Global Academy

No. 8
NİSAN 2026

KÜRESEL STRATEJİK ÖNGÖRÜ

Yıkıcı Teknolojiler Çağında Türkiye'nin Değişen Güvenlik Gündemi ve Algıları

Tolga Ökten

Global Academy

Küresel Stratejik Öngörü
No. 8, Nisan 2026

Yıkıcı Teknolojiler Çağında Türkiye'nin Değişen Güvenlik Gündemi ve Algıları

Tolga Ökten, Milli Savunma Üniversitesi

Özet

Ülkelerin sahip olduğu güç unsurlarını paralize ederek mevcut güç ilişkisini derinden etkileme potansiyeline sahip olan yıkıcı teknolojiler, 21. yüzyılın ikinci çeyreğine girdiğimiz bu dönemde en önemli gündem maddelerinden bir tanesi olarak öne çıkmaktadır. Özellikle Rusya – Ukrayna ve ABD/ İsrail – İran arasında gerçekleşen silahlı çatışmalar, yıkıcı teknolojilerin kullanımı hakkında önemli dersler ortaya çıkarmıştır. Bu çatışmalar, yıkıcı teknolojilerin öngörülemezliği, asimetrik ve dinamik yapısı ile çatışmanın seyrini ani etkileme kapasitesi üzerinden okunabilecektir.

Konvansiyonel ve konvansiyonel olmayan tarzdaki tehdit skalasında hibrit bir konumda yer alan bu teknolojiler, hava savunma harbinden istihbarat operasyonlarına kadar farklı seviyelerde kullanılmıştır. Bu teknolojilerin çatışma bölgelerinin ötesinde de etkili olduğu, özellikle sosyal medya etkileşiminin ve çift kullanımlı materyallerin yayılmasının Batılı ülkeler açısından da önemli bir terör tehdidi haline geldiği de görülmektedir. Hibrit karakterdeki bu tehditler askeri, ekonomik, sosyal vb. alanlarda yıkıcı etkiye sahiptir.

Hibrit alanda ilerleyen bu teknolojiler, Türkiye açısından da önemli bir tehdit unsuru olarak görülmelidir. Bu durum, Türkiye'nin gerek bölgesel rakipleri ile gerekse daha düşük kapasiteye sahip devlet dışı aktörlere yönelik yürüttüğü strateji çerçevesinde incelenmelidir. Bu noktada, Türkiye'nin caydırıcı ve zorlayıcı kapasitesinin devam etmesi açısından yıkıcı teknolojilerin yarattığı asimetri dengelenmelidir. Bu çalışmanın hedefi de Türkiye'nin önümüzdeki dönemde karşılaşabileceği hibrit düzlemde ortaya çıkabilecek faklı karakterlerdeki tehditlerin geniş bir çerçevede farklı senaryolar üzerinden tartışılması ve konu hakkında farkındalık yaratılmasıdır.

Giriş

Rusya'nın Ukrayna'ya yönelik olarak Şubat 2022'de başlattığı işgal her yönüyle geleneksel bir savaş şeklinde başlamıştır. Stratejik noktaların ele geçirilmesi hedefli hava saldırısı ve hava indirme harekâtı ile başlayan savaş, başkent Kiev'in ele geçirilmesi amacıyla yürütülen zırhlı birlik manevrası ile devam etmiştir. Diğer tarafta Rusya'nın manevra stratejisine dayalı konvansiyonel harekâtı kısa sürede başarısız olmuş ve savaş hızla yıpratma savaşına evrilmiştir. Bu süreçte geleneksel araçların kullanımının azaldığı ve daha önce kullanılmayan farklı teknolojilerin de devreye girdiği görülmüştür. Bu yeni araçlar sadece cephe hattında değil cephe gerisinde de hızla yayılmış ve sadece Ukrayna değil Rusya toprakları da bir savaş alanı haline gelmiştir. Benzer bir durum ABD/İsrail – İran çatışmasında da gözlemlenmiştir. İki ülke arasındaki silahlı çatışma sadece karşılıklı hava saldırıları şeklinde yürümemiş, İsrail istihbarat teşkilatlarının gerek İran'ın gerekse bölgesel müttefiki Hizbullah'a karşı operasyonlarına da şahit olunmuştur. Bu kapsamda, Hizbullah kadrolarına yönelik olarak gerçekleştirilen çağrı cihazı saldırıları dikkat çekici görülmektedir.

