ANALİZ

ARALIK 2016 SAYI: 183

SİBER TEHDİTLERLE MÜCADELEDE FARKINDALIK VE HAZIRLIK

MERVE SEREN

SETA

ANALİZ

ARALIK 2016 SAYI: 183

SİBER TEHDİTLERLE MÜCADELEDE FARKINDALIK VE HAZIRLIK

MERVE SEREN

SETA

Uygulama: Hasan Suat Olgun
Baskı: Turkuvaz Haberleşme ve Yayıncılık A.Ş., İstanbul

SETA | SİYASET, EKONOMİ VE TOPLUM ARAŞTIRMALARI VAKFI
Nenehatun Cd. No: 66 GOP Çankaya 06700 Ankara TÜRKİYE
Tel: +90 312 551 21 00 | Faks: +90 312 551 21 90
www.setav.org | info@setav.org | @setavakfi

SETA | İstanbul
Defterdar Mh. Savaklar Cd. Ayvansaray Kavşağı No: 41-43
Eyüp İstanbul TÜRKİYE
Tel: +90 212 395 11 00 | Faks: +90 212 395 11 11

SETA | Washington D.C.
1025 Connecticut Avenue, N.W., Suite 1106
Washington D.C., 20036 USA
Tel: 202-223-9885 | Faks: 202-223-6099
www.setadc.org | info@setadc.org | @setadc

SETA | Kahire
21 Fahmi Street Bab al Luq Abdeen Flat No: 19 Cairo EGYPT
Tel: 00202 279 56866 | 00202 279 56985 | @setakahire

İÇİNDEKİLER

YAZAR HAKKINDA

Merve Seren
Bilkent Üniversitesi Siyaset Bilimi ve Kamu Yönetimi Bölümü'nden mezun oldu. Yüksek Lisans eğitimini, Başkent Üniversitesi'nde ve Erasmus bursuyla gittiği Rheinische Friedrich Wilhelms Universität Bonn'da Avrupa Birliği alanında aldı. Kara Harp Okulu Uluslararası Güvenlik ve Terörizm Bölümü'nde başladığı doktora çalışmalarının ders aşamasını burada tamamladıktan sonra tez aşamasında Polis Akademisi Uluslararası Güvenlik Bölümü'ne geçiş yaptı. "Stratejik İstihbaratın Güvenlik Stratejileri ve Politikaları Açısından Yeri ve Önemi" başlıklı teziyle doktora çalışmalarını tamamladı. 2011'de National Democratic Institute ve Freedom House tarafından yürütülen "Legislative Fellows" programına kabul edildi. 2012'de Atlantic Council tarafından "Young Atlanticist" seçilerek GLOBSEC Forum ve NATO Chicago Zirvesi'ne katıldı. 2013'te Richardson Center'ın düzenlediği "First Middle East Generational Ambassadors Summit" programına seçildi. 2015'te Atlantic Treaty Association ve NATO Public Diplomacy Division tarafından ortaklaşa düzenlenen "Youth Ministerial Meeting" programına katıldı. 2005-2015 yılları arasında TBMM'de Parlamenter Danışmanı olarak görev yaptı. Şubat 2015 itibarıyla SETA ekibine dahil olan Seren güvenlik, savunma ve istihbarat konularında çalışmalarına devam etmektedir.

ÖZET

Elinizdeki çalışma siber-uzayı bireyin ve devletin güvenliğine ilişkin tehdit algılamalarından öteye taşımakta, küresel güvenlik ortamındaki belirsizlik ve istikrarsızlığı tetikleyici başat ögelerden birisi olarak yansıtmaktadır. Bu minvalde siber-uzay alanındaki gelişmelerin günümüzde ulaştığı noktayı, bireysel ve kolektif güvenlik sorunlarına etkisi, tehdit algısının boyutu, savaş alanının sui generis karakteristiği, mücadelenin çehresi ve seyrine odaklanarak güncel vakalar üzerinden izah etmektedir. Çalışmada siber güvenlik alanının, ulusal ve global ölçekli teknolojik ve kriminolojik bir sorundan, stratejik bir meseleye evriminin serencamına da yer verilmektedir. Ayrıca yeni siber tehdit alanları ve türleri karşısında ulusal ve uluslararası/uluslarüstü düzeyde yerel ve uluslararası aktörlerin alabileceği her türlü güvenlik önlemleri, iş birliği ve koordinasyon mekanizmalarıyla birlikte hukuki ve diğer caydırıcı unsur ve uygulamaların neler olabileceği de tartışılmaktadır.

Analizde yeni siber tehdit alanları ve türleri karşısında ulusal ve uluslararası düzeyde yerel ve uluslararası aktörlerin alabileceği güvenlik önlemleri, iş birliği ve koordinasyon mekanizmalarıyla birlikte hukuki ve diğer caydırıcı unsur ve uygulamaların neler olabileceği tartışılmaktadır.

GİRİŞ

Üçüncü milenyumdaki savaş ya da silahlı mücadeleler muharebe ve çatışma meydanlarında "konvansiyonel" ve "asimetrik" unsurların birbirlerine gittikçe daha kuvvetli bir biçimde eklemlendiklerini kanıtlar niteliktedir. Bu yönüyle günümüzün harp sanatı ve stratejisi devletlerin "kara", "deniz", "hava", "hava-uzay", "siber-uzay" ve muhtemelen çok yakın bir gelecekte de "elektromanyetik spektrum üstünlüğü" şeklinde sıralanan güçlerini maksimize edebilecek imkan ve kabiliyetleri kazanmalarını zaruri kılmaktadır. Öte yandan "devlet" ve "devlet-dışı" aktörlerin eş zamanlı, münferit yahut müşterek olarak başvurdukları konvansiyonel ve asimetrik taktiklerin yarattığı (hibrit) tehdit alanları ve boyutu hesaba katıldığında mevzubahis "üstünlük alanları"ndan herhangi birisinin öncelenmesinden veya ihmalinden dikkatle kaçınılmasını gerektiren bir durum ortaya çıkmaktadır. Nihayetinde "hibrit" yapılı tehditlerin bertarafı ve önlenmesindeki etki ve etkinlik/başarı düzeyi hibrit savunma stratejilerinin mütekabilen devreye sokulmasına dolayısıyla bahse konu üstünlük alanlarının entegre ve koordine biçimde işlevsel kılınmasına bağlıdır.

