KÜRESELLEŞME VE TEKNOLOJİDEKİ GELİŞMELERİN GÜVENLİK AÇISINDAN YARATTIĞI YENİ RİSK VE TEHDİTLER

Dr. Ataalp PINARER
Jeopolitürk

Giriş

Küreselleşme; devletler ve şirketler arasında sosyal ve ekonomik alanlardaki küresel işbirliğinin nicelik ve nitelik olarak artışı sonucu, başta ekonomik alanda olmak üzere, devletler arasındaki bağlantı ve bağımlılığın artışı süreci olarak değerlendirilebilir.[1]

Küreselleşme etkileri itibariyle; siyasi, ekonomik, sosyal, kültürel, coğrafi, ekolojik ve teknolojik alanları kapsayan, geniş bir anlam ifade etmektedir.[2] Birçok konunun birbirine doğrudan veya dolaylı etkisi olduğu kabul edilmekle beraber; bu yazıda küreselleşmenin güvenliğe yönelik etkileri üzerinde durulmaktadır. Küreselleşmenin neden olduğu doğrudan veya dolaylı birçok etki ile güvenliği menfi yönde etkileyen birçok gelişme meydana gelmiştir.

Küreselleşmenin en büyük etkisi ulus devlet yapıları üzerinde gerçekleşmektedir. Küreselleşme ile uluslararası ve ulusüstü yapıların gelişmesi, ulusal egemenliğin aşınmasına yol açmakta, ulusal çıkarları sağlamaya yönelik güç politikalarının uygulanmasını güçleştirmektedir.[3]

1 "Globalization and Defense", The Institute of Defence And Strategic Studies (IDSS) Conference Report, 15-16 March 2006, Singapore, s.4

2 Küreselleşmenin Boyutları ve Etkileri, TASAM, 14.12.2006 (http://www.tasam.org/trTR/Icerik/211/kuresellesmenin_boyutlari_ve_etkileri)

3 Yılmaz, Sait, Uluslararası İlişkilerde Güç ve Güç Dengesinin Evrimi, Stratejik Araştırmalar Dergisi 1 (01), 2008, s. 30

Küreselleşme ortamının doğrudan veya dolaylı olarak yarattığı etkilerle, güvenlik kavramı da değişmekte, şekil değiştirmektedir. Güvenlik kavramı mevcut durum itibariyle, genişlemiş, uluslararası ve devletler üstü bir yapıya bürünmüştür. Artık ulus devletler güvenlik konseptlerini yeni koşullara göre tadil etmek durumundadırlar.

Diğer taraftan teknolojik gelişmelerin önümüzdeki yıllarda artan bir hızla devam edeceği; 21 inci yüzyılda insanlığın ürettiği tüm teknolojik birikimin toplamı kadar bir gelişme sağlanacağı öngörüleri yapılmaktadır. Bu gelişmeler yine çok geniş bir alanda insanlığı etkileyecektir. Otomasyon, yapay zekâ, makinelerin iletişimi ve robot teknolojisindeki gelişmelerin sanayi ve ekonomi başta olmak üzere insan, toplum ve devlet üzerinde ne tür radikal değişimlere neden olacağı üzerinde tartışılan güncel bir konudur. Ancak bu yazının temel dayanağı olarak alınan teknolojik gelişmelerin, harp ve çatışmanın doğasına; dolayısıyla ülkelerin güvenliğine etkileri çarpıcı boyutlarda olabilecektir.

Robot teknolojileri ile yapay zekâ uygulamalarının, harp silah, sistem ve araçları üzerinde neden olacağı gelişmelerin, geçmişte ateşli silahlar, motorlu araçlar, roket ve füzelerin harp yöntem, taktik ve stratejileri üzerinde yapmış olduğu etki kadar, devrimsel yeni dönüşümlere yol açacağı düşünülmektedir.

Bu bağlamda tebliğimin 2. Bölümünde, küreselleşmenin güvenliğe yönelik etkileri incelenirken; 3. Bölümde teknolojik gelişmeler etkisinde tehdit ve risklerdeki değişimler; insansız hava araçları ile dronların temini ve silah olarak kullanımı, robot teknolojisindeki gelişmeler ve yapay zekâ ile siber saldırı alt başlıkları ile analiz edilmektedir. 4. Bölümde ise bu gelişmelerin savaş yöntem ve stratejilerinde neden olabileceği gelişmeler üzerinde durulmaktadır. Sonuç bölümünde ise tahlilin neticesi ve alınması gereken tedbirlere yönelik teklifler yer almaktadır.

1. Küreselleşme ve Güvenlik Kavramında Meydana Gelen Değişimler

Küreselleşme, esas olarak ulus devletlerin güvenlik paradigmalarını değiştirmiş, güvenliklerine yönelik birçok yeni tehdit ve riskin ortaya çıkmasına neden olmuştur. Küreselleşmenin etkisiyle başta ekonomik yapı ve egemenlik olmak üzere, ulus devletler genel bir olumsuz etki altında bulunmakta ve ortaya çıkan değişimlere uyum sağlamaya çalışmaktadırlar. Dolayısıyla bu durumda, ortaya çıkış dinamikleri ve yarattığı etkiler itibari ile savaş ve güvenlik kavramları da değişim göstermektedir.[4] Güvenlik kavramı sadece ulus devletler kapsamında değerlendirilemeyecek şekilde, adeta uluslararası ve devletler üstü bir yapıya bürünmüştür. Bu nedenle 21. Yüzyılda ulus devletlerin güvenlik konseptlerini gözden geçirmesi ihtiyacı bulunmaktadır.

