RAPOR

GÜVENLİK YÖNETİMİNDE ÇAĞDAŞ YAKLAŞIMLAR

POLİS AKADEMİSİ YAYINLARI

GÜVENLİK YÖNETİMİNDE ÇAĞDAŞ YAKLAŞIMLAR

POLİS AKADEMİSİ YAYINLARI

Hazırlayanlar
Doktor Öğretim Üyesi İbrahim İRDEM
Araştırma Görevlisi Özlem ALKAN
Araştırma Görevlisi Kübra Betül Biçen GÖREN
Öğretim Görevlisi Özer ARSLAN

Polis Akademisi Yayınları: 135
Rapor No: 58
ISBN: 978-605-7822-84-0
Aralık 2021, Ankara

Tasarım: Nurbanu ARSLAN

Sertifika No: 45724
Polis Akademisi Başkanlığı Basım ve Yayım Şube Müdürlüğü,
Fatih Sultan Mehmet Bulvarı No: 218 06200 Yenimahalle – Ankara

POLİS AKADEMİSİ BAŞKANLIĞI
Necatibey Caddesi No: 108 Anıttepe 06400 Çankaya-Ankara/Türkiye
Tel: +90 (312) 4629085-92-93 / +90 (312) 4629075 / +90 (312) 4629035
www.pa.edu.tr

İçindekiler

YÖNETİCİ ÖZETİ

"Güvenlik Yönetiminde Çağdaş Yaklaşımlar" başlıklı bu raporda küreselleşme ve güvenlik yönetimi ilişkisi çerçevesinde güvenlik yönetiminde örgütsel ve işlevsel değişimlere; küreselleşen dünyada polislik modellerinde ve uygulamalarındaki eğilimlere; küreselleşmenin kent ve güvenlik üzerindeki etkilerine; güvenlik ve insan hakları arasındaki ilişkiye değinilmektedir. Ayrıca teknoloji ve dijitalleşme kapsamında son yıllarda kullanıcı sayısının bariz bir şekilde artış gösterdiği dijital medyada dezanformasyon ve algı operasyonlarına; siber güvenlik sorununa; dijital dönüşümün istihbarat yönetimi üzerindeki etkilerine ve modern biyolojik teknikler ve uygulamalar barındıran biyolojik terör sorununa yer verilmektedir. Bunun yanında 21. Yüzyılda güvenlik yönetimine ilişkin tespit, sorun ve çözüm önerilerine yer verilen raporda yeni güvenlik tehditleri, kırılgan devletler, yeni nesil savaş, düzensiz göç, göçmen kaçakçılığı ve insan ticareti gibi küresel sorunlar ele alınmaktadır.

Bu rapor; 02 Haziran 2021 tarihinde Polis Akademisi Başkanlığı Anıttepe Kampüsünde konferans salonunda düzenlenen "*Güvenlik Yönetiminde Çağdaş Yaklaşımlar Çalıştayı*" sonucunda çıkartılmıştır. Çalıştaya çeşitli üniversitelerden, bürokrasiden, medyadan, düşünce kuruluşlarından, emniyet personelinden ve dinleyicilerden oluşan toplam 64 kişi katılım sağlamıştır. Raporda yer alan bilgi ve fikirler Çalıştay katılımcılarının tartışmaları, değerlendirmeleri ve sunumları çerçevesinde okuyucuyla buluşturulmuştur. Rapordaki ifadeler konuşmacıların Çalıştaydaki konuşma ve sunumlarından derlenmiştir.

Bu kapsamda raporda şu hususlar ön plana çıkmaktadır:

- Küreselleşmenin ilk kez ortaya çıktığı dönemde düşüncelerin ve bilginin sınırlar ötesinde varlık göstereceği ve top-

lumsal alanda pek çok dönüşüm sağlanacağına dair inanç söz konusuyken bu iyimser hava zamanla geri planda kalarak küreselleşmenin çok sayıda güvenlik tehdidine kapı araladığı fikri ağırlık kazanmıştır.

- Küreselleşme sınır aşan suçların, çevresel sorunların, terörün ve düzensiz göçler gibi önemli sorunların küresel olarak dolaşıma girmesine sebebiyet vermiştir.
- Yaşanan gelişmeler neticesinde güvenlik tehditlerinin içeriğinin genişlemesi ve geleneksel güvenlik anlayışının ulusal ve uluslararası güvenlik sorunları ile mücadele etmede yetersiz kalması hem yönetsel süreç üzerinde hem de spesifik olarak güvenlik yönetimi üzerinde önemli kırılmalar meydana getirmiştir.
- Yeni kamu yönetimi anlayışı, "yönetim" kavramının "yönetişim" kavramına evrilerek karşılıklılık esasına dayanan, vatandaşların katkısının da göz önünde bulundurulduğu bir anlayışı ortaya çıkarmıştır. Böylece kamu hizmetleri tüm paydaşların birlikte sahiplendiği bir olgu halini almıştır.
- Toplumsal hayatın içinde kolluk hizmeti veren polis teşkilatı, demokratik sistemlerin doğasıyla uyumlu bir şekilde; güçlü, sivil, dinamik ve esnek bir yapılanmaya sahip olmalıdır.
- Dünyada geçerli olan kolluk yapılanma türlerine baktığımızda üç ayrı modelle karşılaşılmaktadır. Bunlar; çoklu kolluk yapısı, ikili kolluk yapısı ve tekli kolluk yapısıdır.
- İçinde bulunduğu toplumun güvenlik ihtiyacına hizmet etmek üzere, gelişmiş demokratik ülkelerdeki polis eğitimlerinin ortak yönü toplumla uyumlu, sivil otoritenin sevk ve idaresinde, kısa süreli, uygulama ağırlıklı, etkin bir polis eğitimidir.
- Kolluğun en önemli vazifesinin kamu düzenini sağlamak olduğu düşünüldüğünde, bu vazifenin ifası insan hak ve

özgürlüklerinin de göz önünde bulundurulmasıyla mümkündür.

- İnsan hakları kültürünün yalnızca güvenlik sağlayan kolluk unsurlarıyla sınırlı olarak düşünülmesi insan haklarının toplum tarafından benimsenmesine sekte uğratacaktır. Öyle ki insan hakları düşüncesinin yalnızca güvenlik sağlayan unsurlar tarafından değil aynı zamanda güvenlik hizmeti alan kimselerce de benimsenmesi yadsınamaz bir gerçektir.
- Dezenformasyon döngüsü; oluşturma, yayılım, etki ve doğrulamadan oluşmaktadır. Bu konuda bir yaklaşım geliştirerek ister konvansiyonel olsun, ister hibrit olsun her türlü tehdide karşı toplumsal direnci artırmak büyük önem arz etmektedir.
- Teknoloji ile ilgili eğer olumlu kullanımlar varsa bunlardan faydalanmak, eğer riskler varsa bunlara yönelik önlemleri almak büyük önem arz etmektedir.
- Siber tehditler hem teknolojilerde, hem teknoloji destekli uygulamalarda güvenlik sorunlarına yol açmaktadır. Dolayısıyla devlet bir yandan kendi varlığına, hizmetlerine, politikalarına yönelik olarak 'siber alanda' güvenliğini sağlamalı, öte yandan da vatandaşların bu alanlardaki varlığını güvence altına almalıdır.
- Dijital dünyada propaganda, algı yönetimi, dezenformasyon çok daha zahmetsiz ve daha yıkıcı gerçekleşmektedir. İstihbaratı elde etmek kolaylaşırken İKK faaliyetleri giderek zorlaşmaktadır.
- Teknolojinin istihbarat yönetimine girmesiyle birlikte yanıltma ve dezenformasyon giderek çok daha büyük bir risk haline gelmektedir. Bu nedenle veri madencisi ve bunu doğru analiz edebilecek nitelikli insana duyulan ihtiyaç her zamankinden çok daha önemli hale gelmiştir.

- Biyoterörizmin temelinde yatan amaç; özelde insanların genelde ise tüm canlıların üzerinde olumsuz etkileri olan biyolojik patojenleri, biyolojik silah olarak kullanmaktır.
- Bir biyoterör saldırısının tahmin edilmesi zor olsa da sonuçları yıkıcı olabilir. Bu nedenle güvenlik yönetimi sürecinde biyoterör olgusu asla göz ardı edilmemelidir.
- Günümüzde ve yakın gelecekte kamu güvenliğini tehdit edecek sorunlar dört başlık atlında sınıflandırılabilir. Bunlar; insan kaynaklı tehditler, kaynak gereksiniminden doğan tehditler, çevresel tehditler ve dijital tehditlerdir.
- Yeni nesil savaşın amacı rakip gücün siyasi yönetimi ile kamu bürokrasisi arasındaki uyumu bozmak, siyasi iradede çalkantılar oluşturarak kargaşa meydana getirmek, çatışma alanını karşı tarafın en zayıf ve en çok kayıp vereceği alanda belirlemek ve nihayetinde devletin meşruiyetini tartışılır hale getirmektir.
- Yeni nesil savaşta devlet, savaştaki tekelini kaybetmiştir. Savaşın finansörü değişmiş, zafer olgusu belirsizleşmiş, sivil ve askeri alan arasındaki ayrım ortadan kalkmıştır.
- Yeni nesil savaş ile mücadele konusunda özellikle siber saldırılara karşı ülkelerin nitelikli eleman ihtiyacına öncelik vermesi gerekmektedir.
- Salgın nedeniyle toplum genelinde artan endişe, teknoloji kullanımının yaygınlaşması, siber saldırıların sayısında ve kapsamındaki artış, toplumlarda virüsün oluşturduğu kargaşa güvenlik ve asayiş endişesini de beraberinde getirmiştir. Korona virüsün getirdiği bu güvenlik endişesi sadece iç güvenliği etkilememiş, dış güvenliğe de yansımaları olmuştur.
- Korona virüs salgını, salgın hastalıklar, biyolojik silahlar gibi farklı türde tehditlere karşı dayanıklılığın güçlendirilmesini zorunlu kılmaktadır.

- Terör örgütleri salgının bazı ülkelerde ortaya çıkardığı otorite boşluklarından istifade ile yeni palazlanma süreçlerine girişmektedir. Özellikle aşırı sağcı yapılar salgının ortaya çıkardığı ekonomik zorlukları bahane ederek kendilerine zemin oluşturmaya çalışmaktadır.
- Gelişmiş Batılı ülkeler göçün insan hakları boyutunu göz ardı ederek yalnızca bir güvenlik problemi olarak tanımlayıp dışsallaştırma yaklaşımı sergilerken Türkiye göçe insan haklarına saygılı bir yaklaşım açısından bakarak geri kabul anlaşmaları, ikili ülke işbirlikleri, kalkınma odaklı projeler geliştirerek göç sorununu kaynağında kalıcı çözümler üreterek yönetmektedir.
- BM İnsani Güvenlik Komisyonu nihai raporunda geleneksel güvenlik algısına ait ifadeler görülmektedir; ancak bunların hayata yansıması konusunda ciddi sorunlar yaşanmaktadır.
- Uluslararası güvenlikte çalışmalar ve ilgilerin nereye kaydığına bakmak gerekirse buradaki odak noktasının insan olduğu belirtilebilir. Yeni konseptte insana yeni bir bakış açısı söz konusudur.
- Sosyal ağlarda paylaşılan veriler, kişisel verilerin paylaşımı konusu, sağlık güvenliği gibi konular artık uluslararası güvenliğin parçası haline gelmiştir.
- Güvenliğe ilişkin yeni risk alanları karma bir sorumluluk yüklemekte ve güvenliğin farklı yaklaşımlarla ele alınmasını beraberinde getirmektedir.

GİRİŞ

Soğuk Savaş'ın sona ermesiyle birlikte güvenlik çalışmalarında yeni bir dönem başlamıştır. Bu dönemde güvenliğin tanımından başlayarak geniş bir farklılaşma sürecine geçiş yapılmıştır. Geleneksel güvenlik çalışmalarının mevcut sorunlara çözüm üretme noktasında yetersiz kalışı, yeni güvenlik anlayışının toplumsal ihtiyaçlar doğrultusunda genişlemesini ve derinleşmesini beraberinde getirmiştir. Bu çerçevede risk ve tehditlerin belirli bir coğrafyadan gelmesi anlayışı yerine tek merkezden yönetilemeyen, belirsiz ve sınır aşan tehditler ortaya çıkmıştır. İki kutuplu dünya düzeninin ortadan kalkması, küreselleşme olgusunun hız kazanması, ABD'de meydana gelen 11 Eylül 2001 tarihli saldırılar ve terörist eylemler güvenliğin sınırlarını belirsizleştirerek içinde yaşadığımız zaman diliminde güvenlik olgusunun her zamankinden daha önemli bir arayış olmasına neden olmuştur. Sınır ötesinden gelebilecek tehditlere ve tehlikelere karşı dış güvenliği sağlamakla birlikte iç güvenliği tesis etmek de devletlerin en temel kaygısı olmuştur. Böylece güvenliğin küreselleşen karmaşık yapısı karşısında devletler güvenliği tesis etmek amacıyla sürekli bir şekilde yöntem ve stratejilerini revize etmek durumunda kalmaktadır.

Bilgi iletişim teknolojilerinde meydana gelen değişimler, dijital teknolojiler, ulaşım ve iletişim araçlarının gelişmesi; terör örgütleri, bazı devletler, organize suç örgütleri, özel kuruluşlar ve bireyler tarafından yeni saldırı tekniklerinin ortaya çıkmasına ve yeni suç türlerinin oluşmasına zemin hazırlamaktadır. Düzenli savaşların yerini teknolojik aygıtların etkin bir şekilde kullanıldığı yeni nesil savaşların aldığı ve konvansiyonel savaşların yerine hibrit savaşların gündeme geldiği günümüz dünya düzeninde güvenlik yönetimi de bu değişimlerden etkile-

nerek örgütsel ve işlevsel yapısını yeni değişim ve dönüşümlerle uyumlu hale getirmektedir. Güvenlik teşkilatları ve güvenlik sağlayıcı aktörler de değişen güvenlik paradigmalarından ve şehirleşmenin getirdiği toplumsal ilişkiler ağından kaçınılmaz olarak etkilenerek teşkilat yapısından personel istihdamına, eğitim süreçlerinden eğitim müfredatlarına varıncaya kadar değişim ve dönüşüm geçirmek zorunda kalmaktadır. Böylece güvenlik hizmetlerinin sunumu ve güvenlik uygulamaları da değişmektedir.

Küreselleşmenin getirdiği değişimden ilk etkilenen yerler olan kentsel alanlar, bireylerin kamu hizmetlerine olan taleplerinin arttığı yerler haline gelmekte ve güvenli bir kent tesis etmek hiç olmadığı kadar çetrefilli hale gelmektedir. Küreselleşmenin ekonomik boyutu olan neoliberalizm sorunlarını kent üzerinden çözmeye çalışmakta, kentin belli mekanlarının soylulaştırılması yeni suçluluk alanları ortaya çıkarabilmektedir. Bunun yanında dijital medyanın yaygınlaşmasıyla birlikte kitleler üzerinde gerçekleşen algı operasyonları ve psikolojik savaş gibi yöntemler kitlelerin hareket kabiliyetlerini kontrol altına almayı hedeflemektedir. Özellikle sosyal medyanın yaygın bir şekilde kullanılmasıyla birlikte manipülasyonların en önemli hedef kitlesi haline gelen bireylerin farkındalıklarının artırılması ve dezenformasyon konusunda bilinçlendirilmesi oldukça önem kazanmaktadır. Diğer taraftan teknolojideki ilerlemeler ve hızlı gelişme; daha ucuz maliyeti olan, hammadde temin etme konusunda sorun yaratmayan, hızlı yayılma özelliği gösteren, terör örgütlerinin tespit edilmesini zorlaştıran ve gizli kalmayı sağlayan biyolojik silahların kullanılmasını gündeme getirmiştir. Terör örgütlerinin biyolojik silah kullanma eğilimi ortaya çıkmış, biyoterör saldırılarına karşı toplumlar her an hazırlıklı olmak gerçeği ile karşı karşıya kalmıştır.

Bunların yanında tıpkı Suriye örneğinde olduğu gibi kırılgan devletlerde karşılaşılan siyasal istikrarsızlıklar, bu tür devletlerde çok sayıda silahlı gücün varlığını sürdürmesi, sınır güvenliklerini sağlamada karşılaşılan problemler, insan ticareti ve insan kaçakçılığının bölge ülkelere yansımaları; güvenlik yönetiminde izlenecek stratejilerde ve güvenlik politikalarında yeni yaklaşımları gündeme getirmektedir. Bu nedenlerle 21. yüzyılda "sınırları belirsiz'' bir olgu haline dönüşen güvenliğe ilişkin optimal düzeyde bir sonuç elde etme ve çağa ayak uydurarak güvenliği etkin bir şekilde yönetme zorunluluğu doğmaktadır. Bu bağlamda; küreselleşmenin güvenlik yönetimi üzerindeki etkilerini anlamak, küreselleşme ekseninde önemi artan kent güvenliğini değerlendirmek, polislik modellerinde yeni uygulamaları takip etmek, güvenliği tesis ederken insan hak ve hürriyetlerini gözetme hassasiyeti üzerinde durmak, teknolojide meydana gelen değişimler ışığında siber güvenlik ve istihbarat yönetimi konularında çağa ayak uydurmak, dijital ortamda gerçekleştirilen algı operasyonlarına yönelik gerekli çalışmaları yapmak, kontrolü güç olan biyoterör üzerine yoğunlaşmak, düzensiz göç, göçmen kaçakçılığı ve insan ticareti sorununa yönelik çözüm odaklı tedbirler almak ve nihai olarak mevcut sorunlardan ve tespitlerden hareketle güvenlik politikalarına yönelik yeni yaklaşımları analiz etmek büyük önem arz etmektedir.

Bu raporda; öncelikle küreselleşmenin güvenlik yönetimi üzerindeki etkileri tartışılmaktadır. Akabinde de güvenlik yönetiminde teknoloji ve dijitalleşmenin önemine yer verilerek; 21. yüzyılda güvenlik yönetimine ilişkin tespit, sorun ve çözüm önerileri değerlendirilmektedir.

KÜRESELLEŞME VE GÜVENLİK YÖNETİMİ

Ulaşım ve iletişim teknolojilerindeki gelişmelerle birlikte özellikle 18. Yüzyılda hızla adından söz ettirmeye başlayan ve sıkça tartışılan küreselleşme olgusu bir etkileşim ve entegrasyon sürecine işaret etmektedir. Malların, hizmetlerin, kültürlerin, ekonomilerin, insanların, bilginin dolaşımına ve sınır ötesi hareketliliğine vurgu yapmaktadır. Aynı zamanda küreselleşme olgusu yerelleşmeyi de içerisinde barındıran bir kavram olarak yerel olan üzerinde de nüfuz edici bir işlev görmektedir.

1990'lı yıllarla birlikte yoğun bir şekilde tartışılan küreselleşme olgusu hayatın her boyutunu derinden etkilemiştir. Güvenlik anlayışı ve uygulamaları da küreselleşme sürecinden derinden etkilenerek önemli tartışmalara kaynaklık etmiştir.

Küreselleşme süreci esasında iki ana eksen üzerinden tartışılmaktadır. Bunlardan ilki; küreselleşmeye ilişkin iyimser yaklaşımdır. Küreselleşmeye ilişkin iyimser yaklaşımda; küreselleşmenin otoriter rejimleri liberalleştireceği, uluslararası alanda şeffaf rejimler dolayısıyla çatışma yerine daha barışçıl ve güvenli bir dünya düzeni yaratacağı, değerleri küreselleştireceği, toplumları özgürleşeceği, mücadele yerine müzakere sürecini ön plana çıkaracağı, piyasa ekonomisini yaygınlaştıracağı ve uluslararası örgütlerin daha etkin ve güçlü olduğu bir yapıya kaynaklık edeceği gibi fikirler öne sürülmüştür. Ancak 11 Eylül saldırıları sonrasında bu tez zayıflayarak geri plana atılmış ve küreselleşme sürecinde risklerin, sorunların şiddetin, çatışmanın da küreselleşebileceği iddia edilmeye başlamıştır. Böylece daha kötümser bir bakış açısıyla; güvensiz, çatışmacı ve şiddet içeren bir dünyanın ortaya çıkabileceğini iddia eden yaklaşımlar gündeme gelmiştir. Bu duruma cevap olarak da güvenlik yönetimi alanının kendisini yeniden gözden geçirmesi, kendisini yenilemesi, boyut

ve kapasite kazanarak küresel tehditlerle başa çıkabilmesi için kendisini dönüştürme ve geliştirme ihtiyacı hasıl olmuştur. Bu çerçevede küreselleşmenin güvenlik yönetimi üzerindeki etkileri oldukça önem arz etmektedir.

Bu bölümde; küreselleşmenin güvenlik yönetimi üzerindeki etkileri ele alınmakta, küreselleşmeyle birlikte ortaya çıkan polislik modellerindeki değişimler, kent güvenliği ve değişen güvenlik anlayışının insan hakları ile ilişkisi değerlendirilmektedir.