Bu perspektiften yaklaşıldığında "siber-uzay" asimetrik niteliği ve bünyesinde barındırdığı geniş risk yelpazesi itibarıyla devletlerin siber tehditler karşısındaki farkındalık ve hazırlık seviyelerinin sorgulanmasını gerektiren kritik bir alandır. Öyle ki günümüzde siber saldırıların neden olabileceği tahribat "kitle imha silahları"nın (*weapons of mass destruction*) alansal etkisine eş değer bir potansiyel tehdidi bünyesinde barındırdığından bu amaçla kullanılan sistem ve cihazlar, analojik ya da metaforik bir tarzda "toplu inkıta silahları" (*weapons of mass disruption*)[1] kavramıyla ifade edilmektedir. Siber kaynaklı tehdidin savunma ve güvenlik açısından farklı ve vahim olan yönü ise ne geçmişte ne de gelecekte devletin hiçbir zaman bütünüyle kendi tekelinde bulunduramayacağı bir alanı temsil etmesidir. Zira bugün "insan" ve "teknoloji"nin buluştuğu her yer "siber yaşam alanları" olarak karşımıza çıkmakta, bu ise sadece tehdidin etki alanı ve boyutuna değil, zincir-reaksiyonu ve yayılma hızı bakımından gerçek-zamanlı, eyleme geçirilebilir önleyici tedbir ve müdahalelerin zorluğuna da işaret etmektedir.

Nitekim siber tehditlerin "dinamik" ve "asimetrik" şeklinde tasvir edebileceğimiz iki temel karakteristik özelliği, geleneksel savunma anlayışı ve metodolojisinden farklı bir yaklaşım ve karşı mücadele stratejisine dayanmasıdır. Bu nedenledir ki devletler stratejik siber savunma amacıyla genişletilmiş, güçlendirilmiş ve gizlenmiş ağ tabanlı modeller ve elektronik harp üstünlüğü kazandıracak yüksek teknoloji ürünlerine ve ileri düzey analiz yeteneklerine gittikçe artan oranda yatırım yapmaktadırlar. Elinizdeki çalışma siber-uzayı bireyin ve devletin güvenliğine ilişkin tehdit algılamalarından öteye taşımakta, küresel güvenlik ortamındaki belirsizliği ve istikrarsızlığı tetikleyici başat ögelerden birisi olarak yansıtmaktadır. Ayrıca bu yeni tehdit alanı ve türü karşısında ulusal ve uluslararası/uluslarüstü düzeyde yerel ve uluslararası aktörlerin alabileceği her türlü güvenlik önlemleri, iş birliği ve koordinasyon mekanizmalarıyla birlikte hukuki ve diğer caydırıcı unsur ve uygulamaların neler olabileceğini de tartışmaktadır.

1. Burada geçen *disruption* kelimesi elektrik ve su şebekeleri gibi sistemleri sekteye uğratmak suretiyle kesinti/aksaklık yaratılması manasındadır. İngilizce kelimenin Türkçe literatürdeki karşılığı "parçalanma, bozma, aksama, yıkım, kesme" gibi muhtelif kavramlarla tanımlansa da bu analizde doğrudan "kesilme, kesinti" anlamını ifade eden "inkıta" (alternatif bir seçenek olarak "tahrip") kavramının kullanılması tercih edilmiştir.

KÜRESEL GÜVEN(SİZ)LİK ORTAMINDA "İSTİKRARSIZLIK" VE "BELİRSİZLİK"

Küresel güven(siz)lik ortamı tehdit yelpazesinde yer alan aktör ve faktörler itibarıyla akıl almaz bir hızla değişip dönüşmektedir. Bu bağlamda devlet eliyle gerçekleştirilen ve konvansiyonel mukabeleyi zorunlu kılan taciz/işgallerin yanı sıra devlet-dışı aktörlerce yöneltilen asimetrik tehditlerle mücadeleyi zorunlu kılan muhtelif saldırılara da şahit olunmaktadır. Örneğin 2008 yılının Ağustos ayında patlak veren Güney Osetya Savaşı Rusya, Gürcistan, Güney Osetya ve Abhazya arasında vuku bulan kısa süreli bir savaş olarak algılanmışsa da hakikatte Kafkasya bölgesinin geleceğini derinden etkileyen köklü bir değişime işaret etmektedir. Keza Kafkasya'daki güven(siz)lik ortamını yansıtması açısından 1994'teki ateşkese rağmen çözüme kavuşturulamayan, aksine gittikçe derinleşip çıkmaza giren Dağlık-Karabağ sorunu nedeniyle 2016 Nisan'ının ilk haftası Azerbaycan ile Ermenistan askeri güçleri arasında cereyan eden sınır hattındaki şiddetli silahlı çatışmalar da göz önünde bulundurulmalıdır.

Etnik, dinsel, dilsel, siyasi egemenlik, teritoryal özerklik gibi farklı saikler barındıran tarihsel sorunlara yönelik kısa ve orta vadeli çözüm arayışlarının yerini yeniden silahlı güç kullanımına devredebileceğini ifade eden "don(durul)muş çatışma" (*frozen conflict)*[2] kavramına karşılık gelecek çok sayıda örnek saymak mümkündür. Güney Osetya ve Dağlık-Karabağ'ın haricinde Kırım, Ukrayna, Kosova, Kore, Çin, Tayvan, Hindistan, Pakistan gibi farklı aktörlerin başrolü oynadığı, ne taraflar arasında ne de uluslararası toplum nezdinde barışçıl şekilde çözümlen(e)memiş, sıcaklığını hiçbir zaman yitirmemiş, koşullara ve duruma göre patlamaya hazır nitelikte don(durul)muş çatışmalardan bahsedilebilir.

Bu noktadan hareketle Rusya özelinde kabaca temas edebileceğimiz bir kısım gelişmeler küresel ve bölgesel güvenlik ortamı hakkında daha somut ve aydınlatıcı bir fikir verecektir. 2008'deki Güney Osetya Savaşı'nı müteakip süreçte 2014 yılında Kırım ilhak edilmiş, hemen akabinde de Ukrayna krizi zuhur etmiştir. 2015 Eylül ayından itibaren ise Moskova Suriye'deki iç savaşa doğrudan ve yoğun biçimde fiilen müdahil olma kararı almıştır. Suriye'ye intikal eden birliklerle kara, deniz ve hava kuvvetlerini destekleyecek her türlü teçhizat, donanım, mühimmat ve silah sisteminin sevkiyatı harekat alanını dönüştürdüğü için savaşan tarafları da farklı bir pozisyon almaya itmiştir.