4 "Globalization and Defense", The Institute of Defence And Strategic Studies (IDSS) Conference Report, 15-16 March 2006, Singapore, s.4

Soğuk savaş yıllarının ideolojik mücadele ortamının güvenlik anlayışı, klasik iç ve dış güvenlik tehditleri anlayışıyla sınırlıydı. Küreselleşmenin hızlanması ile kapital ve insan dolaşımının serbestleşmesi, ulaştırma imkânlarının gelişmesi, uluslararası ticaretin büyümesi ve internetin çok kısa sürede küresel düzeyde yaygınlaşarak sanal bir dünya oluşturması ile güvenlik ortamı çok yönlü ve çok boyutlu bir alan haline geldi. Günümüzde artık çatışmalar sınırları aşarak hızla çevresine yayılabilmekte, ölümden kaçan mülteci kitleleri başka ülkeler için yeni güvenlik sorunları yaratmaktadır.

Günümüzdeki güvenlik ortamını tanımlayan faktörleri; küreselleşmeye bağlı sınır aşan aktörler, çok kutuplu bir dünya düzeni, ulusal çıkarların tekrar ön plana çıkması, güvenlik kavramının çok geniş bir spektruma yayılması, çatışmaların nedenleriyle birlikte genişlemesi olarak sayabiliriz.[5]

Güvenlik olgusu, artık devletlerin ne bir iç meselesi olarak, ne de birbirleri arasındaki ilişkiler düzlemi kapsamında değerlendirilemeyecek bir boyut kazanmıştır. Uluslararasındaki güvenlik problemleri klasik soğuk savaş anlayışının çok ötesinde, düzensiz ve asimetrik bir boyut kazanmış, ulus devlet mekanizmalarına yönelik tehditler boyut değiştirerek artmış, iç güvenlik ihtiyaçları için devletlerin reorganizasyon çalışmaları yanında, uluslararası işbirliği de gerekli hale gelmiştir.

Artık kontrol edilemeyen mülteci dalgaları da başlı başına bir güvenlik sorunu haline gelmiştir. Güncel bir örnek olarak, Suriye'deki savaş, sınırlarının dışına taşan bölgesel bir krize dönüşmüş ve bu kriz İkinci Dünya Harbi'nden beri görülmemiş büyüklükte bir küresel mülteci dalgası yaratmıştır. Bu durum Türkiye'yi ciddi şekilde etkilerken; Avrupa'yı yaklaşık 60 yıldır adım adım yürütülen AB projesini çökertme tehdidi ile baş başa bırakmıştır.

Paradoksal olarak, çatışmalar sınır tanımadıkça ve bu çatışmaların yayılmasında sınırların etkisi azaldıkça, sınırlar aynı zamanda tekrar önem kazanmaktadır. Berlin Duvarı'nın yıkılmasından beri küresel düzeyde 40'ın üzerinde ülke, 60'dan fazla komşusuna karşı duvar inşa etmiştir. Bunlardan 15'i sadece 2015 yılında inşa edilmiştir. Avrupa'da Şengen bölgesi tehdit altındadır. Ukrayna Kırım örneğinde olduğu gibi sınırlar artık zorla değiştirilmeye başlanmış ve bu durum güvenlik ortamını daha da tehlikeli hale getirmiştir.[6]

Günümüzde eğer devlet olmazsa, ya da işlevlerinde yetersiz kalırsa; büyük ailelerin parçalanmasıyla, artık yalnızlaşmış bireylerden oluşan modern

5 Peter R. Faber: NATO's Military Transformation Past, Present, Future, NATO Defence College Occasional Paper: After Istanbul, Rome, 2004

6 Munich Security Conference 2016 Report, (Boundless Crises, Reckless Spoilers, Helpless Guardians), (www.securityconference.de/en/activities/msr), s.5.

toplumumuzda, Thomas Hobbes'un "İnsan İnsanın Kurdudur" sözü gerçekten yaşanabilir. Çünkü tüm toplum ve devletlerde, güvenlik için istihdam edilen insan sayısı tarihteki en yüksek seviyesine çıkmış olmasına; modern silah, cihaz ve teknolojilerin yaygın olarak kullanılmasına rağmen; terör, radikal akımlar ve suç örgütleriyle mücadele her geçen gün daha da zorlaşmaktadır. Terör ve suç örgütleri teknolojiden maksimum derecede yararlanarak, organize olmakta, genişlemekte ve küresel düzeyde güç oluşturabilmektedirler. Terör, kitle imha silahları, uyuşturucu kaçakçılığı, radikal dinci akımlar, sınır ötesi suç örgütleri, insan ticareti gibi olgular artık uluslararası nitelik kazanmıştır.

Devletlerin emniyet ve güvenlik için gücünü artırması, reorganizasyon çabaları ve daha önemlisi devletlerin işbirliği ve ortak mücadelesi hiç olmadığı kadar önemli hale gelmiştir. Bu bakımdan güvenlik kavramı; bireyi, toplumu, devleti ve uluslararası camiayı aynı derecede ilgilendiren, çok geniş bir anlam kazanmıştır. Güvenlik kavramının kazandığı yeni ve geniş anlam meseleyi bireyin ve toplumun bütün katmanlarının ortak sorunu ve sorumluluğuna dönüştürmektedir.[7]

Klasik veya kitle imha silahlarına dair hassas teknolojiye, hammaddeye ve uzmanlığa birkaç on yıl öncesiyle karşılaştırılamayacak kadar kolay ulaşılmaktadır.

Diğer taraftan, silah tacirlerinin faaliyetlerinin küresel ölçek kazanması, konvansiyonel silahların küresel ölçekte pazarlanabilmesi ve elde edilmelerini daha kolay hale getirmektedir.

Ülkeler dünya üzerindeki konumları her nerede olursa olsun, terör ve siber saldırılar gibi asimetrik tehditlere açık hale gelmiştir ve bu nedenle; geleneksel olmayan savunma ve saldırı yeteneklerine sahip olmak üzere yatırım yapmak durumundadırlar. Bu yatırımlar askere alma, eğitim, kariyer geliştirme konuları başta olmak üzere, gelecekteki güvenlik yapılanması üzerinde büyük değişimlere yol açacaktır.[8]

İletişim teknolojisinin sağladığı kolaylıklar, ulaştırma imkânlarının gelişmesi ve sınırların kazandığı geçirgenlik sebebiyle tüm ülkeler terörist grupların propaganda, yandaş toplama ve hücre oluşturma faaliyetlerine daha açık hale gelmektedirler.