Güvenlik Yönetiminde Yeni Arayışlar: Örgütsel, İşlevsel Değişimler

Devletler 14. Yüzyıl'dan başlayarak 16. Yüzyıl'a kadar bir değişim süreci geçirerek ulus-devlet kimliğine bürünmeye başlamıştır. Uluslaşma süreci toplumlar için önem arz etmektedir; çünkü bilhassa küreselleşmeyle birlikte devletin ulus-devlet kimliği ile ilgili birtakım niteliklere dair tartışmalar günümüze kadar taşınmıştır. Nitekim ulus devletler bulundukları dönemin imparatorluklarına alternatif olarak gündeme gelmiş ve ülke sınırları, dil ve kültür gibi pek çok unsurun uluslaşmasında yadsınamaz role sahip olmuştur. Devletin bu faaliyetleri ile birlikte bugün de etkili olan bir nitelik daha kazanması gündeme gelmiştir: Bu nitelik "Yönetici Devlet" vasfıdır.

Yönetici devlet kimliği devletin bireylerin yaşam alanları ile ilgili kamu politikaları olarak isimlendirilen hedefler belirlemesi ve bunları uygulamaya geçirmesi olarak tanımlanabilmektedir. Bu alanlardan biri de güvenliktir. Güvenlik; bireyin toplumsal düzende tehlikeden uzak yaşam sürdürebilmesi olarak ifade edilmektedir. Devletin ortaya çıkma nedenlerinin başında gelen güvenlik özellikle can ve mal güvenliği ile artı değerin muhafaza edilerek yeniden paylaştırılması gibi farklı ihtiyaçlar ile ilgili

hususlarda oldukça önem arz etmektedir. Kamu düzeninin de unsurlarından biri olan güvenlik küreselleşmenin etkilerinden çok daha evvel devletin varlığına meşruluk kazandırmaktadır. Tüm bu süreçle ilgili bilhassa iletişim ve ulaşım alanında yaşanan gelişmeler ürün ve malların dolaşımı ile bağlantılı olarak sınırlar hakkında tartışmalara da yol açmıştır. Küreselleşmenin ilk kez ortaya çıktığı dönemde düşüncelerin ve bilginin sınırlar ötesinde varlık göstereceği gibi olumlu düşüncelerin ve küreselleşmenin toplumsal alanda sağladığı pek çok dönüşüm sayesinde kolaylaştırıcı rol oynayacağına dair iyimser havanın yanı sıra çok sayıda güvenlik tehdidine de kapı araladığına ilişkin dezavantajlar tartışılagelmiştir. Bu durum sınır aşan suçların, çevresel sorunların, terörün ve düzensiz göçler gibi önemli sorunların küresel olarak dolaşıma girmesine sebebiyet vermiştir. Bunun bir sonucu olarak devletler yalnızca kendi sınırları içerisinde yaşanan bir olumsuzluğu veya güvenlik sorununu çözmenin gerçekte o problemi ortadan kaldırmaya yetmediğini görmektedir. Örneğin; günümüzde tüm insanlığın karşı karşıya kaldığı koronavirüs pandemisi bu duruma örnek teşkil etmektedir.

Soğuk Savaş döneminde ulus-devletlerin güvenlik anlayışı, Sovyetler Birliği'nin dağılmasının ardından küreselleşmenin getirdiği yeni tehditler nedeniyle farklı bir eğilim göstermiştir. Soğuk Savaş döneminde askeri tehditler etrafında şekillenen güvenlik anlayışı Soğuk Savaş sonrası dönemde daha kapsamlı olguları içeren, yalnızca askeri niteliğe sahip güvenlik meselelerinin ötesinde yeni sorunları gündeme getirmiştir. Devlet merkezli askeri güvenlik sorunları yerine bireyi temel alan; terörizm, göç, ekonomi, kimlik, çevre, siber güvenlik gibi uluslararası sorunları içeren güvenlik anlayışı ile karşı karşıya kalınmıştır. Güvenlik tehditleri tek boyutlu niteliğini kaybetmiş, asimetrik ve çok boyutlu bir konuma evrilmiştir. Bilhassa küreselleşme sürecinin de

etkisiyle kamu düzenini sağlama çabası daha geniş bir güvenlik anlayışının göz önünde bulundurulmasını zorunlu kılarak askeri güvenliğe ek olarak birey güvenliğini, içinde bulunduğumuz evrenin güvenliğini de içerecek şekilde entegre bir güvenlik yaklaşımını ortaya çıkarmıştır.

Yaşanan gelişmeler neticesinde güvenlik tehditlerinin içeriğinin genişlemesi ve geleneksel güvenlik anlayışının ulusal ve uluslararası güvenlik sorunları ile mücadele etmede yetersiz kalması hem yönetsel süreç üzerinde hem de spesifik olarak güvenlik yönetimi üzerinde önemli kırılmalar meydana getirmiştir. Bu minvalde 1980'li yılların başında "yeni kamu yönetimi" anlayışı ortaya çıkmıştır. Nitekim yeni kamu yönetimi anlayışı, "yönetim" kavramının "yönetişim" kavramına evrilerek karşılıklılık esasına dayanan, vatandaşların katkısının da göz önünde bulundurulduğu bir anlayışı ortaya çıkarmıştır. Böylece kamu hizmetleri tüm paydaşların birlikte sahiplendiği bir olgu halini almıştır. Akabinde ise "yeni kamu hizmeti" anlayışı gündeme gelmiştir. Bu anlayış, kamu hizmetlerini sunmada yeni bir zihniyet ortaya çıkarmakla birlikte özellikle "birey odaklı" bir anlayışa kapı aralamıştır. Dolayısıyla güvenlik yönetimi sürecinde bireyi temel alan ve birey güvenliğini ön plana çıkaran bir anlayış gelişim kazanmıştır.

Küreselleşmenin baskısı altında değişen bir dünyada güvenliği sağlama çabası, güvenlik yapısını daha insani ve toplumsal boyutlara indirgemekte ve tüm dünyada yeni mücadele alanlarını genişletmektedir. Küreselleşmenin de etkisiyle belirsiz bir niteliğe bürünen tehditlerle mücadele çok sayıda aktörün müdahalesini ve işbirliğini gerektiren bir yapıyı gerekli kılmaktadır.

Güvenlik alanında yaşanan değişimler kolluğun özellikle zor kullanma yetkisinde de yeni anlayışların ortaya çıkmasına zemin

hazırlamıştır. Zor kullanma yetkisi, meşruiyetini yeni kamu hizmetlerine ait ilkelere dayandırarak yasal bir yetki olmanın yanı sıra toplumun geneli tarafından da kabul görmeye başlamıştır. Böylece güvenlik kavramı, birey merkezli ve bireyin temel hak ve hürriyetlerini gözeten bir yapıya doğru bürünmüştür.

Toplumun ihtiyaçlarını karşılamak için güvenlik hizmetleri alanındaki uygulamalar sürekli ilerlemektedir. Küreselleşme sürecinde güvenlik politikalarının/siyasalarının meşruluğu içerecek şekilde, anayasacılık dairesinde, bireyi merkeze alarak yapılması oldukça önemlidir. Sadece yönetenlerin değil yönetilenlerin de dahil olduğu yönetişim anlayışı çerçevesinde icra edilecek güvenlik yönetimi süreci daha etkili bir yönetsel sürecin tatbiki açısından önem arz etmektedir.

Küreselleşme süreciyle birlikte uluslararası küresele ölçekteki tehditlere karşı devletlerin egemenliği tartışılırken, bir başka ifadeyle ulus devletin sonunun gelip gelmediğine ilişkin tartışmalar gündeme gelirken, aslında pratikte küreselleşmenin devletleri daha güçlendirdiği, devletleri daha da merkezileştirdiği ve merkezdeki iktidar yoğunlaşmasını daha da artırdığı söylenebilir. Bu durum genel olarak dikkate alındığında, güvenlik politikası söz konusu olduğunda, özellikle kamu hizmetlerinin muhatapları tarafından sahiplenilmesi meşruluk açısından oldukça önem taşımakta, temel hak ve özgürlükleriyle donatılmış birey merkezli bir güvenlik anlayışı önemini korumaktadır. Bu kapsamda mevcut riskler değerlendirilerek oluşturulan stratejik politikalar, yapısal düzenlemelerle güçlendirilmelidir. Değişen tehdit türlerine daha etkin yanıt verilebilmesi için kamu-özel işbirliğinin ve ulusal kurumlar ile uluslararası kuruluşlar arasındaki bağların artırılması, tatbik edilen uygulamaların meşruiyetini ve toplumsal kabulünü kolaylaştıracaktır.

Polislik Modellerinde ve Uygulamalarında Eğilimler

Her ne kadar tarihin her döneminde benzer yapıda ve benzer görevleri yerine getiren unsurlar bulunsa da kentsel güvenliğin sağlayıcısı olan modern polislik 19. Yüzyıl'ın bir ürünü olarak ortaya çıkmıştır. Bu oluşum Sanayi Devrimi'nin ve ardından meydana gelen yoğun kentleşmenin bir neticesidir. Standart personel yapısının, teçhizatın, bürokratik yapılanmalara dayalı polis teşkilatının doğumu Sanayi devrimi ve sonrasında yaşanan hızlı şehirleşmenin bir ürünüdür.

Günümüzdeki modern polis teşkilatının ilk örneğine 1829 tarihinde İngiltere'de Londra Metropolitan Polis Teşkilatında rastlanmaktadır. Bu trend Osmanlı İmparatorluğu tarafından da takip edilerek 1845 yılında İstanbul'da bir polis teşkilatının kurulduğu görülmektedir. 1891 yılında ise Osmanlı İmparatorluğu'nda başlatılan polis eğitimi aynı geleneğin günümüzde Polis Akademisi'nde de devam etmesine katkı sağlamıştır.

Modern polisliğin doğuşu çok büyük bir paradigma dönüşümünün bir ürünü olduğu gibi bugünün dünyasındaki polis yapıları da büyük dönüşümlerin etkisinde ortaya çıkmıştır. Bu dönüşümler küreselleşme sürecinin getirdiği değişiklikler ile internet devrimi ve iletişim alanında meydana gelen yenilikler neticesinde gerçekleşmiştir. Özellikle 20. Yüzyıl'da dünya nüfusunun pek çoğunun şehirlerde yaşamaya başlaması, şehirlerin metropollere dönüşmesi ve hatta günümüzde megapollerden bahsediliyor olması, polisliğin bu duruma uygun yeni esnek yapılanmalar dahilinde görevlerini ifa etme zorunluluğunu da beraberinde getirmektedir. Toplumsal hayatta meydana gelen değişimler daha karmaşık yapılar ortaya çıkarırken bu durum suçlara ve suçlu profillerine de sirayet etmektedir. Suç tiplerinde ve suçlu sayılarında yaşanan artış polis modellerinin de kendisini bu değişimle

mücadele etme noktasında dönüştürmesine yol açmaktadır. Ayrıca değişen dünyada bireylerin toplumla ve devletle yeni ilişki süreçlerine girmelerinde güvenlik hizmeti sunan polis güçlerinin dönüşümü de yadsınamaz role sahip olmaktadır.

Toplumla iç içe olan bir meslek olan polislik sosyal, iktisadi veya siyasal hayattaki herhangi bir değişiklikten doğrudan etkilenmektedir. İçinde bulunduğumuz modern çağda gerçekleşen ilerlemelere, değişim ve dönüşümlere, vatandaşların talep ve beklentilerine hızlı bir şekilde yanıt verebilmek amacıyla polis birimlerinin de mesleğe alımdan, mesleki eğitime ve meslekteki uygulamalara kadar kendisini dönüştürmesi kaçınılmaz bir hal almaktadır. Bu nedenle profesyonellik çerçevesinde görev yapacak polis teşkilatlarının işleyişinde esnekliğe, uzmanlaşmaya, şeffaflığa, hesap verebilirliğe ve demokratik uygulamalara önem verilmesi hiç olmadığı kadar gerekli hale gelmiştir. Gelişmiş demokratik ülkeler incelendiğinde, polis teşkilatlarının büyük çoğunluğunda yeni bir yapılanma sürecine girildiği, 21. Yüzyıldaki değişen ve gelişen şartların göz önünde bulundurulduğu; meşruluk, hesap verebilirlik ve şeffaflık gibi değerlerin önem kazandığı görülmektedir.

Dünyada geçerli olan kolluk yapılanma türlerine baktığımızda üç ayrı modelin bulunduğu görülmektedir:

1. Çoklu Polislik Yapısı: Çoklu polislik yapısına örnek teşkil eden ülkeler ABD, İngiltere, Kanada, Almanya, Avustralya, Brezilya, Hindistan ve Azerbaycan'dır. Çoklu polislik sistemi ile genel itibariyle federal yapıya ya da özerk bölgelere sahip ülkelerde karşılaşılmaktadır. Federal bir yönetim sisteminin söz konusu olduğu devletlerde farklı polis teşkilatları bulunmaktadır. Polis buralarda daha çok yerel yönetimlere, federal parlamentoya ya da hükûmete bağlı olarak görev ifa etmektedir. Çoklu

polislik yapısına haiz olan ülkelerde polisin uzmanlık alanına göre sınıflandırılması polisliğin işleyişi ile ilgili önemli sac ayaklarından birisidir. Polis teşkilatı parçalı bir bürokratik görünüm arz etmekte, farklı hiyerarşik yapılanmalara sahip olmakla birlikte mutlaka bir sivil otoriteye bağlıdır. Ayrıca bu tür ülkelerde polis istihdamı sürecinde ve mesleki işleyişte tek bir düzenleme söz konusu değildir. Her birim kendi çalışma koşullarına uygun şartlar getirebilmektedir. Ancak son zamanlarda gerek polis alımında gerekse de polis eğitimine ilişkin konularda ulusal düzeyde ortak standartlar geliştirilmiştir. İstihdam sürecinde genellikle eğitim düzeyi yüksek kişiler tercih edilmekte, polis okullarında kısa süreli eğitime önem verilerek polisliğin meslek sırasında öğrenilmesi esası baz alınmaktadır. Batı'daki çoklu kolluk yapısına sahip ülkelerin polislik eğitimi kısa süreli olmakla birlikte eğitim sürekli olarak, mesleğe yayılmış şekilde hizmet içi eğitimlerle desteklenmekte ve personelin mesleki anlamda bilgilerini sürekli tazelemesine dayalı bir biçimde yürütülmektedir. Polislik mekanizması siviller tarafından kontrol edilerek sivil denetime tabi olmaktadır.

2. İkili Polislik Yapısı: İkili polislik yapısı genellikle Akdeniz ülkelerinde rastlanan kolluk yapısıdır. İkili kolluk sistemine örnek olarak Türkiye, Fransa, İtalya ve İspanya ve Portekiz gibi ülkeler verilebilir. İkili polislik yapısı coğrafi alan itibariyle mekânsal bir farka dayalı kolluk yapılanma modelidir. İspanya dışında ikili polislik sisteminin varlık gösterdiği ülkeler üniter bir yapının ve merkezi yönetimin söz konusu olduğu ülkelerdir. Bu ülkelerde kent ve kırda görev yapan iki ayrı polislik kuvveti ile karşılaşılmaktadır. Kentte ve kırda görev yapan her iki kuvvet de hiyerarşik şekilde örgütlenmiş olup birbirlerinden bağımsız teşkilatlara sahiptir. Ancak her iki teşkilatın da genel itibariyle İçişleri Bakanlığı'na bağlı olduğu görülmektedir. Çoklu polis-

lik yapısı ile mukayese edildiğinde her birimin uzmanlaşmış birimleri de içerecek şekilde tek bir hiyerarşik teşkilat çatısı uhdesinde örgütlendiği belirtilebilir. Görev ve sorumluluk sahası kentsel alanlar olan polis genellikle sivil kökenli ve temelli iken; kırsal alanlardan sorumlu jandarma ve benzeri birimler askeri veya yarı askeri temellidir. İkili polislik yapısının olduğu ülkelerin çoğunda polisliğin sivil denetimi konusuna hassasiyet göstermek bağlamında kast sistemine mahal vermemek ve olası bir otonomlaşmayı elimine etmek için amir eğitiminde ara düzeylere yarı yarıya sivillerden alımlar yapılmaktadır. Bu ülkelerde genellikle polis temel eğitimi ve ilk kademe amir eğitimi bir yıl sürmektedir.

Türkiye de ikili polislik yapısı içerisine dahil edilen ve ikili polislik yapısına örnek teşkil eden ülkelerden birisidir. Türkiye'de 2015 yılında gerçekleştirilen ve demokratik gelişmiş ülkelerin polis eğitim modellerini temel alan reform akabinde Polis Akademisi bünyesinde gerçekleştirilen polis ve amir eğitiminde sivil iradeyi esas alan, şeffaflığa, hesap verebilirliğe dayalı, demokratik denetimine açık bir teşkilat oluşturmak amacıyla eğitim düzeyi yüksek kişilerden polis istihdamı sağlanmakta, mesleğe kişiliği ve kimliği oturmuş bireyler tercih edilmekte, kısa süreli ve teknik gelişmeleri içeren bir eğitim müfredatı izlenmektedir. Polis temel eğitimi Polis Meslek Yüksek Okulu (ön lisans düzeyinde 20 ay) ve Polis Meslek Eğitim Merkezi (8 ay) bünyesinde; polis amiri eğitimi ise Polis Amirleri Eğitim Merkezi bünyesinde ilk kademe amir eğitimi ve üst kademe amir eğitimi çerçevesinde demokratik polis eğitimi standartlarında verilmektedir**.**

3. Tekli Polislik Yapısı: Kolluk teşkilatlanmasının tek çatı altında birleştiği modeldir. İsveç, Finlandiya, Belçika, Avusturya, Polonya, Çekya Japonya ve Mısır gibi ülkeler tekli polislik

yapısının varlık kazandığı ülkelerdir. Bu ülkeler üniter bir yapıya sahip olup, polislik sivil bir yapıdadır. Polis İçişleri Bakanlığı'na bağlı olarak görev yürütmektedir.

İsveç, Belçika ve Avusturya gibi ülkelerin bir dönem ikili kolluk yapısına sahipken bunu zaman içinde tekli kolluk yapısına dönüştürdükleri görülmektedir. Şehirleşmenin güçlü şekilde kendini hissettirmesi, toplumsal ilişkiler ağının farklılaşması gibi değişkenler bu ülkelerin jandarma teşkilatlarını lağvederek polislik teşkilatlarını güçlendirmelerini beraberinde getirmiştir. Tekli polislik yapısına sahip olan ülkeler tek bir polis gücüne sahip olmakla beraber polis teşkilatının kendi içinde farklı özel ve yerel bölümleri bulunabilmektedir. Örneğin; Belçika ve Avusturya hem jandarmayı hem de diğer polislik birimlerini tek bir polis teşkilatı altında birleştirmesine rağmen her iki ülkede de federal ve yerel polis birimleri bulunmakta ve bu birimler tek bir ulusal polis teşkilatının birimleri olarak görev ifa etmektedir. Kolluğun sivil denetimi tekli polislik yapısına haiz ülkelerde de oldukça önemlidir. Mesela Belçika'da sivil denetimi daha da güçlendirmek için aynı amir rütbelerinin farklı düzeylerine büyük çoğunluğunu sivillerin oluşturduğu lisans mezunlarından alım yapılmaktadır ve bu amir adaylarına kısa süreli eğitim verilmektedir. Ancak yukarıda belirtilen ülkeler içerisinde Mısır daha otoriter, katı ve askeri eğitim anlayışına tabi bir ülke örneğidir.

Polislik modellerinin yanı sıra her ülkenin kendine has polis eğitim modelleri de bulunmaktadır. Ancak gelişmiş demokratik ülkelerdeki polis eğitimlerinin temel ortak özelliklerine bakıldığında polisin sivil otoritenin sevk ve idaresinde olduğu, kısa süreli, uygulama ağırlıklı eğitim verildiği ve toplumla iç içe bir polislik yapısının inşasının amaçlandığı görülmektedir.

Mesleğe alımlara ilişkin trendlere bakıldığında dikkat çekici olan bazı hususlar öne çıkmaktadır. Özellikle toplumun değişen yapısına adapte olacak şekilde, gelişmiş ülkelerde polis memurlarının ve amirlerinin yüksek düzeyde eğitimlilerden tercih edildiği görülmektedir. Böylece hizmet edilen toplum içerisinde polis teşkilatı olarak o toplumun eğitim seviyesinin altında kalınmamaktadır. Bu konuda yapılabilecek bir başka tespit de demokratik ülkelerde yüksek eğitimli polislerin şeffaflık, hesap verebilirlik gibi ilkeleri daha kolay özümsedikleridir. Bu tür ülkelerde gittikçe artan düzeyde yüksek eğitimli personel polis teşkilatına dahil olmaktadır. Bu nedenle bugünün dünyasında polisliğin militer bir eğitim zihniyetinden uzaklaştırılarak toplumun dinamik ve çeşitlilikler içeren yapısıyla daha uyumlu hale getirilmeye çalışıldığı görülmektedir. Vatandaş odaklı, bireylerin beklentilerine ve çağın gerekliliklerine hızlıca yanıt veren, etkin ve etkili bir polis birimi ortaya çıkmaktadır. Başta polis amirleri olmak üzere polisin eğitim niteliği yüksek, kişilik ve kimlik itibariyle olgun kişilerden seçilmesi polis teşkilatlarını daha nitelikli bir yapıya kavuşturmakta, demokratik ve çoğulcu yapı sayesinde polis birimlerinin belirli bir yapının kontrolünde olmasını ve bürokratik vesayet düzenin ortaya çıkmasını engellemekte ve güvenlik hizmetlerinin sağlanmasında vatandaş-polis etkileşimini sağlayarak suçun önlenmesinde iş birliğini güçlendirmektedir.