Geçen dört senelik sürece bakıldığında Rusya - Ukrayna ve ABD/ İsrail – İran çatışmalarının yıkıcı teknolojilerin çatışma bölgelerindeki kullanımına dair önemli sonuçlar ortaya çıkardığı söylenebilecektir. Bu yıkıcı teknolojilerin gerek cephe hattında gerekse cephe gerisinde yoğun olarak kullanıldığı ve sadece fiziki değil psikolojik açıdan da çatışmanın tarafları üzerinde etkili oldukları görülmüştür. Bu çalışmada da küresel çapta yaşanan çatışmalarda ön plana çıkan yıkıcı özellikteki teknolojilerin ve taktiklerin Türkiye'ye yönelik etkilerinin tartışılması hedeflenmiştir. Bu kapsamda öncelikle yıkıcı teknoloji teriminin nasıl tanımlanması gerektiği incelenmiştir. Sonrasında Türkiye'nin güvenlik gündemi çerçevesinde hangi tehdit senaryolarının ortaya çıkabileceği tartışılmıştır.

Yıkıcı Teknolojilerin Tanımlanması

Yıkıcı teknoloji terimiyle, ülkelerin sahip olduğu güç unsurlarını kullanılamaz hale getirerek mevcut güç ilişkisini derinden etkileme potansiyeline sahip değişkenler kastedilmektedir. Yıkıcı teknolojilerin en önemli özelliği asimetri yaratma kabiliyetleri ile mevcut güvenlik doktrinlerini ve uygulamalarını boşa çıkarma kapasiteleridir. Bu tehditler ile başa çıkabilmek için asimetrinin dengelenmesi ve mümkünse karşı asimetri yaratılması gereklidir.

NATO doktrininde yıkıcı teknolojilerin büyük güç mücadelesi kapsamında değerlendirildiği ve yüksek teknoloji gerektiren araçlar üzerinden yorumlandığı görülmektedir. Bu teknolojiler; otonom sistemler, kuantum teknolojileri, biyoteknoloji, uzay sistemleri, hipersonik füzeler, yeni jenerasyon iletişim ağları, yarı iletken materyal üretimi vb. şeklinde sayılmaktadır (NATO, 2025). Diğer taraftan yıkıcı teknoloji terimini sadece ileri teknoloji üzerinden tanımlamanın doğru olmadığı değerlendirilmektedir. Bu araçlar yeni bir teknoloji üzerinden ortaya çıkabileceği gibi, mevcut bir teknolojinin farklı kullanım alanlarının oluşması üzerinden de ortaya çıkabilir. Bu farklı süreçlerin

ilkine örnek olarak yeni bir silah olan atom bombası, ikincisine örnek olarak 2. Dünya Savaşı'nda tankların farklı bir strateji ve taktik çerçevesinde kullanımı verilebilir. Atom bombası o güne kadar kullanılmamış asimetrik bir teknoloji sağlayarak önce Pasifik Cephesi'ndeki çatışmaya son vermiş sonrasında da günümüze kadar gelen dehşet dengesini sağlamıştır. Tanklar ise yeni bir teknoloji olmamakla birlikte 2. Dünya Savaşı'nın başlarında Yıldırım Savaşı adı verilen müşterek harekatlarda farklı strateji, örgütlenme modeli ve taktikler çerçevesinde o zamana kadar denenmemiş bir şekilde kullanılarak stratejik asimetri yaratmıştır.

Bu durum sadece konvansiyonel bir savaş seviyesinde tartışılmamalıdır. Günümüzdeki tehdit değerlendirmelerinin de yeni bir teknolojiden ziyade mevcut araçların farklı şekillerde kullanılması üzerinden okunabileceği değerlendirilmektedir. Bu duruma verilebilecek en dramatik örnek 11 Eylül saldırılarıdır. 1970'lerden itibaren kitlesel terörizm senaryosu, nükleer tehditler üzerinden kurgulanmıştır. Diğer taraftan beklenen kitlesel terör ticari uçakları akıllı bomba olarak kullanmaya dayalı korkunç ancak yaratıcı bir fikir üzerinden gelişmiştir. Bu eylem sadece insan hayatına değil havacılıktan sigortacılığa kadar çok sayıda kritik sektörde yıkıcı bir etkiye neden olmuş ve havacılık kurallarını temelden etkilemiştir.

Günümüzde de yıkıcı teknolojiler çok yönlü ve dinamik bir karakterdedir. Bu teknolojiler, hipersonik füzelerden ticari mikro İnsansız Hava Araçları'na (İHA), sosyal medyadan mutfak malzemelerine kadar geniş bir yelpazede yer almakla birlikte, ortak noktaları asimetri yaratma ve devletlerin sahip oldukları mevcut güç unsurlarını paralize etme potansiyelleridir.