Terör örgütleri, internet ve mobil uygulamaların sağladığı hızlı organize olma ve koordinasyon yetenekleri ile dünyanın her yerinde saldırı gerçekleştirebilecek duruma gelmiştir.

7 21. Yüzyıl Perspektifinde Türkiye'nin Güvenlik Yaklaşımı" Çalışma Grubu Raporu" ŞUBAT 2015, Cenkler Matbaası, İstanbul, (www.gif.org.tr), ss.8-9

8 Global Defense Perspectives, Mapping Prioritization and Posture in a Challenging World, Public Sector Research Center, (www.psrc.pwc.com), s.7.

Bütün bu etkenlerin sonucu; birey, grup ve devletlerin silahlara, silah olarak kullanılabilecek bilgi ve teknolojiye daha rahatça ulaşması ve dolayısıyla kitle imha silahları, konvansiyonel silahlar ile dronlar, robotik araçlar ve siber saldırı yeteneklerinin yaygınlaşması güvenlik tehdidi olgusunu küreselleştirmiştir. En büyük risk, bu kapasitenin devlet dışı aktörlerin eline geçmesidir. Bu olasılık, büyük yıkımlara yol açma riskini bünyesinde barındırmaktadır.

Diğer taraftan, güvenlik kavramı şekil değiştirirken devletlerin egemenlik kavramı da aşınmakta, şekil değiştirmektedir. Devletler küreselleşmenin etkisiyle yeni pazarlar bulma ve genişletme, doğal kaynaklara erişim, ucuz ve/veya kalifiye insan gücü temini gibi etkenlerle birbirine daha bağımlı duruma gelmiştir. Ancak bu ekonomik karmaşık ilişkilerin sonucu sınırlar ve egemenlik kavramları törpülenmiştir/törpülenmektedir.

Uluslararası Hukuk kurallarına riayet, devletlerin saygınlık ve itibarı için olmazsa olmaz bir kavrama dönüşmüş; devletlerin iç işlerine karışmama geleneğinin sınırları zorlanmaya başlanmıştır. Uluslararası kamuoyu ve duyarlılığın boyutu, bir ülkedeki herhangi bir iç olaya polisin ve yargının müdahale yöntemi ve orantısına kadar genişlemiştir. Artık egemenlik kavramı eski tanımını yitirmektedir. Bu durum devletleri tehditlerle alışılageldik mücadele yöntemlerini değiştirmeye zorlamaktadır.[9]

2. Teknolojik Gelişmeler Etkisinde Tehdit ve Risklerdeki Değişimler

Teknolojik gelişmeler ve bu gelişmelerin toplumda yaygın bir şekilde kullanımı exponansiyel olarak katlanarak büyümektedir. Elektriğin 1873'de keşfedilmesinden sonra, ABD nüfusunun % 25'inin bu teknolojiden faydalanır hale gelmesi için 46 yıl geçmişti. Bu durum büyük ölçüde kâr arayışı nedeniyle, üreticilerin hükümet ve kamusal alana yönelik direncinin yayılımı yavaşlatması sonucu oluşmuştu. Daha sonra teknolojik gelişmelerin daha geniş alanlara yaygınlaşmasının hızı artan bir ivme kazanmıştır. Mobil telefonlar için 13 yıl, internet için ise 7 yıl, ABD içinde % 25 oranında yaygınlaşmaya yeterli olmuştur. Apple iphone 2007'de üretime geçtikten sonra dört ülkede bir yılda altı milyon adet satarken; iphone 3G 2008 yılında sadece altı ayda dünya çapında ve on milyon adet satmıştır. Artık gelişme hızının artışı ve düşen maliyetler yoluyla yapısal dirençlerin etkisiz kılınması teknolojik adaptasyonda sürekli büyümeyi beraberinde getirmiştir. Yükselen talep ve bahse konu yapısal dirençlerin etkisiz hale gelmiş olması sonucu, teknolojiye yönelik açlık ve bunun üretimle doldurulması eğiliminin 2050 ve ötesine kadar devam edeceği tahmininde bulunmak oldukça gerçekçi olacaktır.

9 21. Yüzyıl Perspektifinde Türkiye'nin Güvenlik Yaklaşımı" Çalışma Grubu Raporu" a.g.e., s.5-7

Daha ilginci, teknolojik gelişmelerde liderlik artık son iki yüzyılda şahit olunanın aksine, ABD ve Avrupa dışındaki ülkelere (Güney Kore, Hindistan, Çin, Japonya, Tayvan gibi) geçmektedir.[10]

İşlemci ve bilgisayar uygulamalarındaki gelişmeler, küreselleşme ve internet temelli enformasyon ve iletişim devrimi ile teknolojinin hızla yaygınlaşması sonucu; teknoloji artan bir ivme ile gelişmektedir. Bu gelişmelere paralel olarak, bioteknoloji, bilgisayarlar, robotikler ve diğer teknoloji dalları hızla gelişecek ve yakın gelecekte askeri silah sistemlerine uyarlanacaklardır. Teknolojik gelişmeler aynı zamanda daha küçük, daha karmaşık ve entegre sistemlerin üretilmesinin de yolunu açmıştır. Bu kapsamda, artık nano teknoloji yoluyla, minik İHA'lar (İnsansız Hava Araçları) ve diğer mikro robotların üretimleri başlamış durumdadır.[11]

Teknolojinin etkisiyle yakın gelecekte uluslararası politika ve harbin çehresi büyük olasılıkla, dramatik olarak değişecektir.[12] Harp üzerinde insanın tekeli kırılmaktadır. Harpte robotların kullanılacağı yeni bir döneme girmekte olduğumuzu söylemek mümkündür. Artık savaşların devletler arasında ve konvansiyonel olarak icra edilmesi yerine; devletler ve devlet dışı aktörlerin rol alacağı, gayrinizami harp, terör, gerilla harbi, barışı koruma harekâtı gibi alanlarda olması beklenmektedir. Çatışmalarda muharebe sahasındaki askerlerin yanında büyük oranda robotik silah ve sistemleri kullanılmaya başlanacaktır.[13]

Devlet, kurum ve şahıslara karşı siber saldırılar, sanal alanın ekonomik ve sosyal olarak yaratacağı değişimler gibi birçok alan gelecekteki muharebe ve güvenlik ortamını etkileyecek, şeklini değiştirecektir.