İnsan Hakları ve Güvenlik

İnsan hakları demokratik toplumların vazgeçilmez ölçüsüdür. Doğal haklar öğretisinin bir uzantısı olarak bireyin sadece insan olması nedeniyle sahip olduğu haklar şeklinde tanımlanabilir. Güvenlik ise; korku ya da baskı altında kalmadan yaşayabilmek için gereken şartların tamamıdır. Devletlerin mevcudiyetindeki asıl gerekçe; hak ve özgürlükleri korumak ve güvenceli bir duruma bağlamaktır. Aksi takdirde devlet olgusu kendi varlık nedenini yadsımış olacaktır.

Kolluğun en önemli vazifesinin kamu düzenini sağlamak olduğu düşünüldüğünde, bu vazifenin ifası insan hak ve özgürlüklerinin de göz önünde bulundurulmasıyla mümkündür. Ancak insan hakları kültürünün yalnızca güvenlik sağlayan kolluk unsurlarıyla sınırlı olarak düşünülmesi insan haklarının toplum tarafından benimsenmesine sekte uğratacaktır. Öyle ki; insan hakları düşüncesinin yalnızca güvenlik sağlayan unsurlar tarafından değil aynı zamanda güvenlik hizmeti alan kimselerce de benimsenmesi oldukça önemlidir. Bu kültür hak arama kültürünün de toplum nezdinde bir yansımasıdır. AGİT'in 1991 tarihli Moskova Deklarasyonu'nda da belirtildiği üzere insan hakları konusunda yalnızca kolluk personelinin değil aynı zamanda halkın da bu konuda eğitilmesi ve farkındalığa sahip olması gerektiği belirtilmektedir.

Günümüzde insan hakları kavramı demokratik bir toplumun vazgeçilmez bir ölçütü haline gelmiştir. Ancak insan hakları ve güvenlik konusu özellikle Batı'da 11 Eylül 2001 tarihinde yaşanan terör saldırıları sonrasında farklı bakış açılarının gelişmesine sebebiyet vermiştir. Bu bakış açısına göre insan hakları ve güvenlik kavramları birbirini tamamlayıcı unsurlar olmak yerine birbirinden farklı iki düşünce olarak varlık göstermeye başlamıştır. Ancak vurgulanması gereken önemli bir husus güvenliğin tesisi için bireyin hak ve özgürlüklerinin göz ardı edilmemesi gerektiğidir. İnsan hakları ve güvenlik, bir yandan değişen ve artan tehditlerin merkezinde güvenlik kavramının yer aldığı, diğer yandan da bireysel hak ve özgürlükler ile insan onur ve haklarına saygı gösterilmesi gereken bir toplum yaratılması amacıyla biri diğerine tercih edilemeyecek olgulardır. Dolayısıyla insan hakları ve güvenliğin aslında birbirini ayrıştıran değil, birbirini tamamlayan kavramlar olduklarının altı çizilmelidir.

GÜVENLİK YÖNETİMİNDE TEKNOLOJİ VE DİJİTALLEŞME

Modern teknolojinin gelişmesi ve dijitalleşme bir yandan güvenlik yönetimi sürecinde yeni gelişmeleri mutlaka göz önünde bulundurmayı zorunlu kılmakta; diğer yandan da yeni güvenlik tehditleri ortaya çıkarmaktadır. Yeni teknolojilerin benimsenmesiyle beraber sosyal medyanın büyük bir kullanıcı sayısına eriştiği günümüzde dezenformasyon ve algı operasyonları yürütülmekte, siber saldırıların sayısı artmakta, güvenlik yönetiminde yapay zekâ ağırlıklı uygulamaların etkinliği artmakta, istihbarat faaliyetleri yeni bir dönüşüm sürecine girmekte ve terör faaliyetleri biyolojik saldırılar üzerinden gerçekleşmektedir.

Bu bölümde teknolojik dönüşümlerin ve dijitalleşmenin güvenlik yönetimi üzerindeki etkileri değerlendirilmektedir.

Dijital Medyada Dezenformasyon ve Algı Operasyonları

Dezenformasyon birçok temada Türkiye'yi ilgilendiren kapsamlı bir konudur. Bilhassa gezi olayları ve sonrasında yaşanan 15 Temmuz hain darbe girişimi akabinde dezenformasyon konusu üzerine titizlikle durulmaya başlanılmıştır.

66 numaralı İletişim Başkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesinde Değişiklik Yapılmasına Dair Cumhurbaşkanlığı kararnamesi kapsamında İletişim Başkanlığı Stratejik İletişim ve Kriz Yönetimi Dairesi Başkanlığı kurulmuştur. Daire Başkanlığı devletin kurumları ve kuruluşları arasındaki dezenformasyonla mücadele ile ilgili koordinasyon görevini icra etmektedir. İletişim Dairesi Başkanlığı'nın yanında Milli Güvenlik Kurulu Genel Sekreterliği, İçişleri Bakanlığı, Emniyet Genel Müdürlüğü gibi kurum ve kuruluşlar da bu görevi ifa

etmektedirler. Ancak İletişim Dairesi Başkanlığı'nın hedefi bu konu üzerinde daha fazla yoğunlaşarak, karşı koyma yaklaşımı ortaya koymaktır.

Manipülasyon, algı yönetimi, psikolojik harekât gibi yöntemlerle toplumun belirli hedef kitleleri üzerinde veya tümü üzerinde küresel çapta etkiler yaratılmaktadır. Bunun en bariz örneği yeni kelimelerin icat edildiği pandemi sürecinde görülmüştür. Örnek olarak son zamanlarda sıklıkla kullanılan '*exformasyon*' kelimesi gösterilebilir. Söylenen az kelimeler ile birçok şeyin ifade edilmesine exformasyon denir. Ancak o kadar az kelime söylenmektedir ki ne ifade edildiği veya neyin ima edildiği aslında net olarak belirtilmemektedir. Esasında söz konusu durum bir misenformasyon, malenformasyon ve dezenformasyona faaliyetine dönüşmektedir.

Misenformasyon zarar verme kastı olmadan paylaşılan yanlış bilgidir. Yanlış fotoğraf başlıkları, tarihler, istatistikler, çeviriler veya hiciv maksatlı kasti olmayan hatalar örnek olarak gösterilebilir. Malenformasyon ise zarar verme niyetiyle paylaşılan gerçek bilgiler veya görüşlerdir. Nefret söylemi, taciz, karalama ve kötüleme için kişisel veya kurumsal özel bilgilerin kasıtlı olarak yayınlanması örnek olarak gösterilebilir. Bu çerçevede dezenformasyon ise zarar verme niyetiyle kasıtlı olarak yanlış veya çarpıtılmış bilgiyi paylaşmak ve yaymaktır. Örnek olarak kasıtlı olarak değiştirilmiş işitsel, görsel içerikler, kasıtlı oluşturulan komplo teorileri veya söylentileri gösterilebilir.

Dezenformasyon döngüsü; oluşturma, yayılım, etki ve doğrulamadan oluşmaktadır. Bu konuda bir yaklaşım geliştirerek ister konvansiyonel olsun, ister hibrit olsun her türlü tehdide karşı toplumsal direnci artırmak büyük önem arz etmektedir.

Güvenlik çalışmaları ile ilgili olası her tür tehdide karşı yeni tür yaklaşımlar belirlenmesi bir zorunluluktur. Özellikle dezenformasyon odaklı stratejik iletişim ve kriz yönetimi yaklaşımı geliştirmek birincil derecede öneme sahiptir. Dünyada bunla ilgili birkaç ekol mevcuttur; ancak karşı koyma konusunda bir milli ve yerli yaklaşım geliştirme zorunluluğu söz konusudur.

Dezenformasyon konusunda bazı ekoller şu şekildedir:

- İsrail'in *hasbara* ekolünün dezenformasyonla mücadele konusunda son dönemde kısmen makas değişimi yaptığı görülmektedir. İbranice bir kelime olan hasbaranın en yakın karşılığı bir şeyi anlatmak savunuculuğunu yapmaktır. Hasbaranın amacı; İsrail devletinin her türlü savunmasını yapmak, ona karşı uygulandığı iddia edilen dezenformasyon faaliyetlerine karşı koymak ve dahası dezenformasyon faaliyetlerinde bulunmaktır.
- İkinci ekol ise yakından takip edilmesi gereken İngilizlerin *Government Communication Service* ve *Government Communications Headquarters*'dır. İngilizler sivil ve askeri istihbari yapıları birbirinden ayrı tutmak ve onları ayrı gösterme konusunda başarılıdırlar. Government Communication Service birçok pratiğe sahip olan ve stratejik iletişim konusunda çok başarılı olan bir birimdir. Government Communications Headquarters biraz daha sivil taraflı bir stratejik iletişim ve kriz yönetimi yöntemiyle hareket etmektedir.
- Üçüncü diğer bir ekol ise NATO ekolu, yani, TRATCOM'dur. STRATCOM; benzer şekilde ABD Savunma Bakanlığı'nın komutanlıklarından birisidir. İletişim ve enformasyon etkileme faaliyetleri yürütülmektedir.
- Dördüncü ekol ise Amerika'nın karışık, karmaşık ve yay-

gın ekolüdür. Bu ekolde bir konuyla ilgili birçok kurum mevcuttur. Amerika'nın istihbarat yapısı ve enformasyona karşı koruma yapısına bakıldığında sayıca çok fazla olduğu görülmektedir. Söz konusu bu resmî kurumların birbiriyle olan çatışması, mücadelesi ve işbirliği dikkat çekicidir.

Uluslararası ilişkiler ve siyaset bilimi açısından bir değerlendirme yapılacak olursa bir güç taksonomisinin olduğu görülmektedir. Bu taksonomi konvansiyonel sert güç, yumuşak güç ve ikisinin birleşiminden oluşturulduğu iddia edilen akıllı güçten oluşmaktadır. Ancak teknolojik gelişim, veri temelli iş modelleri, Facebook, Amazon vb. çeşitli platformlar, manipülasyon amacıyla ve insanların algılarını değiştirmek amacıyla verilerin kullanılması gibi durumlar dördüncü bir güç türü olarak siber gücü ortaya çıkarmıştır.

Siber güç Harvard Üniversitesi eski profesörlerinden Joseph Nye tarafından ortaya atılmıştır. Batılı devletler, 2015-2016'lara kadar dünyanın en büyük teknoloji şirketleri arasında bir veya iki Çin şirketinin olduğunu ancak 2021 başı itibariyle on üç tane Çin şirketinin ilk yirmide yer aldığını ve çok güçlü bir şekilde geldiklerini fark etmiştir. Bu durumda Batı Bloğu kendi elinde bulunan hiçbir gücün onlar tarafından kullanılmasına izin vermek istememiştir. Yeni bir yakıştırma, elinde bulundurdukları teknolojik gücü dezenformasyon maksatlı kullanan Rusya, Çin, Kuzey Kore gibi ülkelere yöneliktir. Bu ülkeleri belli bir sepete dâhil ederek keskin güç şeklinde nitelendirmektedirler.

Dezenformasyon konusunda dikkat edilmesi gereken hususlar şunlardır:

- Teorik olarak kullanılan her görsel bizatihi kendisi dezenformasyon aracı olabilir. Sunum hazırlamak ve onu hoş hale getirmek arasındaki denge bir türlü sağlanamamaktadır.

- Yapay zekâ, teknoloji, dijital dönüşüm vb. konularda özellikle dezenformasyon konusuna çok dikkat edilmesi gerekmektedir.
- Bireyler inceleme ve araştırma yapmadan görseller indirerek kullanmaktadır ve söz konusu alıntılar Türkiye'yi dezenformasyonun kaynak ülkesi olarak gösterebilmektedir.
- Dezenformasyon amacıyla yurt dışından gelen tehditlerin kaynağı FETÖ ve aşırı sol örgütlerdir. Türkiye'ye yönelik gerçekleştirilen dezenformasyon faaliyetlerinin temel hedefi Türkiye'nin Azerbaycan, Libya ve Suriye'de yaptığı başarılı çalışmaları gölgelemektir.
- Temelde dezenformasyon sadece Türkiye'nin sorunu değildir. Birçok ülke ve kuruluş şu anda haritalandırma çalışmaları yapmaya çalışmaktadır. Böylece tehdidin nereden geldiği, nasıl melezleştiği, dezenformasyonun ne olduğu, nereye gittiği vb. konular tespit edilmeye çalışılmaktadır.
- Esas itibariyle dezenformasyon bir süreç olabilir ve dezenformasyona en açık kesim, kendine en çok güvenen kesimdir.

Dezenformasyonun ve yanlış bilginin tespit edilebilmesi için;

- Kaynağın kontrol edilmesi,
- Başlığın altının okunması,
- Yazarın kim olduğuna bakılması,
- Tarihin kontrol edilmesi,
- Destekleyici kanıtların incelenmesi,
- Önyargıların kontrol edilmesi,
- Teyit kuruluşlarına bakılması gerekmektedir.

Nihai olarak Türkiye'nin dezenformasyona karşı koyabilmesi için stratejik bir çerçeve geliştirilmesinde yarar vardır. Pozitif bir gündem ile negatif gündem arasındaki bağın kurulabilmesi ve akademik çalışmaların daha kaliteli, daha nitelikli daha nicel araştırmalara yönelik hale getirmesi büyük bir öneme haizdir.

Teknolojik İlerlemeler ve Gelişmeler Işığında Siber Güvenlik

Genelde teknoloji konusu söz konusu olduğunda iki farklı eğilimden bahsetmek mümkündür. Birincisi; tamamen meseleyi distopyalar ile ilişkilendirilen ve bir korku imparatorluğuna çevirme eğiliminde olan despotik yaklaşımdır. İkincisi ise her şeyin mükemmel olacağı, insanların huzurla, mutlulukla yaşayacağı bir gelecek tasavvurudur. Teknoloji ile ilgili eğer olumlu kullanımlar varsa bunlardan faydalanmak, eğer riskler varsa bunlara yönelik önlemleri almak büyük önem arz etmektedir. Burada *Gaddare* kelimesi ile karşılaşılmaktadır. "Gaddere" iki ucu keskin bıçak anlamına gelmekte ve aslında teknoloji denilen şey tam olarak ifade etmektedir.

Teknoloji zaman içerisinde ciddi değişim ve dönüşüm geçirmiştir. Teknoloji insanlık çağını ve alışkanlıklarını değiştirmekte ve dönüştürmektedir. Sabanın icadı nasıl ki tarım üzerinde ciddi değişiklik yarattıysa, ya da barut ve pusula dünyada nasıl önemli kırılmalara neden olduysa günümüzde de bilginin keşfiyle birlikte önemli bir dönüşüm söz konusudur. 20. yüzyılda en çok tartışılan hususlardan biri bilgi toplumu olmuştur. Günümüzde dijitalleşmiş bilgi toplumuna doğru bir eğilim olduğu görülmektedir.

Bit-internet, büyük veri (big data), sosyal medya, nesnelerin interneti-5g, yapay zekâ, arttırılmış gerçeklik, robotik teknolojiler, kayıt zincir (blockchain), akıllı şehir/kent (smart city), yaşam/yaşayan laboratuvarları, derin-karanlık internet, bulut bilişim ve otonom araçlar yeni dönüşümün araçları olmuştur. Söz konusu araçların güvenliğe etkisi ile ilgili ikili bir uçtan bahsetmek mümkündür. Birinci unsur, güvenlik politikalarında teknolojinin kullanılması; ikinci unsur ise teknoloji politikalarında güvenliğin sağlanmasıdır. Yani bir taraftan teknolojiden araç ola-

rak faydalanılması diğer taraftan ise bu yeni alanda güvenliğin sağlanmasının nasıl mümkün kılınabileceği oldukça önem arz etmektedir.

Veri temelli yönetim çok kıymetlidir ve bununla ilgili çalışmaların yapıldığı bilinmektedir. "Veri yeni petroldür" ifadesi klişe olsa da gerçekten çok önemli bir söylemdir. Hayatın her alanında ve yerinde veri ile karşı karşıya kalınmaktadır. Şöyle ki; akıllı saatlerle, akıllı tartılarda, mobil uygulamalarda, sosyal medya hesaplarında, kameralarda veri ile karşı karşıya kalınmakta, her yerde ve her an veri üretilebilmektedir. Özellikle sosyal medyanın yaygınlaşması ile birlikte veriler politika oluşturma sürecinde de etkili bir kaynaktır. Örneğin ABD karşıtlığının ülkeler açısından sosyal medya üzerinden ölçüldüğünü ve mesajlar üzerinden ülkelere özgü politikalar geliştirildiğini söylemek mümkündür.

2020 yılı itibariyle kişi başına düşen internete bağlı cihaz sayısı 6.5'tir. Buzdolapları, kombiler, telefonlar, saatlerin hepsi internete bağlandığında veri miktarı artmaktadır. Dolayısıyla veri temelli yönetimin altyapısının oluştuğu görülmektedir. Veri temelli yönetimin en önemli unsuru ise büyük veridir. Bu veriler çok hızlı şekilde yayılmakta ve anlık olarak çok fazla veri üretilebilmektedir. Söz konusu veriler farklı kaynaklardan gelmektedir. Dolayısıyla bu kaynak çeşitliliği verinin sağlamasının yapılması imkânı sunmaktadır.

Sosyal medyada yapılan bir paylaşım istemsiz veya baskı sonucu yapılabilmektedir. Ancak diğer taraftan kullanılan araçlar onun sağlamasını yapma imkânı sunmakta ve sonuç olarak büyük veri bir değer üretmektedir. Söz konusu veriler ise yapay zekâ eliyle üretilmektedir. Yapay zekâ insanlar gibi düşünen, insanlar gibi davranan ve insanlar gibi rasyonel düşünen sistemler-

dir. Hatta insanlardan daha rasyonel davranan sistemler olarak bile adlandırılabilir.

1990'lara kadar sınırlı ussallık söylemi mevcut iken, yani insanların zihni kapasitesinin sınırlı olduğu ve yeterli veriyi işleyemeyeceği veya en iyi sonucu bulamayacağına yönelik bir söylem söz konusu iken, yapay zekâyla birlikte daha iyi kararların, daha rasyonel kararların, daha akılcı yönetimlerin uygulamaya koyulabileceği görülmüştür. Hatta bu teknoloji marifetiyle polis teşkilatları da büyük bir analiz sistemi kullanarak gerçek zamanlı analizler yapabilmektedir. Yani potansiyel suçlu tespiti ve potansiyel olay tespiti üzerinden hızlı müdahale sistemi geliştirilebilmektedir. Örneğin; ABD/Boston'da büyük veri analiz sistemiyle gerçek zamanlı analiz yöntemiyle 1 yıl içerisinde şiddet suçlarında %17'lik bir düşüş; gasp suçlarında ise %19'luk bir düşüş sağlanmıştır. New York teşkilatı benzer bir sistem kurarak beş yıl içerisinde hırsızlık ve cinayet suçlarında %50 oranında bir düşüş sağlamıştır. Bu durum sadece gelişmiş ülkelere özgü bir durum değildir. Kolombiya'da dahi kapalı devre sistemleri üzerinden toplanan veriler ve yapay zekâ destekli risk modellemeleri kullanılmaktadır. Bir başka örnek ABD Ulusal Güvenlik Ajansı (NSA) ve istihbarat teşkilatı olan CIA'nın sürekli farklı teknoloji şirketleriyle işbirliği yapmasıdır. Bunlardan bir tanesi Palantir şirketidir. "Palantir" kavramı uzakları gören veya uzakları gösteren taş demektir. Palantir dünyanın dört bir yanından veri toplayarak bu veriler üzerinden analizler yapmaktadır. NSA veya CIA bu verileri uluslararası operasyonlarda kullanmaktadır. Örneğin Usame Bin Ladin'in yakalanması ve Sudan'daki iç savaşta Amerika karşıtı muhaliflerin elimine edilmesinde Palantir şirketinin desteğinin olduğu açık kaynaklarda yer almaktadır. Malezya örneğine bakıldığında ise kapalı devre kamera sistemlerinin acil durum yönetimi için kullanıldığını, yangın alarmları-

na bağlı bir sistemle acil durum müdahale sisteminin geliştirildiği görülmektedir. Bu sistemle yangının ilk aşamasına müdahale imkânı verildiği tespit edilmiştir. Aynı sistem trafik kazaları için uygulandığında da %96'lık bir doğruluk payı ile yönlendirme ve tahmin imkânı elde edildiği görülmüştür. Böylece insanın gecikme durumunun sistemden çıkartıldığı ve rasyonel bir yapının sisteme entegre edildiğini görülmektedir. Benzer bir sistemin New York İtfaiye İdaresi tarafından da kullanıldığı bilinmektedir. Ayrıca robotlar Fransa'da askeri eğitimlerde ve tatbikatlarda kullanılmaktadır. Söz konusu robotlar tehlikeli bölgelerde kullanılmakta veya ön bir kuvvet olarak robotlardan faydalanılmaktadır.