Tehdit Değerlendirmesi

Bu çalışmada, yıkıcı teknolojiler Türkiye'nin ulusal güvenliğinin sağlanması açısından sahip olduğu güç unsurlarına yönelik olarak ortaya çıkabilecek tehditler üzerinden tartışılmıştır. Bu tehditler, Türkiye'nin sahip olduğu mevcut güç unsurları göz önünde bulundurularak üç senaryo etrafında şekillendirilmiştir (Tablo-1).

Tablo-1: Yıkıcı Teknolojilerin Yarattığı Güvenlik Sorunları

Hava Üstünlüğü	Hibrit Teknoloji	Siber Alan Hakimiyeti
Muharip Filoların Kapasite Asimetri Yaşaması	Çift Kullanımlı Teknolojinin Yayılması	Propaganda ve Eleman Temin Kanalı Olarak Kullanılması
Çok Katmanlı Hava Savunma Sistemi İhtiyacı	FPV Dronların Cephe Hattı ve Gerisinde Etkili Olarak Kullanılması	Veri Güvenliğinin Korunması
Anti SİHA Teknolojilerinin Yayılması	Dinamik ve Yaratıcılığa Açık Bir Tehdit Olması	Kamu – Özel Sektör İşbirliğine Olan İhtiyaç

Türkiye'nin Hava Üstünlüğüne Dayalı Stratejik Avantajının Engellenmesi

Türkiye'nin gerek bölgesel güç rekabetinde gerekse terörle mücadele harekâtlarında sahip olduğu belki de en önemli caydırıcı ve operasyonel güç hava üstünlüğüdür. Türkiye hem yurt içinde hem de Irak, Suriye, Libya ve Somali'de yürüttüğü harekatlarda hava üstünlüğünü ağırlık merkezi olarak kullanmıştır. Hava üstünlüğünün coğrafi, meteorolojik ya da hava savunma unsurlarının varlığı gibi engelleyici etkenler nedeniyle kısıtlandığı senaryolarda kara harekatının temposu düşmüş ve kayıplar yaşanmıştır. Bu durum gerek geleneksel muharip jet uçakları gerekse Silahlı İnsansız Hava Araçları (SİHA) için geçerlidir.

Türkiye'nin hava üstünlüğüne darbe vuracak en önemli tehdit, Türkiye'nin bölgesel rakiplerinin hayalet *(stealth)* teknolojisine sahip F-35 uçaklarını envanterlerine katmalarıdır. Türkiye'nin en azından beklenen süre zarfında bu teknolojiye sahip olamaması, hava üstünlüğü açısından önemli bir asimetri yaratmıştır. Bu noktada, Rusya-Ukrayna ve ABD/İsrail-İran çatışmalarında öne çıkan önemli gelişmelerden bir tanesi de radar izi yüksek eski nesil uçakların kullanımının kısıtlılığıdır. Özellikle ABD/İsrail-İran çatışmasında gerçekleştirilen hava harekatlarında hayalet teknolojisine sahip hava platformlarının yoğun bir şekilde kullanıldıkları görülmektedir.

Bu senaryoda, özellikle Doğu Akdeniz ve Ege'deki hava üstünlüğünün kaybedilmesi Türkiye'nin caydırıcılığına zarar verecektir. Suriye'nin Türkiye ile İsrail arasında tampon bir bölge olmaktan çıkması ve İsrail'in bölgedeki harekatlarında Suriye hava sahasını kullandığı göz önünde bulundurulduğunda süreçte Türkiye'nin hava üstünlüğüne dayalı caydırıcılığını koruması elzemdir. Benzer şekilde bu teknolojinin Yunanistan ve Suudi Arabistan gibi bölge ülkelerinde de yayılması Türkiye açısından daha da olumsuz bir senaryo oluşturacaktır.

Bu noktada ABD/İsrail-İran çatışmasında ortaya çıkan bir diğer tehdit unsuru da balistik füzelerdir. Özellikle Rusya ve İran'ın kullandığı hipersonik özellikteki füzelerin, kamikaze İHA'larla eş güdüm halinde kullanıldığında, mevcut hava savunma sistemlerini aşabildiği görülmüştür. Türkiye'nin bu tehdide karşı çok katmanlı hava savunma sistemlerinin, erken ihbar / ikaz sağlayacak hava platformlarının ve radar / elektronik harp araçlarının bütünleşmiş olarak çalıştığı bir sistemi inşa etmesi gereklidir.