Rusya'nın Suriye'deki çatışmalara bilfiil müdahil olmasıyla birlikte en basitinden Lazkiye yakınlarındaki Hmeymim Hava Üssü'nde S-300 ve S-400 hava savunma sistemleri konuşlandırılırmıştır.[3] Ayrıca Rus donanmasının lojistik noktası Tartus Limanı'nda uzun menzilli yüksek irtifa hava savunması sağlayan Rif-M (Fort) silah sistemini taşıyan Slava (Project 1164 Atlant) sınıfı güdümlü füze kruvazörü "Moskva" dahil, deniz gücünü oluşturan en etkili ve gelişmiş teknolojiler demirlenmiş vaziyettedir.[4] Ancak Gürcistan, Kırım, Ukrayna ya da Suriye'deki gelişmeler, Kremlin'in dış politikasının sadece "saldırgan", "işgalci", "rövanşist", "öngörülemez" veya "yayılmacı" sıfatlarıyla yorumlanmasından çok daha kritik bir mahiyet arz etmektedir. Zira buradaki esas mesele Putin Rusya'sının agresif, baskıcı ve müdahaleci tutumu değil, bölgesel ve küresel ortamdaki "güvensizlik", "istikrarsızlık" ve "belirsizlik" halidir. Nitekim

2. "Don(durul)muş çatışma" konusu üzerine yayımlanan güncel bir rapor için bkz. Agnia Grigas, *Frozen Conflicts: A Tool Kit for US Policymakers*, ikinci baskı, (Atlantic Council, Washington: Temmuz 2016).

3. "'S-300, S-400 Air Defenses in Place': Russian MoD Warns US-Led Coalition not to Strike Syrian Army", RT, 6 Ekim 2016, https://www.rt.com/news/361800-russia-syria-usa-aistrikes/, (Erişim tarihi: 19 Aralık 2016).

4. Christopher Harress, "Syrian Civil War: Russian Navy Base Tartus in Syria Giving NATO Cause for Concern While Helping to Prop Up Assad Regime", International Business Times, 16 Eylül 2015, http://www.ibtimes.com/syrian-civil-war-russian-navy-base-tartus-syria-giving-nato-cause-concern-while-2092371, (Erişim tarihi: 19 Aralık 2016); "Russia Plans Permanent Naval Facility in Syrian Port of Tartus-MoD", RT, 10 Ekim 2016, https://www.rt.com/news/362209-russian-permanent-naval-facility-tartus/, (Erişim tarihi: 19 Aralık 2016).

Rusya özelinden hareketle mevzubahis gelişmeler ışığında küresel güvenliğin mevcudiyeti ve geleceğine ilişkin bazı çıkarsamalarda bulunabiliriz.

İlk olarak İkinci Dünya Savaşı'nın ardından Birleşmiş Milletler (BM) eliyle ve çabasıyla uluslararası sistemde tesis edilmek istenen kalıcı barış ve istikrarın özellikle Rusya ve Amerika Birleşik Devletleri (ABD) arasındaki ezeli rekabetin bir yansıması olarak bizatihi BM Güvenlik Konseyi'nin daimi üyeleri tarafından ihlal/istismar edilmesidir. Bu yönüyle BM ve NATO gibi uluslararası ve bölgesel ittifakların "geçerliliği" ve imzacı taraflar üzerindeki "bağlayıcılığı" ziyadesiyle tartışmalıdır. Dolayısıyla "devletler (uluslararası) hukuku" ile "iç hukuk" arasındaki "uyum" ve "tamamlayıcılık" ilkesi kadar çok taraflı uluslararası sözleşmelere atılan imzaların söylemden öte (ya da iyi niyet gösterisi olmasının ötesinde) fiiliyatta nasıl ve ne kadar bir "yaptırım gücü" taşıdığı da sorgulanmadır. Bu minvalde Yugoslavya'dan Bosna Hersek'e, Afganistan'dan Irak'a, Yemen'den Suriye'ye, Gürcistan'dan Ukrayna'ya uzanan işgal ve savaşlarda gerek üye devletlerin BM'nin hüküm ve kurallarına riayet edip etmedikleri, gerekse NATO'nun müttefiklerine vaat ettiği ortak savunma mekanizmasının işleyişi ve fonksiyonelliği şüphe ve eleştiriye açıktır.

İkincisi devletlerin taraf oldukları iki veya çok taraflı anlaşmalar, örf ve adet hukuku (teamül kuralları), uluslararası hukukun bağlayıcılığı ve bölgesel/uluslararası ittifakların sunduğu güvenceler üzerinde yaşanabilecek tüm tartışmalar bir tarafa küresel barış ve istikrarın tesisi hakikatte bir ütopyadan ibarettir. Ancak halihazırda yaşanan iç savaş ve çatışma alanlarına bakarak bu hakikatin nedeni "coğrafyanın kaderinde" aranmamalıdır. Başka bir deyişle küresel güvensizlik ortamının failleri ve sorumluları ne Angola, Eritre, Nijerya, Etiyopya, Somali ve Sudan gibi Afrika ülkeleri ne Afganistan, Pakistan, Myanmar/Burma, Tayland ve Filipinler gibi Asya kıtası aktörleri ne de Irak, Suriye ve Yemen gibi Ortadoğu'daki devletlerdir.

Burada asıl referans alınması gereken "taraflar" değil, çatışmayı/savaşı "tetikleyici faktörler" olmalıdır. Yani esas mevzu "kimin kimle savaştığından" ziyade "savaşların niçin kaçınılmaz kabul edilmesi" gerektiğine dairdir. Etnik milliyetçilik, bağımsızlık hareketleri, toprak iddiaları ya da sınır anlaşmazlıkları, dini fundamentalizm gibi çok çeşitli saiklerle ortaya çıkacak muhtelif türdeki savaşlara dünyanın farklı koordinatlarında ve tarihin her döneminde rastlayacağımız kuvvetle muhtemeldir. Açık ve net olan ise en temelinde insanoğlu ve haliyle ülkeler için yaşamsal öneme haiz bir husus olarak yeraltı ve yerüstü kaynaklarının ele geçirilmesi arzusudur. Su, enerji, petrol gibi dünyadaki kullanılabilir doğal kaynakların daralması, tahribatı, kısıtlılığı, verimliliğin düşmesi, kullanım maliyetinin artması gibi unsurlar hesaba katıldığında "kaynakların erişimi ve paylaşımı" nedeniyle savaşların sona ermeyeceği aşikardır. Bu minvalde Kuzey Atlantik'ten ve Karadeniz'den Ortadoğu'ya uzanan askeri müdahaleler "reel politik" anlayışı yansıtan dış politika hamleleri, uluslararası sistemdeki büyük güçlerin enerji kaynakları üzerindeki hakimiyet mücadelesinin bir nevi tezahürü olarak addedilmelidir.

Küresel güven(siz)lik ortamı tehdit yelpazesinde yer alan aktör ve faktörler itibarıyla akıl almaz bir hızla değişip dönüşmektedir.