Esasında teknoloji önemli fırsatlar sunmakla beraber her bir teknoloji veya uygulama yeni bir riski de beraberinde getirmektedir. Özellikle kişisel verilerin korunması hususu bu risklerden birisidir. Türkiye'de verilerin korunması noktasında Kişisel Verilerin Korunması Kanunu (KVKK) çerçevesinde önemli bir adım atılmıştır

Uluslararası ölçekte sosyal medya ağlarında yakın zamanda veri kaçaklarının arttığı gözlenmektedir. Örneğin Amerika'da 10 milyon kişinin sağlık verilerinin çalındığı bilenmektedir. Veri kaçaklarının veya verilerin başkalarının eline geçmesinin önlenmesi için *blokzincir* (*blockchain*) kullanılabilir. Söz konusu veriler farklı yerlerde birbirine bağlı olarak tutulduğu için diğer sistemlerden farklı olarak bu sistemde verileri korumak daha kolay olmaktadır. Ancak; blokzincir sistemi kendi içinde bazı riskler de barındırmaktadır. Söz konusu risklerinden birisi merkezi sistemler kurmasıdır. Bu sistem devletin meşru güç kullanma yetkisine zarar verebilme kapasitesine sahiptir. Fakat devlet bu sistemi kullandığında bazı avantajlarda elde edebilmektedir. Bu sistemler; araç sicilleri, kaza ve bakım kayıtları, oto hırsızlığının

önlenmesi ya da azaltılması, istihbarı kayıtlar, tapu, nüfus, sağlık, sosyal güvenlik kayıtlarında avantajlar sağlamaktadır. Ayrıca ABD'de sınır güvenliği uygulamalarında kimlik kontrollerinin sağlanması, Güney Kore'de de sınır güvenliği ile gümrük kontrollerinde ve İngiltere'de sosyal yardımların dağıtılmasında bu sistemden istifade edilmektedir.

Siber tehditler hem teknolojilerde hem teknoloji destekli uygulamalarda güvenlik sorunlarına yol açmaktadır. Dolayısıyla devlet bir yandan kendi varlığına, hizmetlerine, politikalarına yönelik olarak 'siber alanda' güvenliğini sağlamalı, öte yandan da vatandaşların bu alanlardaki varlığını güvence altına almalıdır. Söz konusu teknolojilerde yerli ve milli imkânların kullanılması büyük önem arz etmektedir. Ayrıca;

- Kritik altyapıların korunması ve mukavemetin artırılması,
- Ulusal kapasitenin geliştirilmesi,
- Yeni nesil teknolojilerin güvenliğinin sağlanması,
- Siber suçlarla mücadele edilmesi,
- Siber güvenliğin milli güvenliğe entegrasyonu sağlanması,
- Uluslararası iş birliğinin geliştirilmesi gerekmektedir.

Dijital Dönüşüm ve İstihbarat Yönetimi

Mevcut üretilen yapay zekâ çözümleri ile verilerin yönetilebilmesine "dijitalleşme" denir. Diğer taraftan verilerin yapay zekâ yardımıyla bilgisayar ortamına aktarılarak ulaşılabilirlik ve bağlantısallık kazandırılmasına "dijitalleştirme" adı verilir. "Dijital dönüşüm" ise dijital ürün ve dijital çözüm üretimlerinin bir arada topyekûn bir yönetim sistemine dâhil edilmesidir. Esasında dijital dönüşüm bir süreçtir. Dijital dönüşüm ile istihbarat yönetimi birer kültürel olgudur ve kendi içinde ortak değerler ile semboller taşımaktadır. Aynı alanda çalışan kişiler tarafından kurulan

organizasyonlarca yönetilmektedir. Ayrıca kendine has yaklaşımlar, davranış kodları, iletişim biçimleri mevcuttur.

Dijital kültür denildiğinde şu unsurlarla karşılaşılmaktadır:

- Dijital habituslar (dijital yerliler ve dijital göçmenler),
- Dijitalleşmenin algının, deneyim ve görgünün önüne geçmesi,
- Veriye kolay erişim,
- Zaman-mekân farklılığının ortadan kalkması,
- Yeni kamusal alanların oluşması,
- Toplumsal kimliklerin akışkanlığı.

Operasyonel çevrede verilerin toplandığı, bu verilerin ayıklanarak işlendiği ve nihai olarak bu verilerin analiz edilerek üretildiği sürece ise "istihbarat yönetimi" denilmektedir. Esasında istihbarat yönetimi bir kültürdür ve temelde bu kültür ülkelerin güvenlik kültüründen çok farklı değildir. İstihbarat yönetimi içerisinde tehditlerin ve risklerin nasıl tanımlandığı önemlidir. Zira her ülke için veya her grup için risk kavramı değişkenlik göstermektedir.

İstihbarat yönetimi kültürünün unsurları şunlardır:

- Devletin yönetim biçimi,
- Tehdit, risk ve gizlilik kavramlarının tanımlanma biçimi,
- Anayasal düzen ve iç hukuk,
- Önleme ve koruma yaklaşımları,
- Sorumluluk ve yükümlülüklerin paylaşımı,
- Teknoloji kullanımı,
- Birey-devlet ilişkisi.

Gizlilikten ne anlaşıldığı, algı düzeyi, teknoloji kullanımı, birey-devlet ilişkisi, anayasal düzen gibi kavramlar bir arada düşünüldüğünde her toplumun ve her ülkenin kendine has bir istihbarat yönetim kültürü olduğu söylenebilir. Birbirinden fark-

lı iki kavram olan dijital dönüşüm ile istihbarat yönetimini bir araya getirildiğinde ise belli kesişim alanlarına sahip oldukları görülmektedir.

Bunlar:

- Finansal istihbarat,
- Sinyal istihbaratı,
- Coğrafi konum istihbaratı,
- Ölçüm ve akustik istihbarat,
- Dijital açık kaynak istihbaratı,
- Dijital ağ istihbaratıdır.

İstihbarat yönetiminde meydana gelen dijital dönüşümle birlikte neredeyse bütün istihbarat alt alanları artık teknolojinin kullanıldığı alanlar haline gelmiştir. Teknolojinin kullanımıyla birlikte istihbarat sürecinde bazı avantaj ve dezavantajlar ortaya çıkmıştır.

Avantajlar:

- Espiyonaj gibi gizli faaliyetlere ihtiyaç azalmaktadır.
- İstihbaratın maliyeti azalmaktadır.
- Uluslararası sorun olasılığı azalmaktadır.
- Önleyicilik daha yüksek seviyede az riskle elde edilebilmektedir.

Dezavantajlar:

- Yanıltma ve dezenformasyon riski bulunmaktadır.
- Herkesin ulaşabildiği bilgide doğru analiz ve veri madencisi analistinin önemi artmaktadır.
- Hukuksal boşluk ve sorunlar oluşabilmektedir.
- İstihbarata Karşı Koyma (İKK) zorlaşmakta, sivil istihbarat analiz şirketleriyle rekabet başlamaktadır.
- Teknoloji erişimi olmayanlar göz ardı edilebilmektedir.

• Yerli teknoloji ve nitelikli eleman ihtiyacı artmaktadır.

Günümüzde istihbarat yönetimi sürecinde; sahada görevlendirilmek üzere yıllarca emek verilerek yetiştirilen ve hedef yerlere gönderilen casusların sızma yaptıklarında deşifre olmaları gibi riskler yerine açık kaynaklardan çok daha fazla istihbarat elde edilebilmektedir. Bunun yanında maliyetlerde de ciddi bir azalma meydana gelmektedir. Ayrıca dijitalleşmenin istihbarat yönetimi üzerindeki etkisiyle birlikte devletlerarasında uluslararası sorun yaşama riski azalmaktadır. Bunun yanında 'daha az risk' ile 'önleyicilik' çok daha yüksek seviyede elde edilebilmektedir.

Dijital dönüşüm istihbarat yönetimi sürecinde yukarıda sayılan avantajlar dışında bazı dezavantajlar da ortaya çıkarmaktadır. Öncelikle teknolojinin istihbarat yönetimine girmesiyle birlikte yanıltma ve dezenformasyon giderek çok daha büyük bir risk haline gelmektedir. Bu nedenle veri madencisi ve bunu doğru analiz edebilecek nitelikli insana duyulan ihtiyaç her zamankinden çok daha önemli hale gelmiştir. Ayrıca devletler bu hızlı değişim ve dönüşüm sürecinde değişime ve dönüşüme ayak uydururken bazı hukuksal boşluklar oluşabilmektedir. Buna ek olarak terör örgütlerinin çoğu internet üzerinden ya da mobil cihazlar üzerinden iz bırakmadan sadece insan istihbaratıyla ortaya çıkarılabilecek bazı hazırlıklar ve faaliyetler yürütmektedirler. Dolayısıyla illegal örgütler tarafından her şeyin dijitalleşmesine bağlı olarak bilgisayar başından istihbarat elde edebilmektedir. Bu durum gerekli önlemler alınmazsa çetrefilli ve zor bir hal yaratmaktadır. Zira tek bir fotoğraf ile birçok farklı veri elde edilebilmektedir.

İstihbarat artık açık kaynaklar marifetiyle, daha kolay bir şekilde, bilgisayar başından herkesçe elde edilebilmektedir. Bir fotoğrafa bakıldığında, o fotoğrafın neresi olduğu; fotoğraf üzerinde oynama yapılmış mı, yapılmamış mı; fotoğrafı kimin çektiği;

kimin yüklediği; ne zaman yüklediği ve mail adresine kadar her bir detayın bulunması mümkün hale gelmiştir. Bu durum bir açık istihbarat faaliyetidir. Elde edilmesi saatlerce sürecek birçok bilgiyi tek bir fotoğraftan elde etmek mümkün olmaktadır.

Profesyonel istihbarat için teknolojik donanımlar önemlidir. Örneğin ANKA-I Elektronik Harp ve İstihbarat, İnsansız Hava Aracı vb. donanımlarla düşman tarafından ya da yabancı unsurlar tarafından tamamen görünmeden her şeyi dinlemek, izlemek veya görmek mümkündür. Ancak sonuca ulaşmak için insana yine ihtiyaç duyulmaktadır.

Dijital dönüşüm güvenlik kültürünün ayrılmaz bir parçası haline gelmiştir ve nitelikli istihbarat elemanlarına duyulan ihtiyaç giderek artacaktır. Sosyal medya ve internet erişimine girmeyen kişilerin takip ve değerlendirmesi gibi hususlarda insan istihbaratı (HUMINT) önemini korumaya devam etmektedir. Dolayısıyla profesyonel insan istihbaratını göz ardı edilmemesi gerekmektedir. Dijital dünyada propaganda, algı yönetimi, dezenformasyon çok daha zahmetsiz ve daha yıkıcı gerçekleşmektedir. İstihbaratı elde etmek kolaylaşırken İKK faaliyetleri giderek zorlaşmaktadır. Dijital dönüşüm, özgürlük-güvenlik dengesinde yeni bir dönemi de beraberinde getirmektedir.

Bu noktada:

- Dijital dönüşüme paralel olarak devletlerin tehdit, risk, koruma, önleme yaklaşımlarının ve hukuksal düzenlemelerin sıklıkla gözden geçirilerek güncellenmesi gerekmektedir.
- Dijital dönüşüme adapte olmuş nitelikli istihbarat çalışanlarının akademik ve mesleki eğitimlerinin ilgili kurumlarca gerçekleştirilmesi önem taşımaktadır.
- İstihbarat yönetimi teknolojiye odaklansa da profesyonel insan istihbaratının göz ardı edilmemesi gerekmektedir.

- İstihbarat yönetimi organizasyonunun içinde etkin psikolojik harp birimlerinin teşkil edilmesi gerekmektedir.
- Sızma, casusluk gibi siber güvenlik önlemleri konusunda çözümlemelere duyulan ihtiyaç İKK faaliyetlerinin de bir parçası haline gelmelidir.
- Açık kaynak istihbaratı sayesinde proaktif güvenlik yaklaşımının reaktif güvenliği öncelemesine imkân tanınmalıdır.

Terörün Yeni Yüzü: Biyolojik Terör

Terör; eylem haline getirilmiş bir olay, terörizm ise terörün dini, siyasi veya ekonomik amaçlarına ulaşma stratejisini veya ideolojisini gerçekleştirmek için izlediği yöntemi anlatmaktadır. Terörizmin nedenleri çok çeşitlidir. Örneğin; ekonomik, psikolojik, etnik, jeopolitik ve sosyo-kültürel olabilir. Başlıca terör çeşitleri; bireysel terörizm, ulus üstü terörizm, biyolojik terörizm, narkoterörizm, devlete karşı terörizm ve küresel terörizmdir.

Biyoterörizm; kişiler, gruplar veya hükümetler tarafından ideolojik, dini, politik veya ekonomik kazanç sağlamak; insanlar, hayvanlar ve bitkiler arasında hastalığa veya ölüme sebebiyet vermek amacıyla biyolojik ajanların kasıtlı olarak kullanılması veya kullanılma tehdididir.

Biyoterörizmin temelinde yatan amaç; özelde insanların genelde ise tüm canlıların üzerinde olumsuz etkileri olan biyolojik patojenleri, biyolojik silah olarak kullanmaktır. Örneğin; II. Dünya Savaşında Japon kuvvetleri, Mançurya'da esirler üzerinde şarbon, veba ve çiçek gibi çeşitli enfeksiyon hastalıklarını deneyip ölümlere neden olmuşlardır.

Günümüzde terörist yapılar ile düzenli ordular arasında vekâlet savaşları yaşanmaktadır ve silah olarak da biyolojik ajanların kullanılması oldukça kuvvetli bir olasılıktır. Bu noktada iki

kavram önem arz etmektedir. Bunlar; biyolojik savaş ve biyolojik terör yani biyoterörizmdir. Askeri yapılanmaları hedef alan saldırılar "biyolojik savaş", sivil halkı hedef alan saldırılar ise "biyoterörizm" olarak kabul edilmektedir.

Biyolojik Savaş

Biyolojik savaş; savaş senaryolarında silah olarak biyolojik ajanların (örneğin; bakteriler, virüsler, mantarlar ve toksinler) kasıtlı kullanımını ifade eder. Biyolojik savaşlar, en küçük miktarlarda bile kullanılsa biyolojik ajana bağlı olarak kitlesel kayıplara ve/veya ölümlere neden olabileceğinden diğer geleneksel (kimyasal) silah sistemlerinden daha ölümcül olabilir.[1]

Mikroorganizmaların (veya toksinlerinin) silah olarak kasıtlı kullanımı neredeyse insanlığın kendisi kadar eskidir. Tarih öncesi ve antik Yunan ve Roma dönemlerinden beri zehirli okların kullanılması veya su kaynaklarının ve kuyuların cesetler veya kadavra ile kirlenmesi gibi örnekler bildirilmiştir. Bu erken aşamadan itibaren biyolojik silahlar savaş alanında ve gizli kullanım için özel mühimmat olarak uygun bir dağıtım sistemi ile ilişkilendirildiğinde bir kitle imha silahı olma haline gelebilmektedir. Bu tür gelişmeler hem mikrobiyoloji hem de biyoteknoloji alanlarındaki gelişmelerin doğrudan bir sonucudur.[2]

Biyolojik silahların tarihsel evrimi üç farklı döneme ayrılabilir. Bunlar:

1. Tarih öncesinden 1900'e kadar: Birkaç vaka dışında, Louis Pasteur ve Robert Koch'un mikrop hastalık teorisinin kabulüyle sonuçlanan çalışmalarının doğrudan bir sonucu olarak, biyolojik silah saldırılarının gerçek tehditler mi yoksa siyasi aldatmacaların bir parçası mı olduğu konusu tartışmalıdır ve açıklığa kavuşturmak zordur.

2. 1900'den 1945'e kadar: Bu dönem, küçük ve karmaşık olmayan ulusal biyolojik savaş programlarının (örneğin; Almanya, Japonya, Sovyetler Birliği ve Amerika Birleşik Devletleri) ortaya çıkması ve her iki Dünya Savaşı'nda biyolojik silahların kullanımından ibarettir.

3. 1945'ten sonra: Biyolojik ajanlara daha geniş erişim ve biyoteknoloji ve biyokimya alanlarında kaydedilen ilerleme, biyolojik savaş programlarının küçük gruplar ve bireyler için erişilebilir olmasını sağlamıştır. Bu dönemde genetik mühendisliğindeki gelişmeler nedeniyle biyolojik savaş ajanlarının ölümcül potansiyeli artmıştır.[3]

Hem mikrobiyologlar hem de tarihçiler için doğal salgınlar ile kasıtlı biyolojik saldırılar arasında ayrım yapmak zordur. Bunun nedenleri ise şunlardır:

1. Özellikle modern mikrobiyolojinin ortaya çıkmasından önce iddia edilen bir biyoterörizm saldırısına ilişkin güvenilir bilimsel verilerin eksikliği;

2. Mevcut belgelerin birden fazla siyasi manipülasyona açık olduğu ve dolayısıyla objektif olarak yorumlanmasının zor olduğu varsayılan herhangi bir biyolojik saldırıyı çevreleyen polemik koşullar;

3. Biyolojik saldırılarla ilgili eski raporlarla ilgili olası yanlış anlaşılmalar.[4]

Biyolojik Ajanlar

Protokoller ve hedefler açısından adli araştırmalar ile *epidemiyolojik* (sağlık verilerini toparlama) çalışmalar arasındaki farklılıkların yanı sıra, ilgili mikroorganizmaların kaynağını belirleme nedeniyle mihrak kaynaklarının araştırılması ve belirli

bir *patojenik* (hastalığa neden olan) ajanın kaza sonucu ve kasıtlı salınımı arasında ayrım yapılması gerekmektedir. Sağlık personeli; olağandışı, beklenmedik veya açıklanamayan hastalıklara karşı her an tetikte olmalıdır.

Hastalık Kontrol ve Önleme Merkezlerine göre, teşhis göstergeleri bir biyolojik ajanın kasıtlı salınmasıyla ilişkili bir bulaşıcı hastalık salgınına işaret edebilir. Bunlar arasında:

1.Halka açık etkinliğe veya toplantıya katılan kişiler veya açıklanamayan bir bulaşıcı hastalık salgınını düşündüren klinik semptomlar gösteren hastalar,

2. Yaygın hastalıklar için alışılmadık bir yaş dağılımı (örneğin, yetişkin nüfusta çocuklara özgü bir hastalıkta artış) gözlenebilmektedir.

Belirli bir biyolojik ajanın kasıtlı olarak salınması gizli veya açık bir eylem olabilir. Gizli eylem durumunda, bu sürüm günlerce hatta haftalarca fark edilmeden habersiz ve gizli kalır. Yayılmanın ilk işareti farkında olmadan başkalarına bulaşabilecek hasta bireylerin ortaya çıkmasıdır. Enfekte bir kişi muhtemelen salınım alanından uzakta tıbbi yardım arayabilir. Aksine; açık bir eylem olması durumunda ise bu durum hemen fark edilir ve hatta halka duyurulabilir. Açık eylem; yaygın bir paniğe neden olmayı amaçlamaktadır.

Patojenik ajanların biyolojik silah olarak kullanılması geleneksel silahlara (kimyasal silahlar) göre daha fazla tehdit içermektedir. Bunlar:

1. Mikroorganizmalar nispeten ucuzdur ve kolayca toplu olarak üretilebilir,

2. Büyük miktarlarda biyolojik ajan, küçük şişelerde zahmetsizce gizlenebilir ve kolayca taşınabilir,

3. Bazı ajanlar suya veya havadan taşınarak kısa bir zaman dilimi içinde geniş bir yayılma alanına neden olabilir,

4. Patojenik ajanların bazıları kişiden kişiye kolaylıkla bulaşabilir.

Biyolojik Silahların Tehdit Oluşturma Nedenleri ve Ortak Özellikleri

Biyolojik silahların çok çeşitli tehdit oluşturma nedenleri vardır. Bunlardan bazıları:

- Birçok çeşitlerinin bulunması ve yayılmalarının kolay olması,
- Kuluçka sürelerinin değişkenliği ve kuluçka dönemi süresince dağılma potansiyeli,
- Yüksek ölüm oranlarına sebebiyet vermeleri,
- Önemli *profilaktik* (hastalığı önleyici) ilaçların/aşıların raf ömrü kısalığı sebebiyle depolanma sorununun olması,
- Biyoterör saldırısı ve doğal salgın arasında hızlıca ayrım yapma zorluğudur.

Biyolojik silahların ortak özellikleri ise şu şekildedir:

- Düşük konsantrasyonlarda bile kalıcı ve giderek artan etki göstermeleri,
- Son derece bulaşıcı ve yüksek etki potansiyeline sahip olmaları,
- Kısa ve tahmin edilebilen kuluçka süresine sahip olmaları,
- Hedefteki popülasyonun ilgili mikroorganizmaya karşı bağışıklığının çok az olması ya da hiç olmaması,
- Üretim ve kullanım kolaylığı ve ucuz maliyet,
- Hedefteki popülasyon tarafından tanımlanmasının zor ve nadir olması,
- Kitleler üzerinde panik yaratması ve sağlık sisteminde çökme meydana getirme potansiyelidir.

Biyolojik Terör: Biyoterörizm

Küresel terörizm; biyoterörizm riskini arttıran ve dünya güvenliği için hızla büyüyen bir tehdittir. Biyoterörizm tehdidi sanayisi ilerlemiş ve gelişmekte olan pek çok ülkeye henüz uzak gibi görünse de; aslında biyolojik ajanları terör eylemlerinde aracı olarak kullanabilecek milletler ve muhalif gruplar mevcuttur.