Hava üstünlüğü sadece konvansiyonel aktörler arasındaki güç rekabeti için değil Türkiye'nin daha düşük kapasiteye sahip devlet dışı aktörlere yönelik yürüttüğü SİHA merkezli harekatlar açısından da çok önemli bir unsurdur. Türkiye 2015 sonrasında özellikle yurt içerisinde elektronik bir alan hakimiyeti sağlayarak PKK/KCK kırsal kadrolarının faaliyetlerini 7/24 kontrol altında tutmayı başarmıştır. SİHA'lar istihbarat ve operasyon faaliyetini tek bir platformda birleştirerek imha zincirini hızlandırmış, sürpriz etkisini PKK/KCK'nın elinden alarak özellikle yurt içindeki örgüt kadrolarını tükenme sürecine sokmuştur. Diğer taraftan açık kaynaklarda, özellikle 2024-2025

döneminde kamikaze olarak da adlandırılan tek yönlü SİHA'ların Türkiye'nin kullandığı MALE sınıfı daha büyük platformlara yönelik olarak etkili şekilde kullanılmaya başlandığı yönünde bilgi bulunmaktadır. Bu tarz bir gelişme Türkiye'nin örgütle mücadele sürecinde sahip olduğu çok önemli bir aracın işlevsiz hale gelmesi anlamına gelecektir. Bu örnekten de görüleceği üzere, hava üstünlüğüne yönelik tehditler sadece ileri teknolojiye sahip yeni araçlardan değil daha basit bir teknolojinin uyarlanması ile de oluşabilmektedir. Bu durum sadece hava değil deniz ortamı için de geçerlidir. Basit bir teknolojiye sahip Silahlı İnsansız Deniz Araçları (SİDA) da Ukrayna tarafından Rusya'nın konvansiyonel deniz platformlarına yönelik olarak sıklıkla kullanılmaktadır. Bu platformların özellikle devlet dışı aktörlerin eline geçmesi, Türkiye'nin deniz platformları açısından önemli bir asimetrik risk unsurudur.

Çift Kullanımlı – Hibrit Ticari Teknolojinin Yayılması

İlk senaryo belli ölçülerde yüksek teknoloji içeren bir özellikte olmakla birlikte, diğer senaryolar daha basit kullanımlı ticari teknolojilerin yıkıcı amaçlarla kullanılmasına odaklanmaktadır. Bu kapsamda özellikle Rusya-Ukrayna savaşı sürecinde bu tarz teknolojilerin sıklıkla kullanıldığı görülmektedir. Sivil amaçlarla üretilen ancak kolaylıkla askeri amaçlı olarak da kullanılabilen araçlar, şiddeti "demokratikleştirerek" ve tehdidi dinamik hale getirerek, takibini zorlaştırmaktadır. Bu araçlar özellikle yalnız aktör eylemlerinde kullanılan ev araç gereçlerinden, ticari olarak satılan mikro İHA'lar ve 3D yazıcılara kadar geniş bir skalada yer almaktadır.

Bu noktada özellikle ticari İHA olan FPV (*First Person View* – Görüntü Aktarımlı Dron) dronların Rusya-Ukrayna savaşında cephe hattında yoğun olarak kullanıldığı bilinmektedir. Hatta FPV'lerin Rusya-Ukrayna savaşında asker kayıplarının %80'ine yakınından sorumlu olduğu da iddia edilmektedir. Bu sayı günlük yaklaşık 1000 kayıp anlamına gelmektedir (Thomas, 2025). FPV dronlar sadece cephe hattında değil, istihbarat ve özel kuvvet unsurlarınca cephe gerisinde sabotaj ve suikast tarzı eylemler için de kullanılmaktadır. Bu araç özellikle Ukrayna tarafından Rusya'nın cephe gerisindeki stratejik askeri üslerine, kritik alt yapı tesislerine ve fabrikalara yönelik olarak etkili bir şekilde kullanılmış ve büyük zararlar vermiştir. İsrail de benzer bir faaliyeti 12 Gün Savaşı'nın başlarında İran hava savunma birliklerine ve komuta kademesine yönelik olarak yürütmüştür.