Üçüncüsü günümüzde ve gelecekte konvansiyonel savaşların geçerliliğini ve güncelliğini yitirmediği/yitirmeyeceğidir. Halihazırdaki kırsal, yerel ve bölgesel ölçekli çatışmalar ile iç savaşların yapısı ve seyri hasebiyle devlet ve devlet-dışı aktörlerin eklemlenmiş rolleri, KİS'lerin imha-etki gücü, İHA'ların istihbarat ve saldırı amaçlı yoğun kullanımı, askeri hedeflerin uzaktan kumandalı el yapımı patlayıcı bombalarla vurulması, sivillere yönelik toplu katliam amacıyla düzenlenen intihar saldırıları gibi araç ve yöntemler daha

fazla ön plandadır. Her ne kadar bugün sıklıkla "düşük yoğunluklu çatışmaları" ya da "vekalet savaşları"nı telaffuz etsek de iki veya daha fazla sayıdaki devletin düzenli ordularının muharebe halinde bulunduğu, silah sistemleri ve harekat alanındaki taktikler itibarıyla konvansiyonel nitelikteki savaşlardan soyutlanmış da değiliz.

Örneğin don(durul)muş çatışma kapsamında zikrettiğimiz Dağlık-Karabağ sorunu, Kafkasya'daki "toprak talebi" saikiyle Azerbaycan-Ermenistan cephesindeki silahlı çatışmaların yoğunlaşmasından tedirgin olan Gürcistan'daki askerileşme sürecini tetikleyici bir rol oynamıştır. Keza Moskova-Kiev çatışması, Kremlin'in Kaliningrad'da en gelişmiş uçaksavar ve füzesavar füze sistemleri dahil, silahlarını ve birliklerini konuşlu vaziyette tutup "anlık tatbikat" faaliyetleri yürütmesiyle birlikte Polonya ve Baltık ülkeleri için öncelikli tehdit algısı Rusya merkezli/odaklı seyretmeye başlamıştır. Öyle ki Avrupa'da yeniden Soğuk Savaş dönemine geri dönüşün sinyallerini verircesine NATO misyonlarına (örneğin Baltic Air Policing) ek olarak ABD, Polonya ve Baltık devletlerini hava (F-15 savaş uçakları sevkiyatı) ve deniz (Karadeniz'de aralıksız seyir icra eden savaş gemileri sevkiyatı) unsurlarıyla destekleme faaliyetlerine girişmiştir. Zaten 2016 Temmuz'unda gerçekleşen Varşova Zirvesi'nde de mutabık kalındığı üzere Kuzeydoğu kanadına 4 tane çok uluslu harbe hazır tabur gönderilmesi kararlaştırılmış, 26-27 Ekim tarihlerinde Brüksel'de düzenlenen NATO Savunma Bakanları Toplantısı'nda Estonya, Letonya, Litvanya ve Polonya'ya konuşlandırılacak askeri birlikler ile savunma kabiliyetlerinin güçlendirilmesine yönelik mevzubahis taahhütlerin uygulama safhasına ilişkin detaylı planlamalar yapılmıştır.[5]

Nitekim Ukrayna krizi ve müteakip süre zarfında Polonya ve Baltık'ta konuşlandırılan askeri birlik ve sistemler, çatışma alanının şartlara ve ihtiyaçlara istinaden yer ve yön değiştirebileceğini, birtakım önceliklerin Ortadoğu'dan Avrupa'ya kaydırılabileceğini göstermiştir. Bundan da mühimi mevzubahis gelişmeler NATO'lu müttefikler için Avrupa'da halen konvansiyonel mukabelede bulunmanın gerçekçi bir ihtimal olarak masaya yatırılabileceğini kanıtlamıştır.

Peki küresel ölçekte güvenlik, barış ve istikrarın tesisi açısından "çatışma/savaşların çehresi", "harekat alanının yeri ve yapısı", "devlet ve devlet-dışı aktörlerin rol ve sorumluluğu" ne derecede önem arz etmektedir? Başka bir deyişle modern zamanlarda teknolojik inovasyon, savaşın taktik ve stratejilerini değiştirip dönüştürdüğüne göre "harbin beşinci boyutu" olarak tanımlanan siber-uzay alanında (devlet/devlet-dışı aktörler tarafından) yeni yeteneklerin kazanılması ve inisiyatiflerin ele geçirilmesi, ulusal ve küresel güvenliği nasıl ve hangi düzeyde tehdit etmektedir?

GÜVENSİZLİĞİN VE BELİRSİZLİĞİN YENİ CEPHESİ: "SİBER YAŞAM ALANLARI"

Yukarıda kabaca resmettiğimiz küresel güvenlik tablosuna daha kapsayıcı ve bütüncül bir pencereden bakabilmek için "siber-uzay" alanındaki gelişmelere mutlaka değinilmelidir. Zira küresel ve bölgesel ölçekteki gelişmeler ışığında sadece yükselen "istikrarsızlık" ve "güvensizlik" değil, aynı zamanda gittikçe bulanıklaşan bir "belirsizlik" de söz konusudur. Nitekim giderek artan ve derinleşen belirsizlik hali karakteristik özellikleri itibarıyla siber-uzay alanında daha fazla ön plana çıkmaktadır. Bu nedenle "siber güvenlik" tehdidi ve bilahare, aynı zamanda her yerde var olma ve hiçbir yerde bulunmama güç ve özelliğine haiz "siber savaş"ın mahiyeti ve maliyeti hakkında birkaç hususun altı çizilmelidir.

Günümüzde "insan" ve "teknoloji"nin daha önce hiç olmadığı kadar hızlı ve beklenmedik biçimlerde yakınlaşıp buluştuğuna şahit olunmak-

5. Brooks Tigner, "NATO Agrees Force Deployments for Eastern Flank", *IHS Jane's Defence Weekly*, 27 Ekim 2016.

tadır. Tesla'nın arabalarına radar entegre etmesi, Delta Havayolları'nın mikroçiplerle bagajların izini sürmesi veya akıllı kontrol teknolojisi sayesinde evdeki enerji tüketiminin kontrol edilebilmesi bu hususa örnek mahiyettedir. Siber güvenlik ve beşeri faaliyetlerin günlük hayattaki kesişimi ve yoğunluğu doğrultusunda "siber yaşam alanları" (*cyber life zones*) ortaya çıkmakta, bu da siber güvenliğin kamu güvenliği perspektifi üzerinden irdelenmesi zaruretini doğurmaktadır. Örneğin 2016 Nisan'ında Atlantik Konseyi bünyesinde siber-uzay alanındaki çatışma, rekabet ve uluslararası iş birliği meselelerine odaklı çalışmalar yürüten "Siber Yönetim Girişimi"nin (*Cyber Statecraft Initiative*-CSI)[6] direktörlüğüne getirilen Joshua Corman, siber yaşam alanlarının ayrıştırılmasına yardımcı üç anahtar özellikten bahsetmektedir.