Biyoterör eylemleri politik, dinsel, fikirsel veya suç nedenli olabilir, grup veya tek bir birey tarafından planlanabilir veya terörist faaliyetlerin bir parçası olabilir. Bir biyoterör saldırısının tahmin edilmesi zor olsa da, sonuçları yıkıcı olabilir. Bu nedenle güvenlik yönetimi sürecinde asla göz ardı edilmemelidir.

Bioterör saldırısında, biyolojik ajanlar kasıtlı olarak bir sivil nüfusa karşı serbest bırakılırlar. Bu yayılma paniğe, kitlesel kayıplara veya ekonomik kayba neden olmayı amaçlamaktadır.[5] Biyolojik ajanlar, doğal halleriyle kullanılabilir veya kitlesel yayılmayı arttırmak amacıyla genetik olarak modifiye edilebilirler.[6] Bir biyoterör atağı olasılığıyla karşı karşıya kalındığında ilgili ajanı tanımlamak; yalnızca popülasyonda paniği önlemek için değil, aynı zamanda ajanın yayılımı ile ilişkili morbidite (hasta sayısı) ve mortaliteyi (ölüm sayısı) kontrol etmek için de çok önemlidir.[7]

Biyolojik ajanların birçok ajandan farkı zamanla vücutta çoğalması ve etkisini gittikçe artırabilme özellikleridir. Bundan dolayı biyolojik silahlar çok yüksek derecede zarar vermektedirler. Çevre şartlarının uygunluğu; biyolojik ajanların etkilerini katlayarak arttırmalarına ve bulundukları ortamlarda da uzun süre kalıcı olmalarına sebebiyet verir.

Literatürde oldukça fazla sayıda biyolojik savaş ajanı belirtilmektedir. Potansiyel biyoterörist ajanlar ve ilişkili oldukları

durumlar bakteriler, virüsler ve toksinler olarak üç temel başlık altında toplanabilir.

Bakteriler

- Bacillus anthracis (şarbon)
- Brucella türleri (bruselloz)
- Coxiella burnetii (Q ateşi)
- Escherichia coli O157:H7 (hemolitik üremik sendrom)
- Francisella tularensis (tularaemi)
- Salmonella türleri (salmonelloz)
- Salmonella typhi (tifo ateşi)
- Shigella türleri (shigelloz)
- Vibrio kolera (kolera)
- Yersinia pestis (veba)

Virüsler

- Arenavirüsler (Junin ve Lassa ateşi)
- Ebola virüsü (Ebola virüsü hemorajik ateşi)
- Lassa virüsü (Lassa ateşi)
- Marburg virüsü (Marburg virüsü hemorajik ateşi)
- Variola major (Çiçek hastalığı)

Toksinler

- Botulinum toksini (botulizm)
- Ricinus communis kaynaklı Risin toksini

Biyoterör ve Biyogüvenlik

Biyolojik ve kimyasal ajanların toplum sağlığı için oluşturdukları tehdit bu ajanların keşfinden itibaren bilinmesine ve eski tarihlerden bu yana da savaş aracı olarak kullanılmalarına karşın, 11 Eylül 2001 saldırılarından sonra tıp çevrelerinin ve kamuoyunun yoğun ilgisini çekmiştir.

Biyoterör saldırısı olduğu düşünülen vakalarda aşağıdaki sorulara dikkat çekilmesi oluşan ve oluşabilecek krizlerin hafifletilmesi veya yok edilmesi hususlarında önemli rol oynayacaktır. Bunlar:

1.Patojenik ajan neydi?

2. Nereden geldi?

3. Doğal olarak nerede bulunur?

4. Olası iletim yolları nelerdir?

5. Herhangi bir taşıyıcı canlı var mı?

6. Hangi olası hedefler etkilenir?

7. Mikroorganizma nasıl gelişti?

8. İlgili toksinler var mı?

9. Mikroorganizmalar hangi antibiyotiklere duyarlı veya dirençlidir?

10.Mikroorganizma, virülans (hastalığa neden olma yeteneği) veya dispersiyon (dağılım) kapasitesi gibi özelliklerini geliştirmek için genetik olarak değiştirildi mi veya kimyasal olarak muamele edildi mi?

Bu sorular bilimsel ve yasal açılardan olmak üzere iki ana alana bölünebilir.

Bilimsel olarak; belirli bir patojenik ajanın kaynağının yüksek bilimsel güvenirlilik ile belirlenmesi amaçlanmaktadır. Bir biyoterör durumunda, sağlık tehlikelerini en aza indirmek için patojeni mümkün olan en kısa sürede tespit etmek çok önemlidir. Biyogüvenlik programlarının oluşturulmasıyla, yalnızca mikroorganizmaların temel konsantrasyonunu tanımlamakla kalınmaz, aynı zamanda mevsimsel dalgalanma gibi varyasyonları

da saptamak için halka açık yerler periyodik olarak izlenebilir.[8] Ayrıca, toplanan bilgiler daha iyi bir müdahale planı geliştirmek ve biyoterör saldırılarını caydırmak için uygulanabilir.

Yasal olarak ise; bir hukuk sistemi içinde tanınan ve uygulanan ilkelere göre, çıkar eylemlerinden (biyolojik savaş, biyolojik terör) kimin sorumlu olduğu veya kimin suçlandığı ile ilgili konuların belirlenmesi amaçlanmaktadır.[9]

Suçlular ve teröristler genellikle biyolojik ajanları (virüs, bakteri, toksin) geleneksel silahlara göre daha çekici bulur ve alternatif olarak görürler. Çünkü biyolojik silah üretimi nispeten düşük maliyetlidir, mikroorganizmalara kolayca erişilebilir, üretilmesi, modifiye edilmesi ve salınması basit olabilir. Ayrıca bunların küresel yayılımında bireyler arasında korku, panik ve depresyona neden olabilir.

Biyolojik bir silahın serbest bırakılması, hastalıklara ve hatta ölüme neden olmayı amaçlar. Genellikle bunlar doğal olarak oluşan mikroorganizmalardır. Ancak bazen hastalığa neden olma veya bilinen terapötik yani tedavi edici yaklaşımlara direnme yetenekleri laboratuvar ortamında arttırılarak zararlı olacak şekilde tasarlanabilirler.

Bu bağlamda; kullanılan biyolojik ajan(lar)ın güvenilir bir biyolojik ajanın salınması ve yayılmasına zamanında ve etkili bir cevap verilmesi için kriz durumunda plan yapmak oldukça önemlidir.

Daha az çalışılmış biyolojik ajanları karakterize etmek için yapılan araştırmaların yanı sıra, önceden bilinen biyolojik ajan verilerine erişim oldukça önemlidir. O halde her an olası bir tehlike olarak değerlendirilen biyoterörizm faaliyetlerinde güvenlik nasıl sağlanmalıdır?

Biyogüvenlik olarak tanımlanan bu kavram modern biyolojik teknikler ve uygulamalar ile biyolojik çeşitlilik üzerinde oluşturabileceği olumsuz etkilerin belirlenmesi ve risk yönetim süreçlerini kapsamaktadır. Daha uzun vadeli çözümler için, tıp camiası hem halkı hem de politikacıları biyoterörizm hakkında bilgilendirmeli ve kullanımını kınayan küresel bir fikir birliği oluşturmalıdır.

Sonuç olarak; olası biyoterörizm tehditlerine karşı gerekli tedbirlerin alınması önem arz etmektedir. Bu yüzden birtakım anahtar mesajlara değinilmesi uygun olacaktır. Bunlar;

- Kasıtlı olarak oluşturulabilecek biyoterör salgınlarına hazırlıklı olmak, doğal salgınlara verilecek cevabı da güçlendirecektir.
- Meydana gelen salgınlar üst düzey liderlik, sorumluluk ve yetki ile sürdürülmelidir.
- Sağlık hizmeti sektörü; biyoterörizm potansiyeli ve bilinmeyen patojenlerin varlığını göz önünde bulundurup, biyolojik ajanlara olan farkındalığı sürdürmelidir.
- Acil servis ve toplum hekimleri potansiyel biyoterörist ajanların neden olduğu hastalıkların klinik belirtileri ve ortaya çıkan bulaşıcı hastalıklar hakkında düzenli olarak güncellenmelidir.
- Kişisel koruyucu donanımlar geliştirilerek halkın kullanımına sunulmalıdır.
- Ciddi, bulaşıcı hastalığı olan hastalarda ani ve büyük artış durumları için sağlık sistemini bu sorunlarla başa çıkmak için hızla revize etme yeteneği geliştirilmelidir.
- Daha hızlı, daha güvenilir tanı testleri geliştirmek için genel ve özel laboratuvarların kapasitesi artırılmalıdır.
- Yeni ve geliştirilmiş aşılar ve tedavi rejimleri geliştirilmelidir.

- Klinik ve çevresel sürveyansın (hastalığın kontrol altına alınması) artması gerekmektedir.
- Sendromik sürveyans sistemleri (belirli hastalıkların nasıl ortaya çıktığı ve dağıldığına ilişkin sistematik olarak yapılan gözlem sistemleri) geliştirilerek doktorlar tarafından bildirilen vakalar bir salgının ilerlemesini izlemek için kullanılabilmelidir.
- Hem ulusal hem de uluslararası bağlamda yeterli miktarda aşı ve ilaç stoğu bulundurulmalıdır.
- Doğal ve biyoterörist salgınlara karşı hazırlığı geliştirmek için, uluslararası işbirliği, birden fazla ülkeyi içeren ortak tatbikatlar ve potansiyel biyoterörizm tehditleri hakkında bilgi alışverişinde iyileştirme ve yönetim sistemleri kurulmalıdır.

21. YÜZYILDA GÜVENLİK YÖNETİMİNE İLİŞKİN TESPİTLER, SORUNLAR VE ÇÖZÜM ÖNERİLERİ

Soğuk savaş sonrasında dünyanın iki kutuplu sistemden çok kutuplu bir yapıya evirlmesi sonucu devlet merkezli, askeri güç odaklı bakış açısı sorgulanmaya başlanmıştır. Küresel güvenlik tehditlerinin, bir ülkenin tek başına üstesinden gelemeyecek boyutlara ulaşmasıyla sosyal, çevresel ve kültürel konular da uluslararası güvenliğin gündemine girmiştir. Soğuk Savaş'ın bitimiyle risk ve tehditlerin belirli bir coğrafyadan gelmesi anlayışı; yerini belirsiz, tek merkezden yönetilmeyen ve sınırı aşan tehditlerin varlığına bırakmıştır. Teknolojinin hızla gelişmesiyle siyasal ve sosyal alanda meydana gelen değişim askeri alanda da kendini göstermiştir. Bu değişimle birlikte savaşların çehresi de değişmiştir. Gayrı nizami harp teknikleri kullanılmaya başlanmış ve dördüncü nesil savaşlarda sivil asker ayrımı ortadan kalkmıştır.

Bu bölümde yeni güvenlik tehditleri ve güvenlikle ilgili yeni yaklaşımlar ele alınmaktadır. Akabinde ise kırılgan devletler ve güvenlik açmazlarını ortaya çıkartan nedenler incelenmekte, düzensiz göç ve ortaya çıkan sorunlar noktasında değerlendirmelere yer verilmektedir. Nihai olarak ise değişen şartlar çerçevesinde ortaya çıkan sorunlara ve çözüm önerilerine ilişkin değerlendirmeler yapılmaktadır.

Yeni Güvenlik Tehditleri

Kamu Güvenliğine İlişkin Sorunlar

Günümüzde ve yakın gelecekte kamu güvenliğini tehdit edecek unsurları dört başlıkta toplamak mümkündür:

- İnsan Kaynaklı Tehditler: Terör, suç, salgın hastalıklar vb.
- Kaynak Gereksiniminden Doğan Tehditler: Yiyecek, su, tıbbi malzeme vb.
- Çevresel Tehditler: Sel, deprem, iklim değişikliği vb.
- Dijital Tehditler: Siber suçlar, kritik altyapılara düzenlenen saldırılar.

Sovyetler Birliği'nin çöküşü ve Soğuk Savaş'ın sona ermesiyle birlikte küresel sorunlar ve tehditler ciddi anlamda artmıştır. Terör, suç ve salgın hastalıklar gibi insan kaynaklı tehditler yanında yoksulluk, gıda kıtlığı, suya erişim, hastalıkların tedavisine yönelik yeterli tıbbi malzemelerin bulunmaması gibi sorunlar başta geri kalmış ülkeler ve kırılgan devletler olmak üzere gittikçe yaygınlaşmaktadır. Yükselen enerji fiyatları ve gıda maliyetlerindeki astronomik artış, yoksul ülkelerde ayaklanmalara ve acil gıda ihtiyaçlarına yol açabilmektedir. Ayrıca küresel ısınma, ekolojik sorunlar gibi çevresel faktörler de kamu güvenliği için ciddi tehdit unsuru oluşturmaktadır. İklim değişikliği; tarımsal uygulamalarda ve tedarik zincirinde aksamalara, insan hayatına mal olabilen afetlere neden olabilmektedir. Doğal kaynakların tükenmeye başlaması ve iklim değişikliklerinin önlenememesi durumunda göçlerin artacağı ve bunun ciddi bir güvenlik tehdidi olacağı ifade edilmektedir. Siber suçlar ve kritik alt yapılara düzenlenen saldırılar da dijital güvenlik açısından önemli bir sorun oluşturmaktadır. Dijital mecraların hayatın her alanına daha fazla nüfuz etmesine bağlı olarak siber suçlar için yeni kapılar açılmıştır. Birleşik Krallık Ulusal Suç Dairesi'nin belirttiğine göre günümüzde siber suç hacmi, fiziksel suç hacmini geçmiştir.

Kamu güvenliğine ilişkin sorunlar içerisinde terör meselesine ayrıca yer vermek gerekmektedir. Nitekim terör kamu güvenliğine yönelik en kadim tehditlerden birisidir. Terör yeni nesil savaş (YNS) kapsamında da üzerinde durulan bir kavram olmakla

birlikte içinde bulunduğumuz süreçte terörün de yüzü değişmeye başlamıştır. Terör, YNS'de kullanılan bir taktik, vekâlet savaşlarının bir aracı olarak karşımıza çıkmaktadır.

Kamu Güvenliği ve Terörün Yeni Nesil Savaş Üzerine İncelenmesi

Savaşın 'Yeni Nesli', 1980'li yılların sonu ve 1990'lı yılların başından itibaren gündeme gelmiş, 11 Eylül saldırılarından sonra ise üzerinde daha sık durulmaya başlanmıştır. Aralarında küçük farklılıkları olsa da literatürde *Yeni Nesil Savaş* (YNS) ile benzer anlamda kullanılan bazı kavramlar bulunmaktadır: Yeni Savaş, 4. Nesil Savaş, Hibrit Savaş, Asimetrik Savaş, Vekalet Savaşları gibi.

Savaşın doğasında zaman içinde değişim yaşanmış ve bu değişim 1. Nesil savaşlardan başlamak üzere dört dönemde incelenmiştir. 1. nesil savaş dönemi 1648 yılında 30 Yıl Savaşları'nın sona ermesinden başlayarak 1. Dünya Savaşı'na kadar olan dönemi kapsamaktadır. 1. nesil savaşın karakteristik özellikleri kitlesel insan gücü kullanımıdır. Dönemin silahları ise ağızdan doldurmalı yivsiz tüfek ve ağızdan doldurmalı sahra topları olarak karşımıza çıkmaktadır. Düz bir alanda orduların karşı karşıya geldiği, galibi net bir şekilde belli olan savaşlardır. 2. nesil savaşlar ise 1914-1940 tarihleri arasında görülen sanayiinin gelişmesine bağlı olarak silah, ulaşım ve lojistik malzemelerinin çeşitlendiği savaşlardır. Makineli tüfek, uçak, buharlı deniz gücü, uzun menzilli toplar, demiryolu sayesinde hızlı sevkiyat 2. nesil savaşların genel özellikleridir. Bu dönemde telgraf, telefon gibi yeni haberleşme araçları da savaşların gidişatına etki eden faktörler olmuştur. 3. nesil savaş noktasında 2. Dünya Savaşı sonrası tanklarla desteklenen makineli piyade unsurları ve artan manevra kabiliyeti ön plana çıkmıştır. Nazi Almanya'sının fırtı-

na teknikleri kullanması da bu dönemdedir. Gayrinizami savaş teknikleri kullanılması 1990'ların sonuna kadar devam edecek dönemin karakteristik özelliğidir. 4. nesil ya da yeni nesil savaş dönemi ise Soğuk Savaş'ın sona ermesi, küreselleşme ve gelişen teknoloji çerçevesinde şekillenmiştir. Devlet otoritesini zayıflatmaya yönelik olan yeni dönem savaşta sivil-asker ayrımı kalmamış, savaş-barış kavramları muğlaklaşmış ve savaş araçları değişmiştir.

Hibrit savaş; askeri ve toplumsal düzeyde düzenli veya düzensiz tekniklerin son teknolojiyle birlikte kullanılmasıyla ortaya çıkan savaştır. Geleneksel ve konvansiyonel metotlar dışında bütün yöntemler kullanılmaktadır. Titiz bir plan gerektirmektedir ve sürekli bir saldırı öngörmektedir. Kısa vadede sonuç alınması beklenmemektedir. Zayıf devletlerin güçlü devletlere karşı gayri nizami harp metotları kullanması şeklinde ortaya çıkmaktadır.

Vekâlet savaşları da direk olarak bir devletin diğer devlete karşı kaynak sağlayarak yürüttüğü savaştır. Vekâlet savaşlarının çıkışını tetikleyen birinci neden konvansiyonel savaşların artan maliyeti, ikincisi ise devletlerin uluslararası hukukta sorumluluk almak istememesidir. Vekâlet savaşı örneği olarak PKK/PYD'nin farklı devletler tarafından kullanılmasıyla yürütülen savaşlar gösterilebilir.

Yeni nesil savaşları ortaya çıkaran koşullar şunlardır:

- İki kutuplu dünya düzeninin sona ermesi,
- Konvansiyonel savaşların artan maliyeti,
- Üçüncü dünya ülkelerindeki kötüleşen yaşam standartları ve gelir eşitsizlikleri,
- Uyuşturucu kaçakçılığı ve buna bağlı para akışı ve yolsuzluklardaki patlama,
- Genişleyen iletişim ve ulaşım ağları,

- İklim değişikliği,
- Dünya nüfusundaki sürekli artış,
- Ekilebilir arazi ve su kıtlığının artması,
- Ortaya çıkmasında insan faktörünün de rol oynadığı salgın hastalıklar olarak sıralanabilir.

Yeni nesil savaşın amacı; rakip gücün siyasi yönetimi ile kamu bürokrasisi arasındaki uyumu bozmak, siyasi iradede çalkantılar oluşturarak kargaşa meydana getirmek, çatışma alanını karşı tarafın en zayıf ve en çok kayıp vereceği alanda belirlemek ve nihayetinde devletin meşruiyetini tartışılır hale getirmektir.

Yeni nesil savaşta devlet, savaştaki tekelini kaybetmiştir. Savaşın finansörü değişmiş, zafer olgusu belirsizleşmiş, sivil ve askeri alan arasındaki ayrım ortadan kalkmıştır. Kullanılan silahların ve savaşın hedef kitlesinin değiştiği yeni nesil savaşta meydana gelebilecek tahribatı tahmin etmek de güçleşmiştir. Yeni nesil savaş belli bir şekli olmayan ve sürekli değişen tehditleri ifade etmektedir. Siber saldırılar, istihbarat, teknolojinin gelişmesi yeni nesil savaşların ana unsurlarını teşkil etmektedir. Amerikalı uluslararası güvenlik uzmanı Stephen Blank, 21.yüzyılda kamu güvenliğini tehdit edici unsurların sistemik, yani kamu güvenliğini tek bir açıdan değil, birden fazla açıdan tehdit eden unsurlar olduğunu dile getirmiştir.

YNS ile terör aynı şey değildir ve amaç, strateji, hedef ve taktik anlamında aralarında önemli farklılıklar bulunmaktadır. YNS'de temel amaç düşmanın askeri varlığını tamamen yok etmek yerine geniş çaplı etkisi olabilecek ahlaki gücünü hedef alarak düşmanı tahakküm altına almaktır. Terörün amacı ise güvensizlik duygusu ortaya çıkararak hedef kitlenin iradesini etkilemektir. YNS, strateji olarak düşmana yönelik kademeli yıpratma, ekonomik maliyetlerini artırma, psikolojik operasyonlar

yapma, propaganda ve diplomasiyi de kullanarak çeşitli yöntemlerle düşmanı askerî açıdan etkisiz hale getirme yoluna gider. Terörün stratejisi ise hedef kitleyi etkilemek için beklenmedik, orantısız ve ölümcül güç kullanarak sürpriz saldırılar yapmaktır. Taktik olarak YNS, düzensiz ancak uzun süreli vur-kaç saldırıları yapmayı, terörü, insan hakları ihlali iddialarını, iletişim ve dijital platformlara yönelik saldırıları ve bunların kesintiye uğratılmasını kullanır. Terörün kullandığı taktik ise bombalı saldırılar, intihar saldırıları, zulüm ve tecavüz, adam kaçırma ve infaz etme olarak özetlenebilir.