Küreselleşmeye bağlı olarak ticaret, kapital ve insan dolaşımının serbestleşmesi yoluyla hassas teknolojilerin yayılımı hızlanmış ve silah ve silah olarak kullanılabilecek bilgi ve teknolojiye erişim kolaylaşmıştır. Bu nedenle, günümüzde devlet dışı aktörlerin, terör örgütlerinin gelişmiş klasik silahlar ve nükleer, biyolojik veya kimyasal kitlesel imha silahlarını ele geçirme olasılığı ciddi bir tehdit olarak ortaya çıkmıştır.

10 Walton, C. Dale, Geopolitics and the Great Powers in the 21st Century: Multipolarity and the Revolution in Strategic Perspective (Geopolitical Theory) Taylor and Francis.(Kindle Edition), ss.90,91

11 The Future Operating Environment 2050: Chaos, Complexity and Competition; Small Wars Journal; (http://smallwarsjournal.com/jrnl/art thefutureoperatingenvironment2050chaoscomplexityandcompetition)

12 Walton, C. Dale. a.g.e., s.88

13 Singer, P. W.. Wired for War: The Robotics Revolution and Conflict in the 21st Century. Penguin Publishing Group. Kindle Edition, ss.41,213,267

Global Trends 2030 Raporu'nun belirttiğine göre; harp araçlarının geniş bir spektrumunun, özellikle nokta vuruş, siber saldırı ve bio-teknolojik yetenek ve silahlarının elde edilmesi daha kolay bir hal almıştır. Gelecekte bireyler ve grupların daha önce sadece devletlerin tekelinde olan, büyük ölçekli şiddet yaratma ve karışıklık çıkarma imkânına ulaşacakları tahmin edilmektedir.[14]

Münih Güvenlik Raporu (2016)'na göre ise; gelecekte çatışmaların esas olarak siber alanda oluşabileceği yönünde tartışmalı iddialar olmakla beraber; siber saldırıların esas hedefinin kritik önemdeki altyapı ile hükümet, şirket ve şahıslara ait data ve bilgiler olacağı öngörülmektedir.[15]

Teknoloji aynı zamanda yıkıcı gücü yüksek yöntemlerin ucuz ve kolay üretilmesine imkân sağlamaktadır. Bio-teknolojideki gelişmelerin salgın hastalıkları tetikleyebilecek yöntemleri kolaylaştırması, üç boyutlu (3-D) üretim gibi yöntemlerin ucuzlamasıyla bazı silah veya silah nitelikli araçların üretiminin kolay hale gelmesi, önümüzdeki dönemin diğer güvenlik riskleri arasındadır.[16]

İnsansız hava araçları ile dronların temini ve silah olarak kullanımı, robot teknolojisindeki gelişmeler, yapay zekâ ve siber saldırılar önümüzdeki dönemin güvenlik ortamında ciddi risk unsuru oluşturacak konular olarak değerlendirilmekte ve müteakip bölümlerde sırasıyla incelenmektedir.

2.a. İnsansız Hava Araçları ile Dronların Temini ve Silah Olarak Kullanımı

İHA (İnsansız Hava Araçları) teknolojisi, üretimi, elde edilmesi ve en önemlisi kullanımı son 5 yılda dramatik ölçüde artmıştır.

2011 yılında yapılan bir çalışmaya göre, o yıl dünyada hükümetler, firmalar ve araştırma merkezlerince yürütülen 680 İHA çalışması mevcuttu ve bu rakam araştırmanın altı yıl öncesinde ise sadece 195 adetti.

11 Eylül saldırılarından önce ABD'de çok az sayıda ve sadece deneysel maksatlı UAV varken; bugün bu alanda en önde gelen ülke konumunda olan ABD envanterinde, 200 adedi silahlı olmak üzere, 7.000 adetten fazla UAV mevcuttur. Diğer taraftan, UAV teknolojisi devletler arasında hızla yayılmaktadır. Dünya üzerinde 86 ülke silahlı veya silahsız UAV yeteneğine sahip olmuş durumdadır.[17]

14 Global Trends 2030, "Alternative Worlds", National Intelligence Council, Aralık 2012, (www.dni.gov/nic/globaltrends)

15 Munich Security Conference 2016 Report, a.g.e., ss.46-51

16 21. Yüzyıl Perspektifinde Türkiye'nin Güvenlik Yaklaşımı" Çalışma Grubu Raporu" a.g.e., s.11

17 International Security Program, "World of Drones Report",(http://securitydata.newamerica.net/worlddrones.html)

Türkiye de, aktif olarak kullanılmaya başlanan Bayraktar TB-2, deneme testleri süren Vestel Karayel ve üretim aşamasında olan ANKA UAV'leri ile bu konuda dünyadaki sayılı ülkeler arasına girmiş bulunmaktadır.[18]

Çatışmada UAV kullanımına yönelik güncel bir örnek; Azerbaycan Ordusunun 4 Nisan 2016 tarihinde Dağlık Karabağ'da Ermeni mevzilerine yönelik İsrail yapımı Harop/Harpy[19] UAV'lerini kullanması olmuştur.[20] Azerbaycan ordusu bu sayede yarattığı sürpriz etkisi ile işgal altındaki topraklarının bir bölümünü kurtarabilmiştir.