Birincisi siber güvenlik zafiyet/hatasının can kaybına neden olabileceğidir. Mesela Şubat 2016'da Hollywood Presbiteryen Tıp Merkezi fidye yazılımı (*ransomware*) mağduru olmuş, hacker/korsanlar farkında olmadan tesadüf eseri elektronik sağlık kayıt sistemine takılmışlar, zararlı kodun otomatikman devreye girmesi üzerine hastane çalışanları 17 bin dolarlık fidye yatırılana kadar sistem dışı bırakılmışlardır.

İkincisi siber güvenlik hatalarının temel sistemlerde güven kaybına yol açabileceğidir. Siber yaşam alanları siber suçlular (*cyber criminals*)[7] için "saldırı yüzeyini" fazlasıyla genişletmiştir ki en basitinden güvenlik araştırmacıları, modern otomotiv sistemlerine sızma yeteneğinin kazanıldığını ispatlamışlardır. Mesela sürücülerin arabanın tekerleklerinin kimler tarafından kontrol edildiğini bilmemeleri ilk sırada güvenilmesi gereken sistemlere karşı duyulan itimadın kaybolması manasına gelecektir.

Üçüncüsü siber güvenlik başarısızlığı finansal piyasalara inancı ciddi oranda zedeleyebileceği gibi vatandaşlarını koruma kabiliyet/yetkinliği açısından hükümete duyulan güvenin de fazlasıyla yara almasına sebep olabilecektir. Bu yüzden nükleer güç santralleri, federal bankalar ve elektrik şebekelerini korumanın çok daha ötesinde havacılık, otomotiv, sağlık, enerji[8] gibi siber yaşam alanlarına dahil tüm sistemlere özgü olarak tasarlanmış ulusal düzeyde stratejiler ve en iyi endüstri uygulamalarını kapsayan bir yaklaşım benimsenmelidir.[9]

Dikkat çekilmesi gereken son bir husus olarak günümüzde sık sık "çift maksatlı kullanım" (*dual-use targets*) şeklinde zikrettiğimiz teknoloji ürünleriyle hem "askeri" hem "sivil" amaçlara hizmet edilmesi kast edilmektedir. İşte bu noktada "siber savaş", siber-uzayın, "kendisine özgü doğası", yani "sui generis karakteri"yle ayrışmaktadır. Teknik tabiriyle "sivil ve askeri alt yapılar arasındaki sistemik bağlantısallık" (*systemic interconnectivity*) açısından farklı bir görüntü sunmaktadır ki uydular, yönlendiriciler, iletkenler/kablolar, sunucular ve hatta bilgisayarların tümü çift mak-

6. CSI programı nezdinde yürütülen projeler ve yayınlar için bkz. "Cyber Statecraft Initiative", Brent Scowcroft Center on International Security, Atlantic Council, http://www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft.

7. Örneğin bugün siber suçlular sadece internet vasıtasıyla online olarak banka hesap bilgilerine ulaşıp kendi hesaplarına para transfer etmemekte aynı zamanda doğrudan bankamatiklere de sızabilmektedirler. Örneğin Tayvan ve Tayland'daki ATM makinelerine Malware virüsü vasıtasıyla girip anında milyonluk nakit parayı çalmışlardır. Ancak hackerlar sadece Tayvan ve Tayland'da değil Ermenistan, Bulgaristan, Gürcistan, Estonya, Moldova, Kırgızistan, Malezya, İspanya, Polonya, Hollanda, İngiltere, Rusya gibi birçok ülkedeki ATM'leri hedef almaktadırlar. Mesela Rus siber güvenlik şirketi Group IB'ye göre, bu yıl Avrupa genelinde 12'den fazla ülkedeki ATM'lere nakit para verecek şekilde kötü amaçlı yazılım ile uzaktan saldırı düzenlenmiştir. Bkz. Jim Finkle, "Hackers Target ATMs Across Europe as Cyber Threat Grows", Reuters, 21 Kasım 2016, http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q, (Erişim tarihi: 19 Aralık 2016).

8. Örneğin "Tropic Trooper Harekatı" adı verilen siber espiyonaj operasyonu Tayvan'da hükümet kuruluşlarının yanı sıra ülkenin enerji sektörünü de hedef almaktadır. İlk defa geçen yıl Trend Micro tarafından analiz edilen Tropic Trooper Operasyonu'nun 2012 yılı ve hatta daha öncesinde de faal olduğu düşünülmekte, Tayvan'daki bakanlıkları ve ağır endüstrileri, Filipinler'de ise orduyu, askeriyeyi hedef aldığı kaydedilmektedir. Örneğin yakın zaman önce Palo Alto Networks tarafından izlenen hadisede siber casusların Tayvan'ın yürütme erkine ve fosil yakıt tedarikçisine saldırı düzenlediği gözlemlenmiştir. Eduard Kovacs, "Cyberspies Target Taiwan Government, Energy Sector", Security Week, 23 Kasım 2016, http://www.securityweek.com/cyberspies-target-taiwan-government-energy-sector, (Erişim tarihi: 19 Aralık 2016).

9. Ian Fairchild, "Protecting Cyber Life Zones", 17 Ekim 2016, Atlantic Council, http://www.atlanticcouncil.org/blogs/new-atlanticist/protecting-cyber-life-zones, (Erişim tarihi 19 Aralık 2016).

satlı kullanılan siber faaliyetlerdir. Örneğin herhangi bir bilgisayarın askeri mahiyeti/niteliğine ilişkin karar verilmesi gerektiğinde bilgisayarın donanım (*hardware*) bileşenleri ve özelliklerinden ziyade bilgisayarda kullanılan yazılım (*software*) programı (eğer deşifrasyon kodları, zararlı veri paketlerinin iletimi vb. faaliyetler amacıyla kullanılıyorsa) göz önünde bulundurulmaktadır. Buna mukabil "askeri veri depolama" havuzunun oluşturulması gibi bilgisayarların tamamen meşru gerekçelere dayanan askeri hedeflere hizmet etmesi de söz konusudur.[10]

Siber yaşam alanları bize ne tür risk ve tehditlerle karşılaşabileceğimiz ve bunların ne kadar yüksek bir maliyet getirebileceğine dair temel bir fikir vermektedir. Öte yandan siber saldırıların önceden tespit edilemeyen risk seviyesinin olası yüksek maliyetinden kaçınmak adına örneğin bankalar, orta ve büyük ölçekli firmalar tarafından her geçen gün çok daha fazla sayıda sigorta şirketinin kapısı çalınmaktadır. Ancak kişilerin/grupların/şirketlerin/sektörlerin yaşayacakları mağduriyet veya ödeyecekleri bedel kadar devletlerin "siber savaş" karşısında yenilgiye uğramaları halinde ne olacağı, kansız savaşların ne denli büyük ve derin yaralar meydana getirebileceği de ayrıca incelenmelidir. Bilgi ve iletişim teknolojisindeki gelişmeler kendiliğinden modern zaman harbini ortaya çıkartmıştır ki günümüzde devletler silah envanterlerindeki "siber arsenalin" mevcudunu ve gücünü hızla artırma çabası içerisindedirler. Bugün siber savaş "kara", "deniz", "hava" ve "uzay"ın ardından "harbin beşinci boyutu"[11] olarak tanımlanmakta, siber dünya savaşın yeni fakat belki de en acımasız ve zor cephesini teşkil etmektedir.