YNS, hedefin veya ittifakın uyumunu bozmak için diplomasi (askeri hizmet anlaşmazlıkları), doğrudan eylem (devlet dışı aktör/vekil aracılığıyla terörizm), kültürel savaş, uyuşturucu kaçakçılığı, çok kimlikli toplumlarda din ve etnik köken temelinde bölünme meydana getirme, ekonomik savaş (dijital ağa saldırı, serbest ticaret dolaşımını yavaşlatma, verimli çalışma sürelerinin kaybına sebep olma) gibi yöntemleri kullanır. Terörün kullandığı yegâne yöntem ise orantısız güç kullanarak ölümcül eylemlerle korku ve güvensizlik ortamı yaratmaktır. Sonuç olarak YNS doğrusal olmayan bir savaştır ve YNS stratejisinde 1+1 her zaman 2 etmeyebilir. Çünkü alanlar belli değildir ve çok uzun dönemli stratejilerle yürütülen bir savaştır. Bunun için de çok fazla yetişmiş insan kaynağı gerektirmektedir ve düşünce kuruluşları bu bağlamda çok önemli bir role sahiptir. YNS'de savaşın merkezi doğrudan kamu (halk) haline gelmiştir. YNS; diplomatik, siyasi, ekonomik ve toplumsal saldırı girişimlerini destekleyen bir savaştır. Rakip tarafın istikrarsızlığına odaklanmaktadır ve düşman ülkenin içten çöküşünü amaçlamaktadır.

YNS ortamında kamu güvenliğine yönelik tehditler de değişmiştir. Sadece askeri değil toplumsal kargaşaya neden ola-

bilmek için farklı gruplar da hedef alınmaktadır. Savaş silahlı eylem, yağma, hırsızlık gibi dar bir eksenden; doğal kaynakların azalması, göç, iklim değişikliği, salgın hastalık, siber saldırı gibi geniş bir eksene kaymıştır. Bu nedenle YNS askeri hedefleri yok etmeyi amaçlamaz, toplumun moralini etkileme, ekonomik sisteme zarar verme, kaynaklara erişimi engelleme veya ortak olma gibi amaçlar da barındırmaktadır.

YNS ile mücadele konusunda özellikle siber saldırılara karşı ülkelerin nitelikli eleman ihtiyacına öncelik vermesi gerekmektedir. 2021 yılında dünya genelinde yeri boş kalmış yaklaşık 3,5 milyon nitelikli siber güvenlik elemanı ihtiyacı olacağı belirtilmektedir. Dijital çağın vatandaşlarının görev ve sorumlulukları konusunda toplum bilgilendirilmelidir. Geleceğin kamu görevlilerinin dijital okuryazarlık becerisine sahip olmalarına özen gösterilmelidir. YNS ile etkin mücadele adına ortaya çıkan farklı tehditler için alınması gereken önlemler ile ilgili birtakım öneriler de sunmak mümkündür. İklim değişikliğinden kaynaklanan tehditler için öncelikle önemli ekosistemler korunmalı ve yeniden canlandırılmalıdır. Yenilenebilir enerji teşvik edilmeli, devletler, yerel emisyon hedefleri belirleyerek hava kirliliğinin nedenlerini azaltmalı ve iklim değişikliği nedeniyle ortaya çıkabilecek tehditler konusunda kamuoyu bilinçlendirilmelidir.

YNS'de terör ile mücadelede strateji değişikliğine gidilmelidir. Dar bir cephe ile sınırlı, bir dizi davranışa odaklanan, durağan, uyum sağlama ve öğrenme yeteneğinden yoksun stratejiler terk edilmelidir. Bunun yerine basit ve esnek planların, olasılıkların göz önünde bulundurulduğu, alternatif olarak birden fazla seçeneğin olduğu, riskten korunmaya yönelik stratejiler içeren ve müşterek bakış açısına dayanan stratejiler takip edilmelidir. Yine terörle mücadele konusunda uluslararası işbirliği geliştiril-

melidir. Etkili mücadele için merkezi devlet otoritesinin demokratik çerçeve içerisinde etkin kullanımı gerektiğinden ordu ve diğer güvenlik bürokrasisi, YNS ortamında farklı enstrümanlara sahip terörle mücadele konusunda bilinçlendirilmelidir. Terörün başlıca hedefi olan halka, tehdidin doğası, potansiyel maliyeti, terörle mücadele hakkında gerekli bilgi verilmeli ve bu mücadelenin önemi anlatılmalıdır.

Korona Virüs Sonrası Dönemde Güvenlik Paradigmasındaki Değişim

İnsanoğlu dünyada var olmaya başladığı günden itibaren birçok risk, tehdit ve tehlike ile karşı karşıya kalmıştır. Bunlardan bir tanesi de salgın hastalıklar olmuştur. İspanyol gribi örneğinde görüldüğü gibi bir salgın hastalık nedeniyle ölenlerin sayısı 1. Dünya Savaşı'nda ölenlerden daha fazla olabilmektedir. Nitekim, dünyanın 21. Yüzyılda karşı karşıya kaldığı ve milyonlarca insanın hayatını kaybettiği salgın hastalıklardan birisi de Kovid-19'dur. Bu nedenle yeni dünya düzeninde korona virüs pandemisini de göz önünde bulunduran güvenlik paradigmasının kodlarına bakmak yerinde olacaktır.

Küresel bir salgın olan korona virüs milyonlarca insanın hayatını olumsuz yönde etkilemiştir. Bir bütün olarak toplum ve iş dünyası üzerinde olağanüstü bir etkisi olmasının yanı sıra güvenlik ile ilgili birtakım hususlar da ortaya çıkarmıştır. Salgın nedeniyle toplum genelinde endişe artmış, teknoloji kullanımının yaygınlaşmasına bağlı olarak dijital suçlar ivme kazanmış ve siber saldırıların sayısında ve kapsamında artış görülmüştür. Dijital mecraların kullanılmasıyla korona virüs döneminde devlet destekli organize grupların kaos ortamından beslenerek çeşitli içerik, doküman, haber ve uygulamalarla siber saldırılar gerçekleştirdiği görülmektedir.

Korona virüsün getirdiği güvenlikle ilgili bu sorunlar yalnızca iç güvenliği etkilememiş, dış güvenliğe ilişkin de yansımalar barındırmıştır. Virüs özellikle Afganistan, Suriye, Libya, Yemen ve Afrika'daki sıcak çatışmaların yaşandığı bölgeleri ve çatışma süreçlerini oldukça etkilemiştir Nitekim arka planında farklı süreçler olmakla birlikte, ABD'nin Afganistan ve bazı diğer bölgelerden askerini çekmesini ya da bu süreci hızlandırmasını salgının çıktılarından birisi olarak değerlendirmek mümkündür.

Korona virüsün yayılması kapsamında alınan önlemlerin başında sınırların kapatılması gelmiştir. Bu minvalde karantina bölgeleri oluşturulmuştur. Sokağa çıkma yasakları hayata geçirilerek virüsün yayılımının kontrol altına alınması amaçlanmıştır. Alınan önlemlerin uygulanmasıyla ilgili kolluk birimlerince gerçekleştirilen faaliyetler virüsün kontrolünde güvenliğin ve güvenlik birimlerinin önemini bir kez daha ortaya koymuştur. Özellikle Türkiye'de kolluk birimleri geleneksel görevlerini yerine getirmeye ek olarak sosyal devlet faaliyetlerinin yürütülmesinde de etkili bir aktör olmuştur.

Salgın, doğal afet ve savaş gibi krizler insanları korku ve panik halinde hareket ettirerek toplumsal güvenliği zedeleyebilmektedir. Bu dönemlerde işyerlerini yağmalamaya yönelik faaliyetlerin engellenmesi ve halkın kriz sürecini güven içinde atlatması noktasında güvenlik ve güvenlik kuvvetlerinin önemi üzerinde durulması gereken bir konudur. ABD'de yaşanan market yağmalama olayları, temizlik ürünleri savaşları bu durumu ortaya koymaktadır. Virüs ile birlikte yaşanan kriz ortamında iç güvenliğin yeterince sağlanamaması iç çatışmalara neden olabilmektedir. Bu durum toplumdaki huzursuzluğun artmasına,

hükümet karşıtı gösterilere ve hükümet krizlerine de sebep olabilmektedir. Almanya, Fransa, Hollanda ve Sırbistan'da bunun örnekleri yaşanmıştır.

Peki salgın ülkelerin jeopolitik çıkarlarını ve dış politika hedeflerini değiştirmiş midir? Bu soruya yanıt ararken, gerçekliğin böyle olup olmadığı ya da ülkelerin önceliklerinin tamamen değişip değişmediğinin tespit edilebilmesi için bazı gelişmelere bakmakta yarar vardır. ABD'nin 1929 krizinden daha büyük bir krizi yönetirken bir taraftan İran ile Arap Denizi'nde askeri mücadeleye devam ediyor olması, bunun yanında Avrupa'nın güvenliği için oluşturulmuş NATO, üye ülkelerin çoğunda sokağa çıkma yasağına varan tedbirler alınmış olmasına rağmen, tatbikatlarına devam etmiştir ve bu da aslında örgütün dış politika hedeflerinden çok da vazgeçilmediğini göstermektedir. Son zamanlarda askeri gücün iç güvenliğe kaydırılması gibi bir görüş yaygınlaşsa da ülkelerin jeopolitik önceliklerini değiştirmediği görülmektedir. Özellikle salgınla mücadelenin jeopolitik mücadelenin önüne geçmeyeceğini belirtmek gerekmektedir. Bütün devletler 'güvenli devlet' olma misyonuyla hareket etmektedir.

Yeni dönemde uluslararası toplum tarafından terk edilmiş olma düşüncesi birçok ülkeyi içe kapanmaya yöneltmiştir. Bu durum ne yazık ki ırkçılık, yabancı karşıtlığı ve İslam düşmanlığı gibi toplumsal marazlara ivme kazandırmıştır. Terör örgütleri salgının bazı ülkelerde ortaya çıkardığı otorite boşluklarından istifade ile yeni palazlanma süreçlerine girişmektedir. Özellikle aşırı sağcı yapılar salgının ortaya çıkardığı ekonomik zorlukları bahane ederek kendilerine zemin oluşturmaya çalışmaktadır.

Geldiğimiz aşamada hepimiz güvende kalana kadar hiçbirimizin güvende olmadığı anlaşılmıştır. Hiçbir ülkenin günümüzde güvenlik meselelerine coğrafi uzaklık/yakınlık merceğinden

bakma lüksü kalmamıştır. Zira artık dünya küresel bir köye dönüşmüş, mesafeler anlamını yitirmiştir. Gelişen ulaşım ve iletişim imkanları insanları ve ülkeleri hiç olmadığı kadar birbirine yaklaştırmıştır. Bu durum, insanlığın ortak sorunlarına çözümler üretebilmek için iş birliğini mecbur kılmaktadır.

Kırılgan Devletler ve Güvenlik Açmazları

Devletin toprakları üzerinde egemenliğini veya meşruiyetini sağlamada yetersiz kaldığı, zayıf devlet kapasitesi ile karakterize edilen devletlere kırılgan devlet olarak adlandırılmaktadır. Kırılgan devletler ve neden oldukları güvenlik açmazlarını izah etmek için bir örnek olay üzerinden konun ele alınması tercih edildiğinde Suriye örnek olarak seçilebilir. Çünkü Suriye kırılgan devlet olmak için gerekli bütün kriterleri sağlamaktadır.

Kırılgan devlet tanımlamasına bakıldığında belli kriterlerin var olduğu görülmektedir:

- Devletin meşru güç kullanma tekelinin farklı yapılar tarafından kullanılıyor olması,
- Bir devletin kendi ülkesinin her yerinde egemenlik tesis edememiş olması kırılgan devletlerin güvenlik açmazı oluşturan başlıca özellikleridir.

Bu iki kriter 2011 sonrasında ortaya çıkmıştır. 2011 öncesinde Suriye'de bu iki kriter tam olarak görülmese de kırılgan devlet özelliklerinin çoğunu içeren bir durum söz konusudur. Bu özellikler şöyle sıralanabilecektir:

- Yozlaşma ve yolsuzluğun yaygın olması,
- Siyasal katılımın olmaması, halkın büyük çoğunluğunun yönetimden dışlanmış olması, bu anlamda eşitsizliğin var olması,
- Halk ile devlet arasında makasın giderek açılması, halkın

devlete yabancılaşması ve giderek devletin halk nezdindeki meşruiyetini yitirmesi,
- Silah kaçakçılığı, uyuşturucu kaçakçılığı, savaş ekonomisinin yaygınlaşması ve kitlesel insan hakları ihlallerinin yaşanması.

Görüldüğü gibi güç kullanma tekelinin devlet dışında yapılar tarafından kullanılması ve egemenliğin tesis edilememesi kriterleri henüz ortaya çıkmamış olmasına rağmen 2011 öncesinde de Suriye'de kırılgan devletin şartlarının pek çoğu ortaya çıkmıştır. 1970 yılında Hafız Esad'ın iktidara gelmesiyle başlayan dönemden itibaren üniter bir yapı ve güçlü bir merkezi yönetimin var olduğu görülmüştür. Bu dönemde güç kullanma tekeli tamamen devlete ait olmuştur ve ülkenin her yerinde egemenlik tesis edilebilmiştir. 2011 sonrasında bu iki kriter açısından da Suriye'de kritik bir değişim yaşanmıştır. Devlet, güç kullanma tekelini ve ülkenin her yerindeki egemenliğini yavaş yavaş kaybetmeye başlamıştır. Bu durumun sonucu olarak güvenlik problemleri ortaya çıkmıştır. Sadece ülke içinde güvenlik problemleri doğmakla kalmamış, bu problemler başta komşu ülkeler olmak üzere yayılma etkisi göstermeye başlamıştır. Klasik egemenlik anlayışı aşınmaya başlamış ve içişlerine karışmama ilkesinin aşınmasını da beraberinde getirmiştir. Sonuçta bölgesel ve bölge dışı aktörlerin Suriye üzerindeki etkileri artmaya başlamıştır.

Güvenlik problemleri açısından bakıldığında ise Suriye'de ilk olarak merkezi gücün zayıflamasına paralel olarak alternatif silahlı grupların ortaya çıktığına şahit olunmuştur. Milisleşme, buna bağlı olarak iç savaşın ortaya çıkması, birbirine rakip olan silahlı grupların çatışmaya girmesi görülmüştür. Milisleşme derken hem rejim taraftarı hem de rejim aleyhtarı gruplar kastedilmektedir. Suriye ulusal ordusunun zayıflaması, parçalanması, güçsüzleşmesi, daha fazla dış desteğe ihtiyaç duyması ile birlikte

özellikle İran ve Rusya'nın desteği ile birlikte milis grupların rejim safında Suriye iç savaşına dâhil olduğu görülmüştür. Bunlar kontrol dışı, merkezi bir otoritenin denetimden muaf, kendi yerel çıkarlarını güden gruplardır ve bu durum güvenlik sıkıntılarını derinleştiren bir faktör olmuştur. Milisleşme muhalif kanatta da ortaya çıkmıştır. Özgür Suriye Ordusu adı altında birbirinden farklı ideolojilerle hareket eden, farklı coğrafi bölgelerde yer alan ve aşiret ilişkilerine sahip gruplar örgütlenmeye başlamış ve rejime karşı mücadele etmeye girişmiştir. Bu durum Suriye'de farklı silahlı grupların sayı ve güç bakımından büyümesine yol açmıştır.

İkinci güvenlik problemi terör örgütlerinin yükselişidir. Kırılgan devletler, terör örgütleri için hem bir üreme hem de barınma alanı oluşturmaktadır. Bunun örnekleri tarihte de görülmekle birlikte Suriye çarpıcı bir örnek teşkil etmektedir. Merkezi otorite zayıfladıkça PKK'nın Suriye kolu olan YPG/PYD'nin, DEAŞ'in, El-Kaide türevi olan örgütlerin Suriye'de giderek zemin kazandığını hatta belki Suriye'de daha önce görülmemiş biçimde alan kontrolü üzerinden egemenlik iddiasında bulunduğu görülmüştür. Sözde hilafet devleti ya da PKK'nın ilan ettiği sözde kantonlar ile tek taraflı egemenlik iddialarına tanık olunmuştur. DEAŞ her ne kadar alan hakimiyetini yitirse de halen önemli bir güvenlik tehdidi oluşturmaktadır. YPG/PKK başta Türkiye olmak üzere bütün bölge için güvenlik riski oluşturmaya devam etmektedir. El-Kaide türevi örgütlerin TSK mensuplarına yönelik saldırılarından da görüldüğü üzere bölge için hala güvenlik tehdididir.

Üçüncü güvenlik sorunu sınırların kontrol edilememesidir. Sınırların kontrol edilemeyişinin iki etkisi olmaktadır. Bunlardan ilki kitlesel göç hareketlerinin yaşanmasıdır. Kitlesel göç

hareketleri sınır ötesine doğru yönelmektedir. İkincisi ise terör örgütleri de dâhil olmak üzere silahlı grupların sınır hattını kullanarak kolay sınır geçişleri gerçekleşmektedir. Bu geçişler sınırı olan ülkeler için önemli güvenlik riskleri doğurmaktadır. Bu durumun en somut örneklerinden birisi YPG'nin Türkiye'ye yönelik terör eylemleri diğeri ise DEAŞ'ın Fırat Kalkanı Harekâtı öncesinde başta sınır illeri ve büyükşehirler olmak üzere düzenlediği terör eylemleridir.

Kırılgan devletlerdeki iç savaşlar ve yaşanan büyük krizler ülke ile sınırlı kalmamakta ve yayılma etkisi göstermektedir. Yayılma etkisini belirleyen birkaç faktör bulunmaktadır:

- Krizin yaşandığı ülke ile sahip olunan sınırın uzunluğu,
- Krizin yaşandığı ülke ile yayılma riski olan ülke arasında etnik ve mezhepsel bağların olup olmaması,
- Ülkeye göç eden mülteci sayısı,
- İç savaşın yaşandığı ülkede çatışan tarafların merkezi otoriteyi yıkmak amacıyla mı yoksa ayrılıkçı bir ideolojiyle mi hareket ettiği: Suriye'de her iki örnek de mevcuttur. Suriyeli muhalifler açısından baktığımızda; rejimi, merkezi otoriteyi yıkmaya dönük bir hareket görülmektedir. PKK/YPG örneğine bakıldığında ise ayrılıkçı bir amaç söz konusudur.
- Komşu ülkenin büyüklüğü ve devletin kapasitesi: Ekonomisi zayıf olan küçük ülkelerin yayılma sonucunda daha fazla etkilendiği görülmektedir. Örneğin, Türkiye'nin kurumlarının kapasitesi, coğrafyası, ekonomik gücü krizin Lübnan gibi ülkelere göre daha kolay atlatılmasını sağlayabilmektedir.

Düzensiz Göç, Göçmen Kaçakçılığı ve İnsan Ticareti

Dünyadaki uluslararası göçmenlerin toplam sayısı 281 milyon civarındadır.[10] Uluslararası göçmenler dünya nüfusunun %3.6'sını oluşturmaktadır.[11] Birleşmiş Milletler Mülteciler Yüksek Komiserliğine göre dünyada yerinden edilenlerin sayısı da 84 milyonu aşmıştır. Rakamlar 2. Dünya Savaşı'ndan bu yana en yüksek seviyeye ulaşmış olup; göçün küresel olarak ele alınması gereken bir konu haline geldiğini göstermektedir.

Düzensiz Göç

İnsan hareketliliğinin büyük bir kısmı düzensiz göç akımları şeklinde gerçekleşmektedir. 21. Yüzyılda iyice tesirini artıran küreselleşme sürecinin etkisi ve buna bağlı olarak sosyal medya kullanımının yaygınlaşması, ulaşım ve iletişim araçlarının çeşitlenmesi gibi hususlar hem düzenli hem de düzensiz insan hareketliliği artmaktadır.

Düzensiz göç; yasal olmayan yollardan ülkeye girmeyi, yasal olarak girip yasal olmayan biçimde kalmayı, yasa dışı yollardan ülkeden çıkmayı ya da teşebbüs etmeyi ve yasadışı çalışmayı ifade etmektedir. Düzensiz göç akımları ülkeleri sosyo-ekonomik ve güvenlik açısından derinden sarsan, hükümetleri zor durumda bırakan, şehirlerin demografik yapılarını değiştiren, terörü ve organize suç örgütlerini besleyen bir tehdit haline gelmiştir.

Düzensiz göçün ortaya çıkardığı ekonomik tehditler kayıt dışı ekonomi, vergi kaybı, istihdamda azalma, mücadele finansmanı ve sınır dışı masrafları olarak karşımıza çıkmaktadır. Düzensiz göçün kriminal açıdan doğurduğu tehditler ise terörizme kanal açılması, gasp, hırsızlık, fuhuş, yağma, uyuşturucu ticareti ve göçmen kaçakçılığı suçları olmaktadır. Toplumsal çatışma,

gettolaşma, bulaşıcı hastalık ve güvensizlik ortamı ise düzensiz göç kaynaklı toplumsal tehditlerdir.

Dünya üzerindeki düzensiz göç yollarına bakıldığında Meksika'dan ABD'ye, Venezuela'dan Kolombiya'ya ve ABD'ye, hatta son günlerde Venezuela'dan İspanya'ya kadar uzanan düzensiz bir göç rotasının olduğu görülmektedir. Özellikle ABD'nin dünyada en fazla düzensiz göçmen yakalayan ülke olduğu söylenebilir. Yine Afrika'dan Türkiye üzerinden, Doğu Akdeniz, Orta Akdeniz ve Batı Akdeniz rotaları üzerinden Avrupa'ya yönelen bir düzensiz göç akımı söz konusudur. Orta Asya ve Orta Doğu'dan benzer şekilde Türkiye üzerinden Avrupa'ya yönelen göç rotaları mevcuttur. Bunun yanında Doğu Avrupa'dan Avrupa'ya düzensiz göçmenlerin izlediği bir göç rotası da bulunmaktadır. Önemli bir göç rotası da Hindistan ve Endonezya'dan Avustralya'ya doğru olan rotadır.