Başta silahlı olmak üzere, UAV'lerin kullanımının devletlerin tekelinde olmaktan hızla çıkması ise asıl riski oluşturmaktadır. Artık Hizbullah, Hamas, DAEŞ gibi devlet dışı yapılar ve terör örgütleri de silahlı UAV elde ederek kullanmaya başlamışlardır.[21]

Uluslararası Güvenlik Programı (The International Security Program) Raporuna göre, DAEŞ UAV teknolojisi kullanmaktadır. Nitekim Fırat Kalkanı Operasyonu sırasında DAEŞ'in silahlı UAV saldırısı gerçekleştirmiş olması bu konudaki riski ortaya koymaktadır.[22]

Hedefleme sorunu daha basit olduğundan UAV'lerin teknolojik olarak daha az gelişmiş aktörler tarafından tercih edileceği beklenmelidir. Örneğin bir terör grubu zırhlı araçlar veya uçaklar gibi pahalı ve gelişmiş silah sistemlerine sahip olmayabilir. Ancak elde edeceği bir UAV, hedef ayrımı yapmaksızın gördüğü tüm zırhlı araçlara veya bir pistteki uçaklara hücum edebilecektir. Hatta UAV'nin ön programlanmış uçuş rotası sonrası, hedef bölgesine varması yeterli olacaktır.[23]

Terör örgütlerince kimyasal, biyolojik maddeler taşıyan UAV'lerin, özellikle sivil halka karşı kullanılmasının yaratabileceği zayiat ve psikolojik etki ise en kötü ihtimali oluşturmaktadır.

---

18 Berkan İsmet, "İnsansız hava aracı'nda öncü ülke olmaya doğru", 17.09.2016, Hürriyet, http://sosyal.hurriyet.com.tr/yazar/ismetberkan_386/insansizhavaaracindaoncuulkeolmayadogru_40225024

19 Harop kamikaze şeklinde hedefe yönelen bir UAV. Katı yakıtlı roket sistemi ile fırlatıldıktan sonra kanatları açılmakta ve pervaneli olarak uçuşunu sürdürmektedir. Hızının 185 km/saat ve seyir menzilinin 500 km. üzerinde olduğu tahmin edilmektedir. Bununla birlikte datalink bağlantısıyla kontrol edilmesi menzili 150 km. ile sınırlamaktadır.

20 Gareth Jennings, London IHS, Jane's Defence Weekly, 05 April 2016.

21 International Security Program, "World of Drones Report",(http://securitydata.newamerica.net/worlddrones.html)

22 "IŞİD Türk Askerine karşı ilk kez 'drone' kullandı", 28.09.2016, Yeniçağ, (http://www.yenicaggazetesi.com.tr/isid-turk-askerine-karsi-ilk-kez-drone-kullandi-147029h.htm

23 Cheap Technology Will Challenge US Tactical Dominance – Analysis, T.X. Hammes. NDU PRESS MAY 30, 2016.

2.b. Robot Teknolojisindeki Gelişmeler ve Yapay Zekâ

İnsansız araçlara yapay zekâ eklenmesi ile otonom çalışma imkânının sağlanması yakın gelecekte mümkün hale gelecektir. Bu kapsamda bağımsız hareket eden muharebe robotları keşif ve saldırı amaçları ile kullanılacaktır.[24]

Makineler uzun süredir harp araçları olarak kullanılmaktadır. Ancak onların nasıl kullanılacaklarına insanlar karar vermiştir. Oysa şimdi makinelerin kontrolünü ve öldürme kararlarını makinelere devretme devri gelmiştir.

Böylesi otonom robotik silah ve makinelerin diğer bir adla "katil robotların" üretilmesi on yılları değil sadece birkaç yılı alacaktır. 2015 yılında, 1000'den fazla teknoloji ve robotik uzmanı – Stefan Hawking, Tesla Motors CEO'su Elon Must ve Apple ortak kurucusu Steve Wozniak'ın da içinde bulunduğu- bu tür katil makinelerin on yıllar gibi uzun sürelerde değil, önümüzdeki yıllarda geliştirileceğini açıkladılar. Açık bir mektup yayınlayan ekip; bu konuda gelecek yıllarda yeni bir silahlanma yarışının kaçınılmaz olacağını ve otonom silahların gelecekte Kalaşnikov tüfeklerinin geçmişte yaptığı etkiyi gerçekleştireceği uyarısında bulundular.

Londra konuşlu Katil Robotları Durdurma Kampanyası yürüten bir organizasyona göre ABD, Çin, İsrail, Güney Kore, Rusya ve İngiltere çatışmalarda makinelere daha büyük otonomi verecek sistemler üzerinde çalışmaktadırlar.[25]

Bazıları çatışma alanlarında robotların kullanılmasının insanların tehlikeye atılmasının önüne geçerek, harpte insan zayiatını önleyeceği iddiasında bulunmaktadır. Bu bir ölçüde doğru olsa da; bu otonom robotik silahlar, zayiat konusunda kamuoyu baskısından kurtulacak olan hükümetlerin elini serbest bırakacak, harp için daha kolay karar vermelerine neden olabilecektir.[26]

Batı dünyasında nüfusun hızla yaşlanması ve refah toplumunun neden olduğu, hayatını tehlikeye atma isteğinin azalması olguları dikkate alındığında; robot savaşçıların dünyanın diğer bölgelerindeki genç ve savaşabilir nüfus fazlalığına karşı bir "önlem" olarak mı düşünüldüğü sorusu, üzerinde tartışılması gereken diğer bir konudur.