ÜÇÜNCÜ MİLENYUMDA HARBİN BEŞİNCİ BOYUTU: "SİBER PEARL HARBOR" GELİYOR MU?

Üçüncü milenyum "siber savaşlar"ın bir rüya değil, yakın gelecekte devletlerin kaçınılmaz bir şekilde sürüklenecekleri muharebe meydanı olacağına işaret etmektedir. Eski CIA Başkanı ve Savunma Bakanı Leon Panetta'nın 2012 yılında yaptığı bir konuşmada Amerikan halkını "siber Pearl Harbor" konusunda ikaz etmesi, terörist bir grup yahut düşman devlet tarafından yöneltilebilecek muhtemel bir siber savaşla kısa veya orta vadede yüzleşmek zorunda kalınacağı gerçeğiyle ilişkilidir. Her ne kadar 1991 yılında siber uzmanı Winn Schwartau "Elektronik Pearl Harbor" kavramını literatüre kazandırıp erken uyarıda bulunmuşsa da yahut Panetta'nın öngörüsü henüz gerçekleşmemiş, devletler fareleri gerçek silah olarak kullanıp birbirlerine stratejik sürpriz saldırılar düzenlememiş olsalar da siber tehdidin artık WikiLeaks sınırlarına hapsedilemeyeceği aşikardır.[12]

Nitekim 21. yüzyılda hipersonik füzeler, hayalet uçaklar, insansız hava araçları, siber, lazer ve uzay silahlarındaki teknolojik gelişmeler savaşın mekanı, zamanı ve aktörleri itibarıyla uğradığı dönüşümü gözler önüne sererken "hava-uzay, siber-uzay ve elektromanyetik spektrum üstünlüğü" güç mücadelesindeki öncelik sıralamasında gittikçe daha fazla önem kazanmaktadır. Ancak mevzubahis alanlardaki gelişmeler "kara" ya da "deniz" üstünlüğüne verilen değerin azalması anlamına da gelmemektedir. Dolayısıyla askeri harekatların başarısında belirleyici faktörler olarak sırasıyla "kara üstünlüğü", "deniz üstünlüğü", "hava üstünlüğü" ve "bilgi üstünlüğü" mevcut önem ve konumlarını

10. Elizabeth Mavropoulou, "Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks", *Journal of Law & Cyber Warfare*, Cilt: 4, Sayı: 2, (Sonbahar 2015), s. 45.

11. Kavrama ilişkin olarak bkz. "Cyberwar: War in the Fifth Domain", *The Economist*, 1 Temmuz 2010; Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends, Memorandum* (Institute for National Security Studies (INSS), Sayı: 117), Mayıs 2012, p. 10.

12. Neal Pollard and Matthew G. Devost, "Is Cyberwar Turning Out to Be Very Different From What We Thought?", Politico, 6 Ağustos 2016, http://www.politico.com/magazine/story/2016/08/is-cyberwar-turning-out-to-be-very-different-from-what-we-thought-214136#ixzz4OClXKt1y, (Erişim tarihi: 19 Aralık 2016).

sürdürmeye devam ederlerken "hava-uzay üstünlüğü" ve "siber-uzay üstünlüğü"ne ilave olarak bunlara "elektromanyetik spektrum üstünlüğü" anlayışı eklemlenmiştir.[13]

Kısaca günümüzün ve geleceğin harekat ortamındaki başat unsurlardan birisi siber-uzay olup bu alandaki imkan ve kabiliyetler her geçen gün çok daha kritik hale gelmektedir. Ne var ki "siber savaş", konvansiyonel savaştan tamamen farklı ve özgün bir yapı barındırdığı için bu alandaki "savunma" ve "saldırı" kabiliyetlerinin kazanılması da daha çetrefilli bir hal almaktadır.

Bu aşamada siber savaşın beş karakteristik özelliğine dikkat çekilmelidir. Birincisi siber-uzay alanında kullanılan silahlar bir ülkeyi harabeye çevirebilecek donanıma haiz olduğundan "gerçek" bir harptir. İkincisi saldırının başlangıcıyla etkisi arasındaki zaman aralığını ölçmeye imkan tanımayacak kadar "ışık hızında" seyretmektedir. Üçüncüsü bilgisayar veya sunuculara yönelik düzenlenen herhangi bir örtülü saldırı kısa sürede birçok ülkeyi muharebenin içerisine çekebilecek kadar anlık ve hızlı bir yayılma etkisi gösterebildiğinden "küresel"dir. Dördüncüsü "geleneksel muharebe meydanına çıkmadan" dünyanın herhangi bir noktasında bulunan düşman ülkenin savunma sistemi ve kritik altyapısı siber-uzaydan kolaylıkla imha edilebilir. Beşincisi "savaş haliyle barış zamanı" bütünüyle iç içe geçtiğinden belirsizlik ve böylece istikrarsızlık durumu çok daha tehlikeli bir boyuttadır.[14]

Görüldüğü üzere hasım addedilen devletler siyasi, askeri ve ekonomik yönlerden zarara uğratılmak istenildiğinde borsa ve bankacılık sistemleri, elektrik ve su şebekeleri, askeri tesisleri ya da kritik altyapıları siber saldırılara hedef olabilmektedir. Kaldı ki devletler doğrudan veya dolaylı yollarla endüstriyel, ekonomik, ticari vb. ihtiyaç, çıkar ve amaçlara yönelik istihdam ettikleri hackerlar aracılığıyla, siber casusluk faaliyetlerine de başvurabilmektedirler. Rusya, ABD, Çin ve kısmen Kuzey Kore arasında cereyan eden siber savaş türleri, bu duruma örnek mahiyettedir. Öyle ki 2014'te Hollywood dahi siber saldırılardan nasibini almış Kuzey Kore lideri Kim Jong-un'la dalga geçen (suikast komplosu tertiplemek gibi) satirik komedi türü "The Interview" filmine şiddetli tepki gösteren Koreli korsanlar Sony Pictures şirketinin bilgisayar sistemlerini hacklemişlerdir. Korsanlar Sony şirketine ait beş yeni film, senaryolar, e-mail trafiği vb. önemli verileri internet ortamında paylaşırlarken Sony'nin filmin New York galasını iptal etmesi, hatta filmin sinema gösteriminin kısıtlanması kararı "Hackerlar savaşı kazandı, mutlak başarı ve zafer elde ettiler" şeklinde yorumlanmıştır.[15]