Dünyada küreselleşmenin ivme kazanması ve iletişim kanallarının artması sonucunda insanlar denizin iki kıyısındaki farklı hayatlardan daha kolay haberdar olabildiği gibi çatışmanın ya da yoksulluğun olduğu kıyıdan diğer tarafa geçmenin, refaha ulaşmanın daha kolay olduğunun da farkına varmışlardır. Elbette refah içinde yaşayan insanlar da kendi refahlarını paylaşmak istemedikleri için bu insanları tehdit olarak görmeye başlamışlardır.

Türkiye'de göçle ilgili verilere bakıldığında ülkede 3.736 milyon Suriyeli, 1 milyon 326 bin ikamet izniyle kalanlar (düzenli), 29 bin uluslararası koruma başvuru sahipleri olmak üzere[12] toplam 5 milyonun üzerinde yabancının bulunduğu görülmektedir. Rakamlar, göç baskısının ülke üzerinde ne denli büyük bir yük olduğunu da ortaya koymaktadır. Türkiye bulunduğu coğrafi ve stratejik konumu nedeniyle, tarih içerisinde önemli göç ve iltica akınlarıyla karşı karşıya kalmıştır ve kalmaya da devam etmek-

tedir. Özellikle son yıllarda Türkiye'nin artan ekonomik gücü, ülkeye yönelik göç hareketleri için çekim unsuru oluşturmaktadır. Türkiye, geçiş ülkesi (transit) konumu yanında hedef ülke konumuna da gelmiştir.

Türkiye'ye yönelen düzensiz göç rotaları farklı coğrafyalardan ülkeye yönelmektedir. Bazı göç rotaları Türkiye'yi transit geçiş ülkesi olarak konumlandırırken bazı rotalar açısından da Türkiye hedef ülke konumundadır. Özellikle Afrika ülkelerinden ülkeyi geçiş sahası olarak kullanıp Avrupa'ya geçmek isteyen bir düzensiz göç rotası bulunmaktadır. Orta Asya'dan legal olarak ülkeye girişlerinin ardından illegal olarak kalmaya devam eden ve genellikle ev hizmetlerinde çalışan bir düzensiz göç kitlesi görülmektedir. Bunun yanında ülkelerindeki baskı, zulüm gibi faktörler veya coğrafyadaki siyasi istikrarsızlık ve savaşlar nedeniyle Orta Doğu ülkelerinden Türkiye'ye yönelen bir düzensiz göçle karşı karşıya kalınmaktadır.

2014 yılında Türkiye'de yakalanan düzensiz göçmen sayısı 58.647 iken bu sayı 2019 yılında 454.662'ye yükselmiştir. Her ne kadar özellikle pandeminin etkisiyle bu sayı 2020 yılında 122.302'ye düşmüş olsa da hala 2014 yılının iki katına denk gelen bir sayıyla karşı karşıya olunduğu görülmektedir. 2021 yılında da bu rakam 162.996'ya ulaşmıştır. 2019 yılında bütün Avrupa'da yakalanan düzensiz göçmen sayısının 128 bin olduğu düşünüldüğünde Türkiye'nin düzensiz göç bağlamında çok büyük sayılarla uğraştığı daha iyi anlaşılacaktır.

Türkiye'ye yönelik düzensiz göçe en fazla kaynaklık eden iki ülke Afganistan ve Pakistan'dır. 2019 yılında yakalanan toplam 454.662 düzensiz göçmenin 201.437'sini Afganlılar oluşturmaktadır. Aynı yıl yakalanan Pakistanlıların sayısı 71.645; Suriyelilerin sayısı ise 55.236 olmuştur. Suriyeliler düzensiz göç kapsa-

mında gösterilmekle birlikte geçici koruma altında olduklarını da belirtmek gerekmektedir. Düzensiz göç sadece ülkeye yasadışı girmeyi değil, yasal olarak girdikten sonra yasadışı kalmaya devam etmeyi, yasadışı yollardan ülkeyi terk etmeye çalışmayı ya da yasadışı çalışmayı da kapsadığı için bu kapsamda yakalanan Suriyeliler de düzensiz göçmen olarak istatistiklere yansımaktadır. 2019-2020-2021 istatistiklerine bakıldığında pandemi nedeniyle ülkeye dışarıdan girişlerde bir düşüş olduğu, daha çok ülke içindeki düzensiz göçmenlerin yakalanmasının söz konusu olduğu görülmektedir.

Düzensiz göçmenlerin doğu sınırından özellikle Ağrı ve Van'dan girdikten sonra bir kuzey bir güney hat olmak üzere iki hattı takip ettiği görülmektedir. Kuzey hat Ağrı, Erzurum, Erzincan hattıdır. Güney hattı ise özellikle sınır duvarlarının inşası ile biraz daha güneye kaymıştır. Van'dan gelip genelde Van Gölü'nü kullanarak Bitlis-Tatvan'a ulaşıp Bitlis, Diyarbakır, Şanlıurfa, Gaziantep, Osmaniye, Adana üzerinden Batı'ya doğru giden bir hat bulunmaktadır. Normalde 2019 yılında doğu ve batıda daha yoğun düzensiz göçmen yakalanırken pandeminin etkisiyle ülke içi düzensiz göçmenler yakalandığı için sadece İstanbul'da yoğunluk görülmüştür.

Düzensiz göçmenlerin sınır dışı edilmesiyle ilgili sayılar incelendiğinde yakalama oranları ile bir paralellik olduğu görülmektedir. 2019 yılında 103.858 kişi sınır dışı edilmiştir. Sınır dışı etmenin maliyetinin de dikkate alınması gereken bu süreçte en fazla yakalananlar Afganlılar olduğu için en fazla sınır dışı edilenler de onlar olmuştur.

Düzensiz göçle mücadele kapsamında alınan tedbirlerde ilk olarak mevzuatta yapılan değişikliklere değinmek gerekmektedir. Düzensiz göçmen sayısının başlarda çok düşük olması

nedeniyle ayrı bir birim ihdas edilmemişken gelinen durumda sayıların artması sonucu hem Emniyet Genel Müdürlüğü hem Jandarma Genel Komutanlığı hem de Göç İdaresi Başkanlığı'nda Düzensiz Göçle Mücadele Daire Başkanlıkları kurulmuştur.

> *Düzensiz göçle mücadelede kurumlar arası koordinasyonun daha etkili bir şekilde yürütülebilmesi amacıyla 2021-2025 yıllarını kapsayan "Türkiye Düzensiz Göç Strateji Belgesi ve Ulusal Eylem Planı" hayata geçirilmiştir. Anılan Eylem Planı düzensiz göçle mücadele tedbirlerini yabancıların ilk çıkış ülkelerinde önlemeye yönelik olarak hazırlanmıştır.*

Eylem Planı'nın hedefleri ise şunlardır:

- Düzensiz göçün kaynağında önlenmesi ve göçle ilgili organize suçlarla mücadele edilmesi,
- Düzensiz göçü kaynağında önlemeye yönelik kalkınma odaklı bölgesel ve uluslararası iş birliklerinin güçlendirilmesi,
- Düzensiz göçmenlerin insan hakları çerçevesinde geri gönderilmesi sisteminin güçlendirilmesi,
- Düzensiz göçle ilgili sistematik veri toplama ve analiz yapma ve düzensiz göç politikalarına katkı sağlayacak araştırmaların yapılması,
- Düzensiz göçmenlerin insan haklarının gözetilmesi ve hassas durumda olanların belirlenmesi olarak sıralanmaktadır.

Yabancılara, meslek edindirici eğitimlerden gelir getirici iş kollarına kadar, geniş bir yelpazede destek sağlanabilmesini için Göç İdaresi Başkanlığı öncülüğünde Dışişleri Bakanlığı, Türk İşbirliği ve Koordinasyon Ajansı ve Türk Kızılay Genel Müdürlüğü paydaşlığında "Ulusal Destekli Gönüllü Geri Dönüş Mekanizması" kurulmuştur.

Sınır güvenliğinin artırılması amacıyla güvenlik duvarlarının inşa edilmesine devam edilmiştir. Doğu illerimizde yol kontrolleri, ülke genelinde de otogar, tren garları vb. yerlerde denetim ve güvenlik tedbirleri artırılmıştır. Yol izin belgesiz hiçbir yabancı bırakılmamış ve sahteciliğin önüne geçilebilmesi amacıyla yol izin belgeleri güvenlikli karekodlu olarak basılmaya başlanmıştır. İzinsiz çalışmayla mücadele ile ilgili olarak İstanbul başta olmak üzere tüm büyükşehirlerde denetim ve rehberlik faaliyeti gerçekleştirilmiştir. Göçe kaynaklık eden ülkelere 'Standart Uygulama Prosedürleri' (SOP) teklif edilmiş, düzensiz göç yoğunluğuna en çok kaynaklık eden Afganistan ve Pakistan'a irtibat personeli görevlendirilmiştir. Tahdit genelgesi çıkarılarak belirli suç türlerinde giriş yasaklarının süresi artırılmış, yeni ihtiyaçlara binaen yeni tahdit kodları oluşturulmuştur.

Dijital dönüşümün hızla yaşandığı içinde bulunduğumuz süreçte düzensiz göçle mücadele konusunda daha sistemsel ve dijital tedbirlerin alınması bir gereklilik olarak ortaya çıkmıştır. Bu bağlamda, hakkında işlem yapılan düzensiz göç kapsamındaki yabancıların Göç İdaresi Başkanlığı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı tarafından anlık olarak görülebilmesini sağlayacak "Düzensiz Göç Ortak Veri Tabanı" 2019 yılında kurulmuştur. Vize başvurusu esnasında dış temsilciliklerde parmak izi kaydı alınmasına başlanmıştır. Potansiyel düzensiz göçmen olabilecek yabancıların Türkiye'ye girişlerinin engellenebilmesi amacıyla hava limanlarında 'Düzensiz Göçle Mücadele Risk Analiz Birimleri' kurulmasına yönelik altyapı çalışmaları tamamlanmıştır. Hudut kapılarında parmak izi doğrulanmasına yönelik olarak çalışmalar başlatılmıştır. Pakistan ile yapılan müzakereler akabinde iki ülke arasında Pakistan vatandaşlarının uyruklarını doğrulamak için sistem kurulmuştur. Sistemin kurulması ile birlikte 2018 yılında %5 olan Pakistan uyruklu yaban-

cıların sınır dışı edilme oranı 2019 yılında %16'ya, 2020 yılında ise %72'ye yükselmiştir.

Göçmen Kaçakçılığı

Düzensiz göç ile mücadelenin en önemli alanlarından birisi de göçmen kaçakçılığı ile yapılan mücadeledir. Göçmen kaçakçılığı suçu; maddi çıkar elde etmek amacıyla yasal olmayan yollardan Türkiye'ye insan sokma veya Türkiye'den yurtdışına insan çıkmasına imkân sağlanmasıyla oluşur. Göçmen kaçakçılığında suç teşebbüs aşamasında kalmış olsa dahi, tamamlanmış gibi cezaya hükmolunur. Göçmen kaçakçılığı suçu ile düzensiz göç akımları arasında pozitif bir korelasyon mevcuttur. Bu sebeple düzensiz göçle mücadelede en önemli unsurlardan biri de göçmen kaçakçılığıyla mücadeledir. Yakalanan göçmen kaçakçısı sayılarına bakıldığında 2019 yılı itibariyle 8.996 ile en fazla yakalama gerçekleşmiştir. Yakalanan 8.996 kaçakçının sadece 1.948'inin tutuklanabilmiş olması hukuki süreci caydırıcı olmaktan çıkarmaktadır.

2017 yılında kanuna eklenen bir KHK ile göçmen kaçakçılığında kullanılan araçlara el koyma (müsadere) ve para cezalarını artırma yetkisi verilmiştir. 2019 Aralık ayında TCK'da yapılan bir değişiklikle göçmen kaçakçılığındaki suçlar ağırlaştırılmıştır (TCK 79). CMK'da yapılan değişiklikle ise göçmen kaçakçılığı suçu katalog suçlar kapsamına alınmıştır. Tutuklamaların artması için gidilen bu değişiklik henüz istenen sonucu tam olarak vermemiştir. Yine 2019 Aralık ayında yapılan değişiklik ile idari gözetime alternatif yükümlülükler ilk defa kanunlaşmıştır. Düzensiz göçmenlerin gönüllü geri dönüşünü sağlamak için kurulacak ulusal mekanizmaya yönelik mevzuat çalışması yapılmıştır. Sınır dışı etme kararına karşı yargı yoluna başvurma süresi ise

15 günden 7 güne indirilmiştir. Yapılan değişikliklerle göçmen kaçakçılığında kullanılan araçlara el koyma ile birlikte suç süreleri değiştirilerek caydırıcılığın artırılması amaçlanmıştır. Karşılaşılan en büyük güçlüklerden birisi olan düzensiz göçmenlerin uyruk tespitine yönelik olarak idari gözetim altına alınan yabancıların uyruk tespitlerini yapabilmek maksadıyla yabancıların iletişim cihazlarında inceleme yapılabileceği düzenlenmiştir. Özellikle Afrikalı düzensiz göçmenler yasal yollarla ülkeye giriş yaptıktan sonra pasaport ve kimliklerini imha edip Türkiye'de diplomatik temsilcisi olmayan ülkelerin vatandaşı oldukları iddiasıyla sınır dışı edilmekten kurtulma yoluna gitmektedir. Yapılan düzenleme ile bu durumun önüne geçilmesi hedeflenmiştir.

İnsan Ticareti

Çağımızın modern köleliği olarak adlandırılan insan ticareti, en yalın hali ile bir kişinin ticari bir meta haline dönüştürülmesini ifade eder. İnsan ticareti suçu bireylerin temel hak ve hürriyetlerini tehdit etmenin yanı sıra kamu düzenine, kamu güvenliğine ve kamu sağlığına karşı da ciddi bir tehdit oluşturmaktadır. BM Uyuşturucu ve Suç Ofisinin (UNODC) verilerine bakıldığında insan ticareti suçunun görülme biçimlerinin yedi farklı şekilde tasnif edildiği görülmektedir: cinsel sömürü, işgücü sömürüsü, zorla evlendirme, çocuk satışı, zorla dilendirme, çocuk askerlik, organ ve doku ticareti.

Her ne kadar burada yedi adet sömürü biçiminden bahsedilse de bunun ucu açıktır. İnsan ticareti suçu dinamik bir yapıya sahiptir. Kendini sürekli yeniler, sisteme kolayca adapte olabilir ve hatta kültürel pratiklerin içine dahi sinebilir. Türkiye'de 2015-2020 yıllarını kapsayan dönemde insan ticareti mağduru olan 1.223 kişi tespit edilmiştir. Mağdurlar içinde 342 ile en fazla Su-

riyeli bulunmaktadır. Bu kapsamda işlenen suçlar kapsamında en fazla görülen ise cinsel sömürü suçudur.

Dünya üzerinde çeşitli coğrafyalarda hala süregelen göç politikalarının gelişimine ve bu politikaların pratikteki sonuçlarına bakıldığında iki yaklaşım öne çıkmaktadır;

- Göçü sadece güvenlik problemi olarak görüp bunun bir çıktısı olan dışsallaştırma yaklaşımıyla göçün engellenebileceğini önceleyen yaklaşım,
- Göçün durdurulamayacağını; ancak insan haklarına saygılı bir şekilde özgürlük ve güvenlik dengesini kurarak problemlere yerinde ve kalıcı çözümler üreten göç yönetimini temel alan yaklaşım.
- Gelişmiş batılı ülkeler göçün insan hakları boyutunu göz ardı ederek, göçü yalnızca bir güvenlik problemi olarak tanımlayıp dışsallaştırma yaklaşımı sergilerken Türkiye göçe insan haklarına saygılı bir yaklaşım açısından bakarak geri kabul anlaşmaları, ikili ülke iş birlikleri, kalkınma odaklı projeler geliştirerek göç sorununu kaynağında kalıcı çözümler üreterek yönetmektedir.

Güvenlik Politikalarında Yeni Meydan Okumalar ve Yaklaşımlar

Uluslararası güvenlik devletlerin varlığına yönelik tehditleri çalışmaktadır: savaş tehditleri, isyanlar, ordular, silahlanma, göç meseleleri, sınır güvenliği vb. Uluslararası güvenlik denilince güvenlik yönetimi ile ilgili akla gelen ilk konu genellikle askeri güç üzerine şekillenmiştir. 1960'larda ve 1970'lerde dünyada nükleer tehdit konusu tartışılmış, 1990'lardan günümüze kadar geçen sürede ise çok daha yeni güvenlik sorunları tartışılmaya başlamıştır. 11 Eylül olayları ile birlikte bütün akademik gündem bir anda teröre doğru kaymıştır.

Yeni güvenlik yaklaşımını bir sınıflandırma üzerinden incelemek için sert güç/yumuşak güç alanları olarak bir ayrıma gitmek işlevsel olacaktır. Uluslararası güvenlik, geleneksel olarak sert güç alanında ele alınmaktadır. Bu bağlamda devletlerarası savaş, silahlanma, uluslararası terörizm gibi konular tartışılmaktadır. Doğal kaynakların ve çevrenin güvenliği, küresel halk sağlığı, ekonomi güvenliği, gıda, tohum, hava, toprak güvenliği gibi alanlar yumuşak güç alanlarını teşkil etmektedir. Uluslararası güvenlik bu minvalde değişim geçirmektedir.

Son dönemde Batılı demokrasilerde insan odaklı bir yaklaşımdan söz edilmektedir. 2003 BM İnsani Güvenlik Komisyonu'nun nihai raporu BM'nin görevlerini sıralamakta ve böylelikle bu görevleri egemen devletlere de zımnen tebliğ etmiş olmaktadır. Bu görevler;

- İnsanları şiddetli çatışmalardan korumak,
- İnsanları silahların yayılmasından korumak,
- Hareket halindeki insanların güvenliğini desteklemek,
- Çatışma sonrası durumlarda kullanılmak üzere insan güvenliği geçiş fonları oluşturmak,
- Genel sağlık hizmetlerinden herkesin yararlanmasını sağlamak,
- Her yerde asgari yaşam standartlarının sağlanması için çalışmak,
- Patent hakları için bir sistem geliştirmek,
- Tüm insanları evrensel nitelikli temel eğitimle güçlendirmek,
- Küresel insan kimliğine olan ihtiyacı netleştirirken aynı zamanda insan özgürlüğünün farklı kimlik ve aidiyetleri içermesini sağlamak şeklinde sıralanmıştır.

BM İnsani Güvenlik Komisyonu nihai raporunda geleneksel

güvenlik algısına ait ifadeler görülmektedir; ancak bunların hayata yansıması konusunda ciddi sorunlar yaşanmaktadır. Örneğin; koruma sorumluluğuna ilişkin olarak bu sorumluluk uluslararası insani norm olarak kabul edilecek diye beklenirken söz konusu nosyon örneğin Libya'da gündeme gelmiş, kısmen uygulanmış ama Suriye'de uygulanmamıştır. Hatta gündeme dahi gelememiştir. Bu norm benzer şekilde Filistin konusunda yine benzer şekilde gündeme gelememiştir. Dolayısıyla uluslararası kuruluşların devletlere enjekte etmeye çalıştığı bu tür güvenlik nosyonlarının uygulamada işlemediği söylenebilir.

Uluslararası güvenlikte çalışmalar ve ilgilerin nereye kaydığına bakmak gerekirse buradaki odak noktasının insan olduğu belirtilebilir. Yeni konseptte insana yeni bir bakış açısı söz konusudur. Bu yeni bakışla ilgili irdelenmesi gereken önemli bir nokta da yeni bir alan olarak devlet dışı aktörlerdir. Devlet dışı aktör bir taraftan silahlı yapıları içine alırken diğer taraftan da Zuckerberg'in şirketleri olabilmektedir. Bu durumda Zuckerberg'in Facebook adlı şirketi bir anda devlet dışı aktöre dönüşebilmektedir. Tabi burada devlet dışı olarak nitelendirilen aktörlerin ne kadar devlet dışı olduğu da ayrı bir tartışma konusudur. Dolayısıyla sorunları ve konuları devletin varlığının ötesinde ve çoğu zamanda devletin varlığının içinde (dışında olduğu durumlar da olabilir) tanımlamaya başladığımızda ve bunula ilgili de bilgi üretmeye başladığımızda bambaşka bir dünya ile karşı karşıya kalınmaktadır. İçinde bulunduğumuz dünyanın içerisinde çok derin ve tehditlerle dolu konular yer almaktadır.

Günümüzde bilgi üretimi astronomik boyutlara ulaşmıştır. Bu çağda günlük 2,5 kentilyon (10 üssü 18) bayt bilgi üretilmektedir. Bu bilgi bireyler olarak üretilmektedir ve artık bilgi çağı insanları ile karşılaşılmaktadır.