Mevcut durumda, yapay zekâ içermeyen, uzaktan kumandalı silahlı araçların üretimi ve kullanılması hızla yaygınlaşmaktadır. Irak Ordusu'nun DAEŞ'e karşı uzaktan kumandalı saldırı aracı geliştirmesi, Suriye hükümet güçle-

24 Walton, C. Dale, a.g.e. ss.92,94

25 New Report Calls for Ban on 'Killer Robots' Amid UN Meeting", By THE ASSOCIATED PRESS UNITED NATIONS, Apr 11, 2016.

26 Singer, P. W., a.g.e., s.318

rinin Halep'te muhaliflere karşı Rus yapımı robot saldırı araçlarını kullanması buna örnek teşkil etmektedir.[27]

2.c. Siber Saldırı

Enformasyon teknolojisi hayatın her alanına yayılmış durumdadır ve bu durum, siber saldırı ihtimalini artırmaktadır. Bu saldırıların ticari veri yanında, kritik milli altyapıyı hedef alması yüksek bir ihtimaldir. Günümüzde gelişmiş ülkeler siber yetenek ve savunmalarını geliştirmek için milyarlarca dolar tahsis etmektedirler. Ancak gelişmelerinin devamı için IT altyapısının sağlıklı işlemesine muhtaç olan gelişmekte olan ülkeler, böylesi bir kaynak ayırma güçleri olmadığından, siber saldırılara daha açık bir hedef durumundadırlar.[28]

Siber saldırı olasılığı öylesine artmıştır ki; dünyanın en gelişmiş ve güçlü devletleri dahi gruplar ve hatta bireylerden gelebilecek siber saldırı tehdidi ile karşı karşıyadırlar.

Siber saldırılar dijital olarak yönetilen, ülkenin güvenlik sistemleri, enerji şebekesi, su, iletişim, finans sistemleri, boru hatları, ulaştırma, hava trafik kontrolü ve barajları gibi kritik alt yapılara büyük darbeler vurma ve bunun sonucunda ekonomik, fiziksel ve insani felaketlere yol açma riski taşımaktadırlar.[29]

Saldırılar başka bir devletten veya devlet destekli siber saldırı grubundan gelebileceği gibi; devlet dışı aktörlerden de kaynaklanabilir. Siber saldırıların kaynağını tespit etmek çok güçtür. Bu nedenle karşılık vermenin veya cezalandırmanın pek mümkün olamaması, bu yeni tehdit alanını daha da zor hale getirmekte, aynı zamanda caydırıcı savunma yöntemlerini zayıflatmaktadır.[30]

Devletler tarafından icra edilen/ettirilen siber saldırıya güncel bir örnek olarak, 23 Aralık 2015'te Ukrayna'da 225.000 kişiyi, dondurucu kışın tam ortasında elektriksiz bırakan genel elektrik kesintisi (blackout) verilebilir. ABD Ülke Güvenlik Departmanı (Department of Homeland Security) yetkilileri, yaptıkları incelemeler sonunda, bu elektrik kesintisinin bir siber saldırı sonucunda gerçekleştirildiğini duyurmuştur. Uzmanlara göre, elektrik hatlarının

27 Iraq Is Preparing an Armed Robot to Fight ISIS,By Patrick Tucker, August 22, 2016 (http://www.defenseone.com/technology/2016/08/iraqpreparingarmedremotecontrolrobotfightisis/130935)

28 Munich Security Conference 2016 Report, a.g.e., s.51

29 The Future Operating Environment 2050: Chaos, Complexity and Competition | Small Wars Journal. (http://smallwarsjournal.com/jrnl/art/thefutureoperatingenvironment2050chaoscomplexityandcompetition)

30 21. Yüzyıl Perspektifinde Türkiye'nin Güvenlik Yaklaşımı" Çalışma Grubu Raporu" a.g.e., s.10

kesilmesine yönelik bilinen ilk başarılı siber saldırı olarak değerlendirilen bu saldırıyı, Rus "Sandworm" adında bir hacker grubu gerçekleştirmiştir.[31]

3. Savaş Strateji ve Yöntemlerindeki Gelişmeler

Geleceğin harplerinde robotlar, başta otonom görevler, istihbarat toplama faaliyetleri ve planlama görevleri olmak üzere geniş bir alanda kullanılacaktır. Harp plan, strateji ve taktikleri de buna göre geliştirilecektir.[32]

Diğer taraftan ülkeler arasında resmi ilişkiler dışında güçlenen bağlar ve silahların ulaşmış olduğu yıkım gücü çatışmaların maliyetini çok artırdığından klasik harp artık bir seçenek olarak görülmemekte, klasik harp yerine ekonomik harp, siber saldırılar, terör, yıkıcı bölücü hareketler ve gayri nizami harp tekniklerinin kullanılması tercih edilmektedir.

Bunun en güncel örneğini Suriye'deki iç savaşta görmekteyiz. Türkiye'nin en yakın müttefikleri tarafından, PKK'nın Suriye kolu olan YPG-PYD'nin, Türkiye'nin tüm uyarılarına rağmen nasıl desteklendiği; "kullanışlı bir alet" haline gelmiş olan DAEŞ'e karşı savaşın, YPG-PYD terör örgütüne alan açmak için nasıl kullanıldığı bu konudaki en güncel örneği oluşturmaktadır.

Günümüzde başvurulan diğer bir harp türü ekonomik savaştır. Devletler arasındaki mücadelelerin askeri olmaktan ziyade ekonomik alana genişlemesi nedeniyle; ekonomik güç bir dış politika aracı olarak kullanılarak siyasi hedefler gerçekleştirilmek istenmektedir.[33]

Uluslararası sermaye, özellikle cari açığını sıcak para ile finanse eden ülkelerde, tüm ekonomik dengelerin sarsıldığı ciddi kırılganlıklar yaratabilmektedir. Küresel finansın reel üretim ve ticareti desteklediği gibi, spekülatif amaçlı olarak bazı emtia piyasalarına ve sektörlere girip çıkması, ekonomiyi ve siyasi sistemi etkileyebilmektedir.

