim). Podpalenie stacji Starlink. Od ustaleń ABW i Policji do zatrzymań w Niemczech. https://www.abw.gov.pl/pl/aktualnosci/2846,Podpalenie-stacji-Starlink-Od-ustalen-ABW-i-Policji-do-zatrzyman-w-Niemczech.html

Amante, A. (2026, 12 Kasım). Italian schools defy new wave of bomb threats to remain open. Reuters. https://www.reuters.com/world/europe/italys-meloni-seeks-curb-hoax-bomb-evacuations-2026-11-12/

Associated Press. (2026, 16 Kasım). A technical issue at JPMorgan Chase triggers online banking delays for major US banks. https://www.seattlepi.com/business/customers-nation-s-largest-banks-reporting-a22533729

Avrupa Birliği Konseyi. (2026, 16 Mart). Council conclusions on advancing the European Union's capacity to counter hybrid threats (ST 7349/26). https://data.consilium.europa.eu/doc/document/ST-7349-2026-INIT/en/pdf

Avrupa Komisyonu. (2025, 26 Mart). EU Preparedness Union Strategy to prevent and react to emerging threats and crises (IP/25/856). https://ec.europa.eu/commission/presscorner/detail/en/ip_25_856

Belçika Ulusal Kriz Merkezi. (2026, 1 Ekim). Prepared together: National Crisis Center launches practical guide to help people prepare for emergencies. https://crisiscenter.be/en/newsroom/prepared-together-national-crisis-center-launches-practical-guide-help-people-prepare

Broussard, S. M., & Weintraub, E. L. (2021, 4 Kasım). Statement of reasons in the matter of Cambridge Analytica LLC, et al. (MURs 7350, 7351, 7357, and 7382). Federal Election Commission. https://www.fec.gov/files/legal/murs/7350/7350_57.pdf

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (2025). Vorsorgen für Krisen und Katastrophen. https://www.bbk.bund.de/vorsorge

Cabinet Office. (2026, 22 Ekim). Households encouraged to take small, simple steps to stay prepared in an emergency. GOV.UK. https://www.gov.uk/government/news/households-encouraged-to-take-small-simple-steps-to-stay-prepared-in-an-emergency

Centre de coordination des crises cyber. (2026, 9 Kasım). Activités cyber offensives menées par des acteurs iraniens liés au CGRI: Imputation d'attaques à but de sabotage et de déstabilisation ciblant la France (CERTFR-2026-CTI-009). https://cert.cyber.gouv.fr/cti/CERTFR-2026-CTI-009/

Cormac, R., & Van Puyvelde, D. (2025). Introduction: Broadening the study of covert action. In M. Long, R. Cormac, G. Lester, M. Stout, & D. Van Puyvelde (Eds.), Covert action: National approaches to unacknowledged intervention. Georgetown University Press.

Danish Emergency Management Agency. (2024). Prepared for crises: Checklist. https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisekommunikation/2024/-prepared_for_crises_checklist-.pdf

Deutsche Welle. (2026, 3 Kasım). Polonya'da Starlink saldırısı: Türk şüpheli Almanya'da tutuklandı. https://amp.dw.com/tr/almanyada-bir-t%C3%BCrk-tutukland%C4%B1-starlink-sald%C4%B1r%C4%B1s%C4%B1n%C4%B1n-azmettiricisi-oldu%C4%9Fu-ileri-s%C3%BCr%C3%BCl%C3%BCyor/a-79846848

DSB (Direktoratet for Samfunnssikkerhet og Beredskap). (t.y.). Self-preparedness. https://www.dsb.no/en/egenberedskapsuka/Self-preparedness/

Federal Bureau of Investigation. (2014, 19 Aralık). Update on Sony investigation. https://www.fbi.gov/news/press-releases/update-on-sony-investigation

Federal Communications Commission. (2026, 16 Eylül). Public Safety and Homeland Security Bureau announces nationwide test of the Emergency Alert System (EAS) on November 17, 2026 (DA 26-989). https://docs.fcc.gov/public/attachments/DA-26-989A1.pdf

Federal Trade Commission. (2019, Aralık). Commission issues opinion in Cambridge Analytica case. https://www.ftc.gov/business-guidance/blog/2019/12/commission-issues-opinion-cambridge-analytica-case

Fransa İçişleri Bakanlığı. (2026, 6 Kasım). Bilan de la mobilisation lycéenne et de la journée nationale d'action du 5 novembre 2026. https://www.interieur.gouv.fr/actualites/communiques-de-presse/bilan-de-mobilisation-lyceenne-et-de-journee-nationale-daction-du-5-novembre-2026

Galtung, J. (1969). Violence, peace, and peace research. Journal of Peace Research, 6(3), 167–191. https://doi.org/10.1177/002234336900600301

House of Commons Defence Committee. (2009). Russia: A new confrontation? (Tenth Report of Session 2008–09, HC 276). https://publications.parliament.uk/pa/cm200809/cmselect/cmdfence/276/276.pdf

Johnson, L. K. (1989). America's secret power: The CIA in a democratic society. Oxford University Press.

Johnson, L. K. (2022). The third option: Covert action and American foreign policy. Oxford University Press. https://doi.org/10.1093/oso/9780197604410.001.0001

Jowett, G. S., & O'Donnell, V. (2019). Propaganda & persuasion (7. basım). SAGE Publications.