Devletlerin FPV'lerin kullanımını Arap Baharı sürecinde DEAŞ ve diğer örgütlerden öğrendiklerini söylemek de çok yanlış olmayacaktır. Kronolojik olarak önce FPV'lere havan ya da el bombası düzeneği eklenmiş sonrasında ise yöntem geliştirilerek FPV'ler doğrudan hedefe çarpan silahlar haline getirilmiştir. Bu süreç tıpkı bomba yüklü araç saldırıları gibi doğaçlamaya dayanmaktadır. Devlet dışı aktörlerin FPV'leri kullanmaya artarak devam ettiği de görülmektedir. Bağımsız bir çatışma takibi ve analizi merkezi olan ACLED tarafından 2025 yılında hazırlanan bir rapora göre devlet dışı aktörler bu tarz İHA'ları aralarında Meksika, Kolombiya ve Suriye gibi ülkelerin bulunduğu 17 ülkede aktif olarak kullanmıştır. 2020 yılında sadece 10 devlet dışı aktör

İHA saldırısı düzenleme kapasitesine sahipken 2025 yılında bu sayı 469 olarak belirtilmiştir (Carboni ve Murilla, 2025). Bu tarz çatışma bölgelerinde kullanılmak üzere her gün kontrolsüz bir şekilde binlerce FPV üretilmektedir. Çatışma bölgelerinin fazlalığı örgütlerin öğrenme süreçlerini hızlandırarak bu tarz basit yıkıcı teknolojilere daha hızlı bir şekilde uyum sağlamasına neden olmuştur. Tanksavarların Arap Baharı sonrasında kontrolsüzce dağılarak ülke ordularına yönelik büyük bir tehdit oluşturması gibi FPV'ler de giderek daha fazla kullanılmaktadır.

Bu çerçevede FPV'lerin PKK/KCK tarafından Irak'ta konuşlu Türk Silahlı Kuvvetleri birliklerine yönelik olarak bir dönem yoğun şekilde kullanıldığı bilinmektedir. Bu teknolojinin örgüt tarafından basit ve etkili bir araç olarak görüldüğü söylenebilecektir. Bu aracın ayrıca, örgütler ve yabancı istihbarat teşkilatlarınca yurt içerisinde stratejik tesislere ve sivil alanlara yönelik olarak sürü şeklinde kullanılma tehdidi de her zaman mevcuttur. Bu kapsamda FPV'ler; havalimanları, boğaz trafiği, savunma sanayi tesisleri, tedarik zincirleri, boru hatları, enerji nakil hatları vb. kritik altyapının yanı sıra insanların toplandıkları alanlara yönelik olarak sürü halinde kullanılması basit ama önemli bir tehdit senaryosu olarak görülmelidir.

Bu noktada tek hibrit teknolojik tehdit FPV'ler değildir. Türk Silahlı Kuvvetlerinin 2016 sonrasında gerçekleştirdiği sınır hattı ve ötesindeki askeri harekatlar nedeniyle Türkiye'ye kadro ve malzeme aktarımında sorun yaşayan PKK/KCK'nın, sınır hattını geçmek amacıyla paramotorları kullandığı görülmüştür. Bir diğer örnekte de İsrail, istihbarat teşkilatı üzerinden yürüttüğü operasyonda çağrı cihazlarını kullanmış ve Hizbullah'ın güvenli haberleşme amacıyla satın aldığı cihazları birer bombaya dönüştürerek Hizbullah kadrolarına büyük bir zarar vermiştir. İsrail'in bölgesel rakiplerine karşı yürüttüğü istihbarat faaliyetlerinin geleneksel anlamda espiyonaja dayalı siyasi askeri casusluk sınırını aştığı ve suikast - sabotaj gibi özel faaliyetlerde yararlanmak üzere tedarik zincirlerine ve lojistik kanallarına sızmaya çalıştığı görülmektedir. Burada dikkat çekici nokta çift kullanımlı basit teknolojiyi silah olarak kullanmada yaratıcılığın bir sınırının olmamasıdır. Diğer bir deyişle henüz fikrimiz olmayan tarzdaki saldırılarla karşı karşıya olduğumuzun bilinmesi gereklidir. Bu noktada önemli olan sürekli olarak alarmda kalabilmek, tehditleri sadece geleneksel yöntemlerden beklememek ve savunma açısından da hayal kurabilmektir.

Bu tarz yaratıcı araçlar, herhangi bir teknik - taktik tecrübesi olmayan ve lojistik açıdan örgütten yardım almayan yalnız aktörler tarafından sıklıkla kullanılmaktadır. Bu nedenle özellikle bıçak, araç ya da marketlerden temin edilen malzemelerden üretilen el yapımı silahlar kullanılarak gerçekleştirilen saldırılar önemli bir tehdit önceliği haline gelmiştir. Bu konuda yayımlanan bir raporda, Batı da son 5 yılda gerçekleştirilen terör eylemlerinin %93'ünün yalnız aktör saldırısı olduğu belirtilmektedir (Institute for Economics and Peace, 2025). Bu saldırganlar basit silahlar kullanan sıradan insanlardır. Bu saldırganların ve kullandıkları araçların yıkıcı etkisinin en önemli nedeni geleneksel istihbarat yöntemlerinin etrafından dolanabilmeleridir. Bu yöntemde, eylem öncesinde somut tehdit emareleri

vermemektedirler. Sahip oldukları kapasitenin sıradan olması ve dikkat çekici bir hazırlık gerektirmemesi istihbarata karşı önemli bir asimetri yaratmaktadır.