Dünyada çok önemli veri işleyen merkezler mevcuttur: Google, Amazon vb. Bu "big data" denilen veriler dünyadaki insanlar hakkında çok detaylı, özel alanı da içeren bilgilere sahiptir. Kullanılan mobil telefonlar aracılığıyla her anı takip edilen milyarlarca insan bulunmaktadır. Türkiye olarak son on yılda neler yaşanıldığı üzerinden gidilecek olursa geleneksel güvenlik yapıları reforme edilmiştir. Bu alandaki eksikliklere ve karşılaşılan meydan okumalara bağlı olarak güvenlik sistemi yenilenme ve etkinleştirme sürecine girmiştir. Türkiye'de pek çok konuda olduğu gibi bilgi iletişim teknolojileri ve dijitalleşme alanında da çok önemli kapasite gelişimi yaşanmıştır.

Sosyal ağlarda paylaşılan veriler, kişisel verilerin paylaşımı konusu, sağlık güvenliği gibi konular artık uluslararası güvenliğin parçası haline gelmiştir. Yeni risk alanları karma bir sorumluluk yüklemektedir. Bütün bunlar güvenlik meselesinin çok farklı yaklaşımlarla ele alınacağını göstermektedir. Güvenlik meselelerinin siyasallaşması söz konusudur. Mesela devlet dışı aktörlerin meydan okumaları üzerine Twitter'ın Trump'ın hesabını kapatması önemli bir örnek teşkil etmektedir. Bu noktada sorunların tamamına hâkim olacak, analitik düşünce ile hareket edebilecek, öngörüleri yüksek yetişmiş insanlara ihtiyaç bulunmaktadır. Sürekli yenilenen teknolojik altyapıya gereksinim söz konusudur. Otantik veri girişleri yapabilecek konuma gelmek gerekmektedir. Elde edilen verileri analitik olarak ele alıp politikaya dönüştürecek, nihayetinde de bu politikaların uygulanmasını sağlayacak kadrolara ihtiyaç gittikçe artmaktadır.

SONUÇ

Modern dünyayı dönüştüren ve şekillendiren, üzerinde kapsamlı tartışmalar barındıran küreselleşme olgusu; yoğunlaşan ilişkiler ve etkileşimler sayesinde çok kültürlülüğü; özgürlük, eşitlik, insan hakları gibi vurgularla demokrasiyi; iletişim ve ulaşım araçlarındaki gelişmeler sayesinde teknolojik araçların, yeniliğin ve enformasyonun yayılmasını sağlayıp kıtalar arası ekonomik, sosyal ve siyasi entegrasyonu beraberinde getirse de, bu olumlu özelikler yanında birtakım dezavantajlara da sahiptir. Küreselleşmenin hem avantaj hem de dezavantaj sağladığı alanlardan birisi de 'güvenlik' meselesidir. İçinde bulunduğumuz süreçte tanık olduğumuz üzere, küreselleşme; bulaşıcı hastalıkların yayılmasından siber suçlara, siber saldırılardan çevre sorunlarına, terör faaliyetlerinden organize suçlara, etnik çatışmalardan düzensiz göç hareketlerine kadar ulus devletleri ve uluslararası örgütleri ulus ötesi güvenlik tehditlerine açık hale getirmektedir. Bunun yanında küresel tehditlerle etkili mücadelede edebilmek adına güvenliği çağdaş paradigmaları ve gelişmeleri esas alarak yönetmeyi, güvenlikle uğraşan organizasyonların ve aktörlerin teknolojik gelişim ve değişimlere entegre olmasını zorunlu kılmaktadır.

Çalıştayda güvenlik yönetimi konusu küreselleşme, teknoloji ve dijitalleşme boyutlarıyla ele alınmış olup; 21. Yüzyılda güvenlik yönetimine ilişkin tespitler, sorunlar ve çözüm önerilerine yer verilmiştir. Çalıştayda genel olarak öne çıkan tespitler, sorunlar ve öneriler şu şekilde özetlenebilir:

- Geleneksel güvenlik çalışmalarının mevcut sorunlara çözüm üretme noktasında yetersiz kalışı, yeni güvenlik anlayışının toplumsal ihtiyaçlar doğrultusunda genişlemesini ve derinleşmesini beraberinde getirmiştir.

- Küreselleşmenin baskısı altında değişen bir dünyada güvenliği sağlama çabası, güvenlik yapısını daha insani ve toplumsal boyutlara indirgemekte ve tüm dünyada yeni mücadele alanlarını genişletmektedir.
- Küreselleşmenin de etkisiyle belirsiz bir niteliğe bürünen tehditlerle mücadele çok sayıda aktörün müdahalesini ve iş birliğini gerektiren bir yapıyı gerekli kılmaktadır.
- Küreselleşme sürecinde güvenlik politikalarının/siyasalarının meşruluğu içerecek şekilde, anayasacılık dairesinde, bireyi merkeze alarak yapılması oldukça önemlidir. Sadece yönetenlerin değil yönetilenlerin de dahil olduğu yönetişim anlayışı çerçevesinde icra edilecek güvenlik yönetimi süreci daha etkili bir yönetsel sürecin tatbiki açısından önem arz etmektedir.
- Polislik her şeyden önce toplumla iç içe olan bir meslektir. Bu nedenle sosyo-ekonomik ve siyasal hayattaki herhangi bir değişiklik polisliği doğrudan etkilemektedir. Günümüz modern toplumlarında yaşanan hızlı dönüşümlere ayak uydurabilmesi ve değişen şartlara ve beklentilere yanıt verebilmesi için polis teşkilatlarının da bu değişime uyum sağlaması önem arz etmektedir.
- Toplumun değişen yapısına adapte olacak şekilde, gelişmiş ülkelerde polis memurlarının ve amirlerinin yüksek düzeyde eğitimlilerden tercih edildiği görülmektedir.
- Modern demokratik ülkelerde yüksek eğitimli polislerin şeffaflık, hesap verebilirlik gibi ilkeleri daha kolay özümsedikleri görülmektedir. Bu tür ülkelerde gittikçe artan düzeyde yüksek eğitimli personel polis teşkilatına dahil olmaktadır.
- Bugünün dünyasında polisliğin militer bir anlayış ve eğitim zihniyetinden uzaklaştırılarak sivil bir yaklaşımla

toplumun dinamik ve çeşitlilikleri içeren yapısıyla daha uyumlu hale getirilmeye çalışıldığı görülmektedir. Böylece vatandaş odaklı, bireylerin beklentilerine ve çağın gerekliliklerine hızlıca yanıt veren, etkin ve etkili bir polis birimi ortaya çıkmaktadır.

- Gelişmiş demokratik ülkelerdeki polis eğitimlerinin temel ortak özelliklerine bakıldığında polisin sivil otoritenin sevk ve idaresinde olduğu, kısa süreli, uygulama ağırlıklı eğitim verildiği ve toplumla iç içe bir polislik yapısının inşasının amaçlandığı görülmektedir.
- İnsan hakları ve güvenlik birbirini ayrıştıran değil, birbirini tamamlayan kavramlardır.
- Güvenliğin tesisi için bireyin hak ve özgürlüklerinin göz ardı edilmemesi gerekmektedir. İnsan hakları ve güvenlik, bir yandan değişen ve artan tehditlerin merkezinde güvenlik kavramının yer aldığı, diğer yandan da bireysel hak ve özgürlükler ile insan onur ve haklarına saygı gösterilmesi gereken bir toplum yaratılması amacıyla biri diğerine tercih edilemeyecek olgulardır.
- Dezenformasyon odaklı stratejik iletişim ve kriz yönetimi yaklaşımı geliştirilmesi dezenformasyonla mücadele önem taşımaktadır.
- Türkiye'nin dezenformasyona karşı koyabilmesi için stratejik bir çerçeve geliştirilmesi gerekmektedir. Pozitif bir gündem ile negatif gündem arasındaki bağın kurulabilmesi ve akademik çalışmaların daha kaliteli, daha nitelikli daha nicel araştırmalara yönelik hale getirmesi büyük bir öneme haizdir.
- Yapay zekâ insanlar gibi düşünen, insanlar gibi davranan ve insanlar gibi rasyonel düşünen sistemlerdir. Hatta insanlardan daha rasyonel davranan sistemler olarak bile adlandırılabilir.

- Yapay zekâ teknolojisi marifetiyle potansiyel suçlu tespiti ve potansiyel olay tespiti üzerinden hızlı müdahale sistemi geliştirilebilmektedir.
- Uluslararası ölçekte sosyal medya ağlarında yakın zamanda veri kaçaklarının arttığı gözlenmektedir. Veri kaçaklarının veya verilerin başkalarının eline geçmesinin önlenmesi için blokzincir (blockchain) kullanılabilir. Söz konusu veriler farklı yerlerde birbirine bağlı olarak tutulduğu için diğer sistemlerden farklı olarak bu sistemde verileri korumak daha kolay olmaktadır.
- Dijital dönüşüm ile istihbarat yönetimi birer kültürel olgudur ve kendi içinde ortak değerler ile semboller taşımaktadır. Aynı alanda çalışan kişiler tarafından kurulan organizasyonlarca yönetilmektedir. Ayrıca kendine has yaklaşımlar, davranış kodları, iletişim biçimleri mevcuttur.
- İstihbarat yönetiminde meydana gelen dijital dönüşümle birlikte neredeyse bütün istihbarat alt alanları artık teknolojinin kullanıldığı alanlar haline gelmiştir.
- Dijitalleşmenin istihbarat yönetimi üzerindeki etkisiyle birlikte devletlerarasında uluslararası sorun yaşama riski azalmaktadır. Bunun yanında 'daha az risk' ile 'önleyicilik' çok daha yüksek seviyede elde edilebilmektedir.
- Dijitalleşme ve istihbarat yönetimi bir arada değerlendirildiğinde şu hususlar ön plana çıkmaktadır:
    - Dijital dönüşüme paralel olarak devletlerin tehdit, risk, koruma, önleme yaklaşımlarının ve hukuksal düzenlemelerin sıklıkla gözden geçirilerek güncellenmesi gerekmektedir.
    - Dijital dönüşüme adapte olmuş nitelikli istihbarat çalışanlarının akademik ve mesleki eğitimlerinin ilgili kurumlarca gerçekleştirilmesi önem taşımaktadır.

- İstihbarat yönetimi teknolojiye odaklansa da profesyonel insan istihbaratının göz ardı edilmemesi gerekmektedir.
- İstihbarat yönetimi organizasyonunun içinde etkin psikolojik harp birimlerinin teşkil edilmesi gerekmektedir.
- Sızma, casusluk gibi siber güvenlik önlemleri konusunda çözümlemelere duyulan ihtiyaç İKK faaliyetlerinin de bir parçası haline gelmelidir.
- Açık kaynak istihbaratı sayesinde proaktif güvenlik yaklaşımının reaktif güvenliği öncelemesine imkân tanınmalıdır

• Biyolojik terör ile ilgili önemli bir sorun onların doğal olarak gerçekleşen olaylardan tespit edilmesinin zorluğudur.
• Suçlular ve teröristler genellikle biyolojik ajanları (virüs, bakteri, toksin) geleneksel silahlara göre daha çekici bulmakta ve alternatif olarak görmektedirler. Çünkü biyolojik silah üretimi nispeten düşük maliyetlidir, mikroorganizmalara kolayca erişilebilir, üretilmesi, modifiye edilmesi ve salınması basit olabilir.
• Olası biyoterörizm tehditlerine karşı tedbirlerin alınması önem arz etmektedir. Bu yüzden şu hususlar önem taşımaktadır:
    - Kasıtlı olarak oluşturulabilecek biyoterör salgınlarına hazırlıklı olmak, doğal salgınlara verilecek cevabı da güçlendirecektir.
    - Meydana gelen salgınlar üst düzey liderlik, sorumluluk ve yetki ile sürdürülmelidir.
    - Sağlık hizmeti sektörü; biyoterörizm potansiyeli ve bilinmeyen patojenlerin varlığını göz önünde bulundurup, biyolojik ajanlara olan farkındalığı sürdürmelidir.

- Acil servis ve halk sağlığı doktorları potansiyel biyoterörist ajanların neden olduğu hastalıkların klinik belirtilerini ve ortaya çıkabilecek bulaşıcı hastalıkları düzenli olarak güncellemelidir.
- Kişisel koruyucu donanımlar geliştirilerek halkın kullanımına sunulmalıdır.
- Ciddi, bulaşıcı hastalığı olan hastalarda olası ani ve büyük artış durumları göz önünde bulundurularak sağlık sistemine kendisini hızla revize etme yeteneği kazandırılmalıdır.
- Daha hızlı, daha güvenilir tanı testleri geliştirmek için genel ve özel laboratuvarların kapasitesi artırılmalıdır.
- Yeni ve geliştirilmiş aşılar ve tedavi süreci geliştirilmelidir.
- Klinik ve çevresel sürveyansın (hastalığın kontrol altına alınması) artması gerekmektedir.
- Sendromik sürveyans sistemleri (belirli hastalıkların nasıl ortaya çıktığı ve dağıldığına ilişkin sistematik olarak yapılan gözlem sistemleri) geliştirilerek doktorlar tarafından bildirilen vakalar bir salgının ilerlemesini izlemek için kullanılabilmelidir.
- Hem ulusal hem de uluslararası bağlamda yeterli miktarda aşı ve ilaç stoğu bulundurulmalıdır.

• Doğal ve biyoterörist salgınlara karşı hazırlığı geliştirmek için, uluslararası iş birliği, birden fazla ülkeyi içeren ortak tatbikatlar ve potansiyel biyoterörizm tehditleri hakkında bilgi alışverişinde iyileştirme ve yönetim sistemleri kurulmalıdır.

• Yeni güvenlik anlayışı ile birlikte uluslararası terörizm, or-

ganize suç örgütleri, siber terör, saldırı amacı güden devletler, konvansiyonel kitle imha silahlarının yaygınlaşması gibi tehditler, ulusal fiziki varlığa yönelik tehditler olarak konumlanmaya başlamıştır.

- Koronavirüs sürecindeki yeni dönemde uluslararası toplum tarafından terk edilmiş olma düşüncesi birçok ülkeyi içe kapanmaya yöneltmiştir. Bu durum ne yazık ki ırkçılık, yabancı karşıtlığı ve İslam düşmanlığı gibi toplumsal marazlara ivme kazandırmıştır.
- Terör örgütleri salgının bazı ülkelerde ortaya çıkardığı otorite boşluklarından istifade ile yeni palazlanma süreçlerine girişmektedir. Özellikle aşırı sağcı yapılar salgının ortaya çıkardığı ekonomik zorlukları bahane ederek kendilerine zemin oluşturmaya çalışmaktadır.
- Kırılgan devletler, terör örgütleri için hem bir üreme hem de barınma alanı oluşturmaktadır. Bunun örnekleri tarihte de görülmekle birlikte Suriye çarpıcı bir örnek teşkil etmektedir. Merkezi otorite zayıfladıkça PKK'nın Suriye kolu olan YPG/PYD'nin, DEAŞ'in, El-Kaide türevi olan örgütlerin Suriye'de giderek zemin kazandığını hatta belki Suriye'de daha önce görülmemiş biçimde alan kontrolü üzerinden egemenlik iddiasında bulunduğu görülmüştür.
- Kırılgan devletlerde sınırların kontrol edilemeyişinin iki etkisi olmaktadır: ilki kitlesel göç hareketlerinin başlaması, ikincisi ise terör örgütleri de dâhil olmak üzere silahlı grupların sınır hattını kullanarak geçişkenlik kazanmasıdır. Bu geçişkenlik sınırı olan ülkeler için önemli güvenlik riskleri doğurmaktadır. Bu durumun en somut örneklerinden birisi YPG'nin Türkiye'ye yönelik terör eylemleri diğeri ise DEAŞ'ın Fırat Kalkanı Harekâtı öncesinde başta sınır illeri ve büyükşehirler olmak üzere düzenlediği terör eylemleridir.

- Suriye krizi egemenlik ilkesinin aşınması ve içişlerine karışmama ilkesinin ihlali bakımından da oldukça çarpıcı bir örnektir. Bu durum bir güvenlik tehdidi oluşturmaktadır. Merkezi otorite zayıfladıkça komşu ülkeler veya küresel aktörler o ülkenin yarattığı güvenlik risklerini bertaraf edebilmek ve kendine dönük güvenlik tehditlerini minimize edebilmek açısından soruna müdahil olmaktadırlar.
- Türkiye gerek DEAŞ'ın terör saldırıları gerekse PKK'nın devletleşme çabalarının Türkiye'nin güvenliğine yönelik tehditler içermesi nedeniyle ve bu amaca yönelik olan terör faaliyetlerini önlemek misyonuyla Suriye'deki duruma müdahil olmuştur. Ancak Suriye'de bölge dışı aktörlerin de müdahil olduğu bir kriz süreci yaşanmaktadır.
- Düzensiz göçle mücadelede kurumlar arası koordinasyonun daha etkili bir şekilde yürütülebilmesi amacıyla 2021-2025 yıllarını kapsayan "Türkiye Düzensiz Göç Strateji Belgesi ve Ulusal Eylem Planı" hayata geçirilmiştir. Anılan Eylem Planı düzensiz göçle mücadele tedbirlerini yabancıların ilk çıkış ülkelerinde önlemeye yönelik olarak hazırlanmıştır.
- Uluslararası güvenlik, geleneksel olarak sert güç alanında ele alınmaktadır. Bu bağlamda devletlerarası savaş, silahlanma, uluslararası terörizm gibi konular tartışılmaktadır. Doğal kaynakların ve çevrenin güvenliği, küresel halk sağlığı, ekonomi güvenliği, gıda, tohum, hava, toprak güvenliği gibi alanlar yumuşak güç alanlarını teşkil etmektedir.
- Güvenlik meseleleri siyasallaşmakta, sürece devlet dışı aktörler de müdahil olmaktadır.
- Güvenlik tehditleri ile başa çıkmada analitik düşünce ile hareket edebilecek, öngörüleri yüksek yetişmiş insan gücüne ve sürekli yenilenen teknolojik alt yapıya ihtiyaç duyulmaktadır. Otantik veri girişleri yapabilecek konuma gelmek gerekmektedir.

- Elde edilen verileri analitik olarak ele alıp politikaya dönüştürecek, nihayetinde de bu politikaların uygulanmasını sağlayacak kadrolara ihtiyaç gün gittikçe artmaktadır.

SON NOTLAR

[1] Bkz. N. Khardori, T. Kanchanapoom, Overview of Biological Terrorism: Potential Agents And Preparedness Clin. Microbiol. Newsl., 27 (2005), pp. 1-8; R.M. Atlas, Combating the Threat of Biowarfare and Bioterrorism: Defending Against Biological Weapons is Critical to Global Security, BioScience, 49 (1999), pp. 465-477; E.M. Eitzen, Use of Biological Weapons, Medical Aspects of Chemical and Biological Warfare (1997), pp. 437-450.

[2] L. Szinicz, History of Chemical and Biological Warfare Agents, Toxicology, 214 (2005), pp. 167-181./ L.G.W. Christopher, L.T.J. Cieslak, J.A. Pavlin, E.M. Eitzen , Biological Warfare: A Historical Perspective, JAMA, 278 (1997), pp. 412-417.

[3] W.S. Carus, A Short History of Biological Warfare: From Pre-history to the 21st Century Government Printing Office (2017); V. Barras, G. Greub History of Biological Warfare and Bioterrorism Clin. Microbiol. Infect., 20 (2014), pp. 497-502.

[4] V. Barras, G. Greub, History of Biological Warfare and Bioterrorism, Clin. Microbiol. Infect. 20 (2014) 497–502./ N.J. Beeching, D.A. Dance, A.R. Miller, R.C. Spencer, Biological Warfare and Bioterrorism, BMJ 324 (2002) 336–339

[5] H.-J. Jansen, F.J. Breeveld, C. Stijnis, M.P. Grobuschm Biological Warfare, Bioterrorism, and Biocrime Clin. Microbiol. Infect., 20 (2014), pp. 488-496

[6] J.A. Pavlin Epidemiology of bioterrorismm Emerg. Infect. Dis., 5 (1999), p. 528

[7] D.C. Lehman Forensic microbiology Clin. Microbiol. Newsl., 36 (2014), pp. 49-54

[8] R.S. Murch, Bioattribution Needs A Coherent International Approach to Improve Global Biosecurity, Front. Bioeng. Biotechnol. 3 (2015) 80./ R.S. Murch, Designing An Effective Microbial Forensics Program for Law Enforcement And National Security Purposes, Arch. Immunol. Ther. Exp. 62 (2014) 179–185

[9] P.S. Keim, B. Budowle, J. Ravel, Microbial Forensic Investigation of the Anthrax-Letter Attacks, Microbial Forensics, Elsevier, 2011, pp. 15–25./ A.S. Khan, P.S. Amara, S.A. Morse, Forensic Public Health: Epidemiological and Microbiological Investigations For Biosecurity, Microbial Forensics, Elsevier, 2020, pp. 105–122.

[10] Uluslararası Göç Örgütü (2020). World Migration Report,https://publications.iom.int/books/world-migration-report-2020-turkish-chapter-2 (E.T: 13.01.2022).

[11] United Nations (2020). International Migration 2020 Highlights,https://www.un.org/en/desa/international-migration-2020-highlights (E.T. 14. 01. 2022).

[12] Göç İdaresi Başkanlığı, İstatistikler, https://www.goc.gov.tr/uluslararasi-koruma-istatistikler (E.T. 16.01.2022).