Ekonomik ve finansal yaptırımlar bir anlamda küresel düzlemde mücadelenin ve güvenlik arayışının bir yöntemine dönüşmüş durumdadır.

2015 yılındaki uçak krizi sonucu Rus yönetimince yürürlüğe sokulan ekonomik yaptırımlar, bize yönelik güncel bir örnek olarak, hafızalarımızda tazeliğini korumaktadır. Bir diğer örnek ise Kırım'ın ilhakı sonucu ABD ve AB'nin Rusya'ya karşı yürürlüğe koydukları ekonomik yaptırımlardır.

---

31 "U.S. government concludes cyber attack caused Ukraine power outage", Dustin Volz, Feb 25, 2016. Reuters Canada, (http://ca.reuters.com)

32 Singer, P. W., a.g.e., s.430

33 Blackwill, Robert D.; Harris, Jennifer M.. War by Other Means,Harvard University Press, (Kindle Edition), s.8

Diğer bir alan siber savaş ya da enformasyon ve bilgi savaşıdır. Siber saldırılar; buna başvuran tarafa, en az risk ve kayıpla oldukça önemli bir zarar verme imkânı sağlamasıyla; artık devletler tarafından sıklıkla başvurulabilecek bir harp yöntemi haline gelmiştir.

Bu kapsamda; küresel enformasyon ve iletişim teknolojileri sayesinde, propaganda malzemelerinin hızla yayılması ve böylece toplum kesimlerinin harekete geçmesi sağlanarak toplumsal hareketler/olaylar yaratılabilir. Ayrıca hassas kamusal ve şahsi bilgiler ile kritik altyapıya karşı siber saldırılarda bulunarak devlet ve toplum üzerinde çok yıkıcı hasar ve karmaşa yaratılabilir.

Tüm bu harp nevilerinin uygun bir zamanlama içindeki entegre kombinasyonu içeren Hibrit Savaş da artık gündemimize girmiş bulunmaktadır.

Harp türlerinin harp sahnesinde her zaman bir kombinasyon olarak kullanılageldiği unutulmamalıdır. Bu bakımdan, bu tabir yeni bir harp türü olarak algılanmamalıdır. ABD Milli Güvenlik Üniversitesi'nden Frank Hoffman hibrit savaşı; "Siyasi hedeflerin elde edilmesi maksadıyla; konvansiyonel silahlar, gayri nizami taktikler, terörizm ve kriminal faaliyetlerin aynı harp sahasında, uygun şekilde kombine edilerek, simultane şekilde uygulanması" olarak tanımlamaktadır.[34]

Hibrit Harp yöntemini geliştirerek etkin bir şekilde uygulamaya başlayan devlet Rusya'dır. Ancak Hibrit Savaş yöntemlerinin hızla taklit edilerek, diğer devletlerce de uygulanabileceği gözden uzak tutulmamalıdır.

Rusya 2010 Askeri Doktrini'nde modern harp; "askeri güç ve askeri olmayan güç ve kaynakların entegre bir şekilde kullanılması" ve "askeri güçleri kullanmadan siyasi hedefleri elde etmek maksadıyla; askeri güç kullanımı öncesinde, enformasyon harbi yöntemlerinin uygulanması" olarak tanımlanmıştır.[35] Rus Askeri Doktrini'ni, Rusya'nın mevcut gelişmeleri yakından takip ederek, milli hedeflerini gerçekleştirmek maksadıyla; elindeki milli güç unsurlarının uygun bir kombinasyonunu, "hibrit harp" olarak adlandırılan şekilde kullanmak için nasıl planlı olarak çalıştığını gözler önüne sermektedir.

NATO Avrupa Müttefik Komutanı Philip M. Breedlove, Rusya'nın Kırım ve doğu Ukrayna'da giriştiği hibrit faaliyetlerini şöyle tarif etmiştir. *"Şimdi Rusya'nın harbe bu hibrit yaklaşımında gördüğümüz şu; bir ülkeyi istikrarsız-*

34 A Closer look at Russia's "Hybrid War", By Michael Kofman and Matthew Rojansky, KENNAN CABLE No. 7 l April 2015. (www.wilsoncenter.org/kennan)

35 2010 Rus askeri doktrini İngilizce versiyonu,"The Military Doctrine of the Russian Federation," February 5, 2010, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

laştırmak için sahip oldukları tüm yetenekleri kullanıyorlar; enerji, finans, her türlü enformasyon harbi yöntemlerini kullanarak ortalığı karıştırıyorlar ve bu karışıklığı askeri imkânları ile istismar ediyorlar. Tıpkı şimdi Kırım'da, doğu Ukrayna'da gördüğümüz gibi, Rus düzenli ve düzensiz kuvvetleri ve birlikleri, rütbe işareti olmayan şu yeşil adamlarla bu işi yapıyorlar."[36]

Savaşa karmaşık ve hibrit bir uygulama getiren, açık veya örtülü askeri, milis ve sivil unsurların dâhil olduğu bu entegre tehdide karşı uygun ulusal karşı tedbirler ve yaklaşımlar üzerinde çalışılması gerektiği çok açıktır.

Şekil 1: Hibrit savaşta kullanılan unsurlar

Sonuç

Sonuç olarak küreselleşmenin etkisinde güvenlik kavramı genişlemiş; yeni riskler ve tehditler ortaya çıkmıştır. Artan hızla gelişen teknoloji, yakın gelecekte harp silah, araç ve gereçlerinde radikal değişimlere neden olacak ve bu değişimler beraberinde harp yöntem, strateji ve taktiklerindeki dönüşümü tetikleyecektir.