Siber Alan Hakimiyetinin Kaybedilmesi ve Şiddetin Tabana Yayılması

Yıkıcı teknolojilerin sadece askeri kapasite üzerinden değil, sosyal yapıyı ve iç güvenliği paralize edecek tehditler üzerinden de okunması gereklidir. 21. yüzyılda hayatımızın çok önemli bir bölümünü kaplamaya başlayan siber alanın da yıkıcı amaçlı olarak kullanıldığı söylenebilecektir. Bu kapsamda; sosyal medya ve yapay zekâ etkileşimlerinin siber alandaki radikalleşme süreçlerini tetiklemesinin ve sosyal hareketleri provoke etmesinin engellenmesi, veri güvenliğinin sağlanması, dezenformasyonun önlenmesi vb. tehdit unsurları ön plana çıkmaktadır. Bu mecralarda yürütülen yıkıcı faaliyetler; devlete olan güvenin yıpratılması, kara paranın aklanması, yasa dışı oluşumların finansmanı, vatandaşların güvenliğinin tehlikeye atılması ve Türkiye'ye yönelik uluslararası kamuoyu nezdindeki algının olumsuz şekilde etkilenmesine neden olma tehdidi taşımaktadır.

Siber alan ayrıca, tehdidin tabana yayılması tehlikesini de bünyesinde barındırmaktadır. Bu mecra yasa dışı örgütlerin gençlere erişimindeki en önemli araçtır. Bu noktada dikkat çeken husus, son dönemde gerçekleştirilen saldırıların ortak özelliğinin, çoğunlukla ani bir şekilde eyleme geçen gençlerden oluşmasıdır. İstihbarat teşkilatlarının yanı sıra terör ve diğer suç örgütlerinin kendini kanıtlama arayışında olan gençleri eyleme yönelttikleri görülmektedir. Özellikle sosyal medyanın bir eleman temin mecrası olarak kullanılarak gençlerin sokak çeteleri üzerinden silahlı eylemlere yönlendirilmesi söz konusudur. Bu kapsamda, gençlerin sosyal medya ve sanal oyun platformları üzerinden şiddete yönlendirildikleri belirtilmektedir. Şiddeti amaçsallaştıran ve nihilist olarak adlandırılan türdeki radikallerin nefret, intikam ve kahramanlık arayışlarının sosyal medya üzerinden uzaktan manipüle edilmesi çok kolay olmaktadır. Sosyal medya, eylem talimatlarının yanı sıra eylem teknik ve taktiklerinin de online dergilerde paylaşılarak geniş bir vasata ulaşmasını sağlayan bir mecra haline gelmiştir. Söz konusu yasadışı yapıların ayrıca sosyal ağ üzerinden kurdukları ulusötesi ağlar sayesinde küresel seviyede esnek bir konsorsiyuma dönüştükleri ve eylem kapasitelerini ulusötesi bir seviyeye taşıdıkları görülmektedir.

Siber alan radikalleşme ve suça yönelme süreçlerini iki kanal üzerinden etkilemektedir. Dikey ve yatay olarak sınıflandırılabilecek olan bu kanallar kişiyi eyleme yönlendirmektedir. Dikey kanalda, örgütlerin potansiyel eylemciyi sosyal medya üzerinden yürüttüğü ideolojik propaganda ile dolaylı olarak etkiledikleri görülmektedir. Aslında siber alan örgütün ideolojisini tabana ulaştırması bakımından en önemli kanal haline gelmiştir. Pasif bir etkileşim sağlayan bu kanallar örgüt propagandası ve talimnamelerini hereksin cebinde taşınmasına imkân sağlamaktadır. Bu noktada bazı durumlarda sanal planlayıcı olarak adlandırılan bir örgüt mensubu ya da istihbarat personeli ile de bağlantıya geçilebildiği görülmektedir. Bu kapsamda, gençlerin Rusya tarafından suikast ve sabotaj gibi faaliyetlerde kullanılmasının