Yakın geçmişten bir başka örnek ise 21 Ekim 2016'da ABD'de başlatılan "tarihinin en büyük ve en güçlü siber saldırısı" olarak nitelenen ve diğer ülkelerde de etkileri görülen "DDoS saldırıları" siber saldırıların yol açabileceği zararların boyutunu ve dolayısıyla "siber güvenlik" konusunun önemini bir kez daha gözler önüne sermiştir. Söz konusu siber saldırıdan etkilenen bütün şirketlerin, kullanıcılarına internette bir siteyi bulabilmesini kolaylaştıran hizmetler sağlayan "DynDNS" adlı firmanın müşterisi olduğu açıklanmıştır. Saldırı DynDNS'nin "DDoS" akronimiyle bilinen "Dağıtık Servis Dışı Bırakma" (*Distributed Denial of Service*)[16] verilerine boğulmasıyla başlamıştır. Bu da mevzubahis hizmeti kullanan internet kullanıcılarının aradıkları

13. Cengiz Karaağaç, *Geleceğin Hava Kuvvetleri: İHA Sistemleri Yol Haritası 2016–2050*, (Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. (STM) Yayınları, Ankara: Ocak 2016), s. 25.

14. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (Harper Collins, New York: 2010), s. 30-31.

15. "The Interview: A Guide to the Cyber Attack on Hollywood", BBC, 29 Aralık 2014.

16. Bilgi sistemlerinin servis vermesini engelleyen DDoS saldırıları çok sayıdaki bilgisayardan bir sisteme e-mail göndererek belirli bir ağ trafiğinin yönlendirilmesiyle gerçekleşmekte, internet bağlantısı yahut sunucu, bu ağır trafiği kaldıramadığından çalışamaz hale gelmektedir. DDoS saldırıları çoklu sistemlerde hedef sistemin kaynakları ya da bant genişliği istilaya uğradığı zaman oluşmakta, öyle ki bazı durumlarda saldıran bilgisayar sayısı yüz binleri bulabilmektedir. Kısaca bir veya birden fazla web sunucusunu hedef alan saldırganlar çeşitli yöntemler kullanarak sistemleri bağdaştırmakta, çok sayıda bilgisayar üzerinden istekler gönderilerek sürekli meşgul edilen sunucu da siteye erişmeye çalışan kullanıcılarına yoğunluktan dolayı yanıt verememektedir.

sitelere ulaşmalarını güçleştiren bir etki yaratmış ve ülke genelinde internet hızını düşürmüştür. Saldırının ilk etkisi kullanıcıların Twitter, Amazon, Reddit, Pinterest, Etsy, Github, Soundcloud, Spotify, Netflix, PayPal başta olmak üzere 80'i aşkın popüler siteye erişimini zorlaştırmak olmuştur ki DynDNS'nin çok sayıda firma tarafından dünya çapındaki kullanıcılar için "bir küresel adres rehberi" gibi kullanılması saldırıyı haliyle çok daha etkili ve yaygın kılmıştır.[17]

Ayrıca 2016 Kasım'ındaki ABD Başkanlık seçimleri öncesinde kamuoyunun açık erişimine sızdırılan gizli yazışma ve belgeler üzerindeki tartışmalar süregiderken Demokratik Ulusal Komite'nin (DNC) bilgisayar sistemlerine düzenlenen siber saldırıların akabinde Hillary Clinton'ın, Cumhuriyetçi rakibi Donald Trump'ı Kırım'ın ilhakına destek verip Rus devleti hackerları ile iş birliği yapmakla suçlaması oldukça çarpıcıdır. Nitekim 8 Kasım'daki ABD Başkanlık seçiminde Trump'ın ipi göğüslemesine büyük destek veren ve galibiyeti ilk kutlayan Kremlin, 18 aylık seçim maratonu süresince Rus hackerlar aracılığıyla ele geçirip medyaya servis ettiği birtakım gizli veriler/bilgiler sayesinde Clinton'ın ulusal kamuoyu nezdindeki kredibilitesini tahminlerin çok daha ötesinde zedelemeyi başarmakla itham edilmiştir.[18]

17. "Dev Siber Saldırı Twitter Dâhil Birçok Siteyi Etkiledi", BBC Türkçe, 21 Ekim 2016; "Friday's Third Cyberattack on Dyn "Has Been Resolved," Company Says", CNBC, 21 Ekim 2016; "US Security Chiefs Stumped Over Source of Global Ddos Attack-Obama", RT News, 25 Ekim 2016, https://www.rt.com/usa/364008-us-ddos-attack-dyn/, (Erişim tarihi: 19 Aralık 2016).

18. "Donald Trump to Russia: Hack and Publish Hillary Clinton's 'Missing' Emails", *The Guardian*, 27 Temmuz 2016; "Clinton Blames Russia for DNC Hack as Trump Seems to Back Annex of Crimea", *The Guardian*, 31 Temmuz 2016; Dan Merica, "Hillary Clinton: Timing of Russian Hack Aimed at Helping Trump", CNN, 06 Eylül 2016; "Putin on Trump Victory: Russia is Ready to Restore Relations with US", RT News, 9 Kasım 2016, https://www.rt.com/news/365966-putin-trump-congratulates-victory/, (Erişim tarihi: 19 Aralık 2016); "Intel Chief: Russia Eased Hacking After U.S. Accused Kremlin", Military Times, 17 Kasım 2016, http://www.militarytimes.com/articles/intel-chief-russia-eased-hacking-after-us-accused-kremlin?utm_source=Sailthru&utm_medium=email&utm_campaign=DFN%20EBB%2011.18.16&utm_term=Editorial%20-%20Early%20Bird%20Brief, (Erişim tarihi: 19 Aralık 2016).