Bütün bu yeni risk ve tehditler ile harp silah ve araçlarındaki değişimler, devletlerin tedbir alma ve yeni ortama uyum sağlama konusundaki çalışmalarını hızlandırmalarına yol açacaktır.

Gelinen noktada, ulusal güvenlik politikalarının önceki "askeri tehdit

36 Munich Security Conference 2015 Report, "Collapsing Order, Reluctant Guardians", (www.securityconference.de/en/activities/msr), s.34

algılamaları" odaklı yapısının, çok daha geniş bir yelpazeyi kapsayacak şekilde geliştirilmesi ihtiyacı olduğu ortadadır.

Bu kapsamda istihbarat yapılarının re-organize edilmesi; yüksek eğitimli ve uygun yeteneklere sahip insan gücüne dayanan, profesyonel orduya geçilmesi; enformasyon harbi, siber harp, ekonomik harp, hibrit harp gibi yeni harp kavram ve uygulamalarına yönelik eğitim, teşkilatlanma ve planlama çalışmalarının yapılması gereklidir.

Alınacak tedbirlerin tehditler şekil değiştirmeden veya yeni tehditler ortaya çıkmadan hızla uygulanması başarı açısından temel faktör olacaktır. Alınacak tedbirlerin ne derece başarılı olacağını, devletlerin ve kurumların yeni güvenlik ortamına uyum sağlamadaki hızı ve etkinliği belirleyecektir. Çünkü yeni güvenlik ortamı hızla şekil ve kabuk değiştiren, asimetrik tehditleri içermektedir. Bu bakımdan; alınacak tedbirler, reaktif değil, proaktif bir zihniyetle oluşturulmalı ve tehditler oluşmadan önlem alınmasını sağlamalıdır. Bunun için güvenlik, harp nevileri, strateji ve taktiklerine yönelik fikri çalışma ve öngörü araştırmalarının yapılması, konferans ve kongrelerin düzenlenmesi faydalı olacaktır.

KAYNAKÇA

1. "Globalization and Defense", The Institute of Defence And Strategic Studies (IDSS) Conference Report, 15-16 March 2006, Singapore,
2. Küreselleşmenin Boyutları ve Etkileri, TASAM, 14.12.2006 (http://www.tasam.org/trTR/

Icerik/211/kuresellesmenin_boyutlari_ve_etkileri)

3. Yılmaz, Sait, Uluslararası İlişkilerde Güç ve Güç Dengesinin Evrimi, Stratejik Araştırmalar Dergisi 1 (01), 2008
4. "Globalization and Defense", The Institute of Defence And Strategic Studies (IDSS) Conference Report, 15-16 March 2006, Singapore
5. Peter R. Faber: NATO's Military Transformation Past, Present, Future, NATO Defence College Occasional Paper: After Istanbul, Rome, 2004
6. Munich Security Conference 2016 Report, (Boundless Crises, Reckless Spoilers, Helpless Guardians), (www.securityconference.de/en/activities/msr)
7. 21. Yüzyıl Perspektifinde Türkiye'nin Güvenlik Yaklaşımı" Çalışma Grubu Raporu" ŞUBAT 2015, Cenkler Matbaası, İstanbul, (www.gif.org.tr)
8. Global Defense Perspectives, Mapping Prioritization and Posture in a Challenging World, Public Sector Research Center, (www.psrc.pwc.com)
9. Walton, C. Dale, Geopolitics and the Great Powers in the 21st Century: Multipolarity and the Revolution in Strategic Perspective (Geopolitical Theory) Taylor and Francis.(Kindle Edition)
10. The Future Operating Environment 2050: Chaos, Complexity and Competition; Small Wars Journal; (http://smallwarsjournal.com/jrnl/art/thefutureoperatingenvironment2050chaoscomplexityandcompetition)
11. Singer, P. W.. Wired for War: The Robotics Revolution and Conflict in the 21st Century. Penguin Publishing Group. Kindle Edition
12. Global Trends 2030, "Alternative Worlds", National Intelligence Council, Aralık 2012, (www.dni.gov/nic/globaltrends)
13. Berkan İsmet, "İnsansız hava aracı'nda öncü ülke olmaya doğru", 17.09.2016, Hürriyet,
14. Gareth Jennings, London IHS, Jane's Defence Weekly, 05 April 2016.
15. International Security Program, "World of Drones Report", (http://securitydata.newamerica.net/worlddrones.html)
16. "IŞİD Türk Askerine karşı ilk kez 'drone' kullandı", 28.09.2016, Yeniçağ, (http://www.yenicaggazetesi.com.tr/isid-turk-askerine-karsi-ilk-kez-dro-

ne-kullandi-147029h.htm

17. Cheap Technology Will Challenge US Tactical Dominance – Analysis, T.X. Hammes. NDU PRESS MAY 30, 2016.
18. New Report Calls for Ban on 'Killer Robots' Amid UN Meeting", By THE ASSOCIATED PRESS UNITED NATIONS, Apr 11, 2016.
19. Iraq Is Preparing an Armed Robot to Fight ISIS,By Patrick Tucker, August 22, 2016 (http://www.defenseone.com/technology/2016/08/iraqpreparingarmedremotecontrolrobotfightisis/130935)
20. "U.S. government concludes cyber attack caused Ukraine power outage", Dustin Volz, Feb 25, 2016. Reuters Canada, (http://ca.reuters.com)
21. Blackwill, Robert D.; Harris, Jennifer M.. War by Other Means,Harvard University Press, (Kindle Edition)
22. A Closer look at Russia's "Hybrid War", By Michael Kofman and Matthew Rojansky, KENNAN CABLE No. 7 l April 2015. (www.wilsoncenter.org/kennan)
23. 2010 Rus askeri doktrini İngilizce versiyonu,"The Military Doctrine of the Russian Federation," February 5, 2010, http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.
24. Munich Security Conference 2015 Report, "Collapsing Order, Reluctant Guardians", (www.securityconference.de/en/activities/msr)