Avrupa'da giderek yaygınlaştığı iddia edilmektedir. Buna göre, Rus istihbarat servislerinin, Ukrayna savaşı başladığından beri hedef aldığı Batı Avrupa ülkelerinde toplam 145 sabotaj ve kundaklama eylemi gerçekleştirdiği belirtilmektedir. Bu eylemleri gerçekleştirenler çoğunlukla sosyal medya üzerinden irtibat kurulan yerel sokak çetesi mensupları olmuştur. (Deutsche Welle, 2025). İkinci kanal ise örgüt merkezli olarak değil, yatay düzlemde sosyal çevre üzerinden ilerlemektedir. Fiziki dünyada irtibat kurması mümkün olmayan benzer dünya görüşlerine sahip gençlerin siber alanda sosyalleştikleri ve birbirlerini tetikledikleri söylenebilecektir. Diğer bir deyişle günümüzde hücre evlerinin yerini internetteki gizli sohbet odaları ve forumlar almaya başlamıştır.

Siber alandaki tehdidi sadece silahlı eylemler üzerinden sınıflandırmak da doğru değildir. *Deepweb* ve *Darkweb*'in finansal suçlar için kullanılması, kişisel verilerin kontrolsüzce yayılarak suç örgütlerinin eline geçmesi, yanlış bilgilerin bilinçli olarak yayılarak dezenformasyon ve manipülasyon faaliyetinde kullanılması, yapay zekâ üzerinden ses klonlama ve şiddet propagandası yapılması gibi çok farklı olasılıklar söz konusudur. Özellikle İsrail'in gerçekleştirdiği saldırılar göz önüne alındığında veri gizliliğinin sağlanamaması önemli bir sorun olarak görülmelidir. İsrail istihbarat servislerinin hedefleme faaliyetinin açık, yarı açık ve kapalı kaynaklardan toplanan büyük verinin yapay zekâ üzerinden analizi üzerinden yürüttüğü göz önünde bulundurulduğunda, kişisel verilerin korunması ve siber altyapının dayanıklılığı da önemli bir unsur olarak ön plana çıkmaktadır. Bu durum devlet dışı aktörlerin faaliyetleri açısından da geçerlidir. Araştırmacı gazetecilik faaliyeti yürüten *Bellingcat* de Rus istihbarat servislerinin faaliyetlerini deşifre ederken, sızdırılan verilerden yoğun olarak yararlanmaktadır.

Bu senaryoda ortaya çıkan en önemli tehdit unsuru siber alan hâkimiyetinin kaybedilmesi ve kontrolsüz bir mecranın ortaya çıkmasıdır. Siber alan devletlerin güç tekelinin bulunmadığı ve devlet dışı aktörlerin hatta tek tek bireylerin devletlere meydan okuyabildiği bir alandır. Bu alanın kontrolü fiziki alandan daha fazla teknolojik uzmanlık gerektirmektedir. Bu nedenle sadece devletlerin değil özel sektörün de önemli katkısı olmaktadır. Dayanıklılığın sağlanması, tehditlerin tespiti ve önlenmesinde erken uyarı mekanizmalarının hızlı bir şekilde işlemesini teminen özel ve kamu güvenlik mimarisi içerisinde iş birliğinin arttırılması hedeflenmelidir. Bu doğrultuda teknoloji şirketleri ile yakın iş birliğinin yaratacağı fırsatların değerlendirilmesi gereklidir.

Sonuç

Rusya-Ukrayna ve ABD/İsrail-İran çatışmaları kapsamında ön plana çıkan teknolojilerin Türkiye'nin gerek konvansiyonel gerekse konvansiyonel olmayan tarzdaki güvenlik gündemi ve algılarını önemli ölçüde etkilediği görülmektedir. Bu tehditler, etkisi öngörülemeyecek ve zararı kısa sürede giderilemeyecek şekilde ortaya çıkabilecektir.

Türkiye'nin önündeki en önemli tehdidin hava üstünlüğünü kaybetmesine neden olabilecek teknolojik gelişmeler olduğu değerlendirilmektedir. Özellikle ABD/İsrail-İran çatışması gibi dolaylı bir strateji kapsamında hızlı tempoda ve güvenlik mimarisini paralize edecek şekilde yürütülen bir çatışmada gerek hava gerek hava savunma gerekse elektronik harp boyutunca üstünlüğün kaybedilmesinin acı sonuçları olduğu görülmüştür. Bu durum Türkiye'nin PKK/KCK gibi terör örgütlerine yönelik yürüttüğü harekatlar için de geçerlidir. Özellikle SİHA'lar üzerinden oluşturulan elektronik alan hakimiyetinin kaybedilmesi terörle mücadele stratejisine zarar verecektir.