Kennan, G. F. (1948, 4 Mayıs). The inauguration of organized political warfare [Policy Planning Staff memorandum]. İçinde Foreign Relations of the United States, 1945–1950: Emergence of the Intelligence Establishment (Belge 269, ss. 668–670). U.S. Department of State. https://history.state.gov/historicaldocuments/frus1945-50Intel/d269

Miller, C. (2026, 10 Kasım). Apple confirms ongoing outage affecting iCloud and more. 9to5Mac. https://9to5mac.com/2026/11/10/apple-confirms-ongoing-outage-affecting-icloud-and-more/

Murray, I., & Deliso, M. (2026, 17 Kasım). National intelligence director says no signs of cyberattack amid tech outage concerns. ABC News. https://abcnews.com/US/national-intelligence-director-signs-cyberattack-amid-tech-outage/story?id=138229967

Myndigheten för samhällsskydd och beredskap. (2024). In case of crisis or war (MSB2400). https://rib.msb.se/filer/pdf/30874.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2025). Prepare for an emergency situation. https://english.denkvooruit.nl/documents/2025/11/25/information-booklet-prepare-for-an-emergency-situation

National Security Archive. (2013, 19 Ağustos). CIA confirms role in 1953 Iran coup. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB435/

National Security Council. (1948, 18 Haziran). National Security Council directive on Office of Special Projects (NSC 10/2). İçinde Foreign Relations of the United States, 1945–1950: Emergence of the Intelligence Establishment (Belge 292, ss. 713–715). U.S. Department of State. https://history.state.gov/historicaldocuments/frus1945-50Intel/d292

Obama, B. (2009, 4 Haziran). President Obama's speech in Cairo: A new beginning [Konuşma metni]. U.S. Department of State. https://2009-2017.state.gov/p/nea/rls/rm/2009/124342.htm

Özcan, Nihat Ali. "Energy Security and the PKK Threat to the Baku-Tbilisi-Ceyhan Pipeline," last modified September 22, 2008, https://jamestown.org/energy-security-and-the-pkk-threat-to-the-baku-tbilisi-ceyhan-pipeline/, (accessed February 08, 2026).

Polonya İçişleri ve İdare Bakanlığı. (2025). Safety handbook. https://www.gov.pl/attachment/f9e92e15-5ef7-4d2a-82b6-4a5acbee776e

Reuters. (2026a, 17 Kasım). Apple works to restore services after outage caused by internal update. https://www.reuters.com/business/retail-consumer/apple-works-restore-services-after-outage-caused-by-internal-update-2026-11-17/

Reuters. (2026b, 17 Kasım). Norway's Equinor detects ongoing cyberattack, oil and gas output unaffected. https://www.reuters.com/technology/equinor-detects-ongoing-cyberattack-output-unaffected-2026-11-17/

Reuters. (2026c, 17 Kasım). Tech outage wave reaches US government; Trump says all is "fine". https://www.reuters.com/business/aerospace-defense/trump-shrugs-off-spate-us-outages-says-things-like-that-happen-2026-11-17/

Reuters. (2026d, 17 Kasım). US official says recent tech woes not tied to cyberattacks. https://www.reuters.com/world/us-official-says-recent-tech-woes-not-tied-cyberattacks-2026-11-17/

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Robarge, D. (2018, 10 Nisan). The CIA and the covert Cold War [Konferans konuşması, video kaydı]. Columbia University, European Institute. YouTube. https://www.youtube.com/watch?v=OLc0e8lq3eQ

Secrétariat général de la défense et de la sécurité nationale. (2025). Tous responsables: Face aux risques, agissons. https://www.sgdsn.gouv.fr/publications/guide-tous-responsables

Sky News. (2026, 11 Kasım). Threatening emails sent to thousands of schools across UK, Ireland and Italy treated as hoaxes. https://news.sky.com/story/threatening-emails-sent-to-hundreds-of-schools-in-northern-ireland-scotland-and-italy-treated-as-hoaxes-13610920

Sözcü. (2026, 12 Kasım). Avrupa ülkeleri alarma geçti: Okullar bir bir tahliye edildi. https://www.sozcu.com.tr/avrupa-ulkeleri-alarma-gecti-okullar-bir-bir-tahliye-edildi-p380774

Suomi. (2026, 29 Haziran). Guidance on preparedness, home emergency supplies and acting in crises. https://www.suomi.fi/guides/preparedness/how-to-prepare-for-incidents-and-crises/general-instructions-on-preparedness-home-emergency-supplies-and-on-what-to-do-in-different-situations

Toropin, K., & Tucker, E. (2026, 17 Kasım). Classified communications network at the National Security Agency goes down, defense official says. Associated Press. https://apnews.com/article/22dc6be1bf1d1f5f86a7167f016e9526

U.S. Department of State. (1981). Soviet “active measures”: Forgery, disinformation, political operations (Special Report No. 88). Bureau of Public Affairs. https://www.govinfo.gov/content/pkg/GOVPUB-S-PURL-gpo90452/pdf/GOVPUB-S-PURL-gpo90452.pdf

U.S. Department of State, Office of the Historian. (t.y.-a). The Bay of Pigs invasion and its aftermath, April 1961–October 1962. https://history.state.gov/milestones/1961-1968/bay-of-pigs

U.S. Department of State, Office of the Historian. (t.y.-b). Congo, 1960–1968 [Editör notu]. Foreign Relations of the United States, 1964–1968, Volume XXIII. https://history.state.gov/historicaldocuments/frus1964-68v23/d1

U.S. Senate Select Committee on Intelligence. (2019). Report on Russian active measures campaigns and interference in the 2016 U.S. election: Volume II, Russia’s use of social media. https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf

U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. (1975, 20 Kasım). Alleged assassination plots involving foreign leaders (S. Rep. No. 94-465). https://www.intelligence.senate.gov/sites/default/files/94465.pdf

United Nations Security Council. (2015, 2 Eylül). Implementation of Security Council resolution 2178 (2014) by States affected by foreign terrorist fighters: Second report (S/2015/683). https://digitallibrary.un.org/record/803417/files/S_2015_683-EN.pdf