Sadece ileri teknoloji değil hibrit olarak da adlandırılabilecek olan çift kullanımlı basit teknolojilerin de giderek daha büyük bir güvenlik sorunu ortaya çıkardığı söylenebilecektir. Evde bulunan malzemelerden FPV'lere kadar geniş bir skalada yer alan bu araçlar küresel çapta önemli bir tehdit olarak görülmektedir. Özellikle ticari olarak satışı bulunan FPV'lerin askeri amaçlı kullanımı, Irak ve Suriye iç savaşlarını takip eden süreçte giderek daha fazla artmış ve gerek cephe hattında gerekse şehirlerde sabotaj amaçlı saldırılarda giderek daha fazla kullanılmaya başlanmıştır. Bu kapsamda mevcut sofistike silahların örgütlerin eline geçmesi kadar basit teknolojilerin örgütler ve istihbarat teşkilatlarınca hızla uyarlanarak etkili bir şekilde kullanılması da önemli bir tehdit önceliğidir.

Son olarak, yıkıcı teknoloji açısından sadece askeri tehditler değil siber alanda ortaya çıkan gelişmeler de önemli görülmelidir. Bu noktada sadece siber sabotaj eylemleri değil; kişisel verilerin temini, gençlerin sosyal medya üzerinden radikalleşmesi ve örgütlerin eleman temini faaliyeti de önemli bir güvenlik sorunu olarak ortaya çıkmıştır. Bu noktada Türkiye'nin siber alan hakimiyetini koruması önem arz etmektedir. Ayrıca, bu tehditlerin önlenmesinde istihbarata karşı koyma ve terörle mücadele faaliyeti yürüten birimler ile özel sektörün iş birliği yapması önemli görülmektedir.

Kaynakça

NATO, *Emerging and Disruptive Technologies*, 25 Haziran 2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies (Erişim Tarihi: 01.01.2026).

Richard Thomas, "Drones Now Account for 80% of Casualties in Ukraine-Russia War," *Army Technology*, 8 Nisan 2025, https://www.army-technology.com/news/drones-now-account-for-80-of-casualties-in-ukraine-russia-war/ (Erişim Tarihi: 03.01.2026).

Andrea Carboni ve Ciro Murilla, What's driving conflict today? A review of global trends, *ACLED Raporu*, Aralık 2025, https://acleddata.com/report/whats-driving-conflict-today-review-global-trends?utm_source=t.co&utm_medium=social&utm_campaign=index_watchlist_2026 (Erişim Tarihi: 27.12.2025).

Institute for Economics and Peace. *Lone Wolf and Youth Terrorism: Evolving Patterns of Terrorism & Radicalisation in Western Democracies*, Sidney, 2025.

Deutsche Welle, 18 Aralık 2025, https://www.dw.com/en/acts-of-sabotage-linked-to-russia-surge-in-europe/video-75217660 (Erişim Tarihi: 28.12.2025).

Global Academy

Tolga ÖKTEN

Dr. Tolga ÖKTEN Milli Savunma Üniversitesi'nde öğretim üyesidir. Lisans eğitimini Başkent Üniversitesi İşletme Bölümü'nde, yüksek lisans eğitimini TOBB ETÜ'de, doktorasını Milli Savunma Üniversitesi'nde Güvenlik Araştırmaları programında tamamlamıştır. Güvenlik, terörizm ve istihbarat konularında çalışmakta olup bu alanlarda yayımlanmış Türkçe ve İngilizce eserleri bulunmaktadır.

Global Academy

Global Akademi, yatay düzlemde ortak çalışmanın hâkim olduğu, kamuya yönelik kâr amacı gütmeyen gönüllü üretim ile proje-bazlı çalışmaların bir arada yürütüldüğü, her tür bilgi, fikir, yorum ve analizin serbestçe ve kapsamlı tartışılması yoluyla mükemmeliyetin hedeflendiği bir araştırma ve öğrenme merkezidir.

Çalışmalarında uluslararası düzeyde mükemmelliği hedefleyen Global Akademi, küresel gelişmeler ile ilgili olarak bağımsız, tarafsız, bilimsel bilgiye dayanan araştırmalar gerçekleştirmek, basit ve anlaşılır veri üretmek, ihtiyaç duyan kişi ve kurumlara danışmanlık ve çözüm ortaklığı sunmak, eğitim, yayın ve yayım faaliyetlerinde bulunmak ve küresel düzeyde insanlığın karşılaştığı sorunları anlama, anlatma ve çözüm bulma çabalarına katkıda bulunmak amacıyla kurulmuştur.

/ TRGlobalAcademy

www.globacademy.org