NATO'NUN SİBER SAVAŞLA MÜCADELESİ

2000'li yılların başından itibaren NATO'nun gündemine giren "siber savaş" kavramı ilk olarak 1999 yılında NATO'nun Sırbistan'a düzenlediği askeri operasyonları protesto etmek amacıyla NATO ve üye devletlerine karşı yapılan yoğun siber saldırılara bilahare Rusya ve Çin kaynaklı siber eylemlere ve sızmalara dayanır.[19] Bu nedenledir ki NATO 2002 yılındaki Prag Zirvesi'nde "Siber Savunma Programı"nı kabul ederek "siber saldırılar" gibi "geleneksel olmayan tehditler"e karşı üye devletlerin savunma yeteneklerinin güçlendirilmesi gerektiği beyanında bulunuştur.

Siber güvenliğin sağlanmasına ilişkin alınan karar çerçevesinde NATO, ilk önce "Bilgisayar Olaylarına Müdahale Gücü Teknik Merkezi" (*Computer Incident Response Capability Technical Centre*-NCIRC) adıyla özel bir birim kurmuş müteakiben "Prag Yetenekler Taahhüdü" (2002) ve "Kapsamlı Siyasi Yönerge" (2005) vasıtasıyla siber savunma sistemlerinin korunması ve güçlendirilmesine yönelik politikalarını devam ettirmiştir. Bu minvalde İttifak liderleri, 2006 yılında gerçekleşen Riga Zirvesi'nde bilgi ve iletişim sistemlerine ilave koruma sağlanmasına ihtiyaç duyulduğunu teyit ederlerken komuta-kontrol konsepti ile bilişim altyapısının savunmasında iyileştirmeye gidilmesi gerektiğine dikkat çekmişlerdir.

Ancak 2007 yılının Nisan ve Mayıs aylarında Estonya'nın savunma sistemini felç eden devlet daireleri, bankalar ve medya başta olmak üzere kamu ve özel kurum ve kuruluşların internet sayfalarına yapılan geniş kapsamlı siber saldırılar NATO'nun muhtemel siber saldırıların yaratabileceği tehdide yönelik algısını tümüyle değiştirmiştir. Başka bir deyişle artık İttifak 21. yüzyılda siyasi, ekonomik ve bilişim güvenliğine bu denli

19. NATO'nun siber savunma politikası hakkında kapsamlı ve detaylı bilgi için bkz., "Cyber Defence", NATO, (güncellenmiş, 25 Temmuz 2016), http://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 19 Aralık 2016).

zarar verebilen siber saldırıları "öncelikli risk arz eden tehdit" olarak tanımlamış, akabinde de birlik içerisinde ortak bir mücadele zemini yaratabilmek amacıyla üye ülkelerin teknik ve politik altyapısını güçlendirmek için gerekli çalışmaları başlatmıştır.

Ertesi sene gerçekleşen 2008 Bükreş Zirvesi'nde üye devletlerin siber saldırılara karşı yeteneklerinin geliştirilmesi ve bu kapsamda mücadele stratejilerinin oluşturulmasına duyulan ihtiyaç bir kez daha güçlü şekilde teyit edilmiştir. Bu çerçevede NATO onayladığı siber savunma politikası kapsamında "Sanal Savunma Yönetim Otoritesi" (CDMA) ve Estonya merkezli "Siber Savunma Mükemmeliyet Merkezi"ni (CCD COE) kurmuş, ayrıca 2012 yılı sonunda tamamen operasyonel hale getirilen "Acil Müdahale Takımları" (RRT) oluşturulması kararını almıştır. Söz konusu kurumların temel amacı ise belirlenen ilkelere istinaden gerek NATO'nun ve gerekse üye ülkelerin siber saldırıları önleme, erken uyarı ve bunlara karşı daha koordineli mukabele yeteneği geliştirmelerine yardımcı olmak şeklinde tanımlanmıştır.

Ne var ki ulusal ve uluslararası iletişim şebekelerine yapılan siber saldırıların sıklaşması, bilgi güvenliğine ve altyapı hizmetlerine verdiği zararın artması, NATO'nun siber tehdit algılamasında meydana gelen bilinci daha ileri düzeye taşırken İttifak'ın siber savunma konusunda yeni bir politika ve eylem planı geliştirmesini zaruri kılmıştır. Zira 2007'de Estonya, 2008'de ABD askeri bilgisayar sistemleri ve Gürcistan, 2010'da İran (Nükleer Programı, Stuxnet virüsü) ve Fransa (G20 Zirvesi öncesi), 2011'de Belçika (AB Zirvesi öncesi), WikiLeaks Olayı, Çin kaynaklı siber casusluk faaliyetleri, hacker grupları Anonymous ve LulzSec tarafından CIA, FBI, Pentagon, NATO, Vatikan gibi ulusal ve uluslararası kurum ve kuruluşlara yapılan siber saldırıların her birisi tehdidin riskini ve boyutunu çarpıcı şekilde gözler önüne sermiştir. Diğer bir deyişle NATO ve üye devletler 21. yüzyılın üstün teknolojisini kullanan, zaman, mekan, sınır tanımayan, ülkelerin askeri sistem şebekelerini ve altyapılarını çökertebilecek, resmi/gayri resmi kurum ve kuruluşların faaliyetlerini tamamen durdurabilecek ve dolayısıyla insanların günlük hayatlarını felç edebilecek kapasitedeki düzensiz ve asimetrik bir tehdit sorunu ile başa çıkmak zorunda kalmışlardır.

Üçüncü milenyum "siber savaşlar"ın bir rüya değil, yakın gelecekte devletlerin kaçınılmaz bir şekilde sürüklenecekleri muharebe meydanı olacağına işaret etmektedir.

Dolayısıyla NATO yeni güvenlik tehdidine uyum sağlamak ve mekanizmalarını güncelleştirmek amacıyla üye devletlere yardım sağlanması, etkin bilgi paylaşımı ve iş birliğinin geliştirilmesi yönünde bir dizi kritik kararlar almıştır. Bu bağlamda "Yeni Stratejik Kavram" ve "Lizbon Zirve Bildirisi" (2010) söz konusu yöntem ve stratejilerin daha somut bir şekil kazandığının açık göstergesidir. Zira alınan kararlarda siber tehdit İttifak'ın öncelik verdiği güvenlik riskleri arasında yer almış ve bu yönde oluşturulacak savunma politikalarının "aciliyet" ve "hassasiyet" gerektirdiği vurgulanmıştır. Hatta ABD Savunma Bakanlığının hazırladığı siber savunma stratejisinde siber saldırılar "savaş sebebi" sayılabilecek ve ortak savunma sisteminin devreye sokulmasına sebep olabilecek nitelikte bir muhtemel gelişme olarak tanımlanmıştır. Öte yandan İttifak'ın revize ettiği ikinci Siber Savunma Politikası, Haziran 2011'deki NATO Savunma Bakanları Toplantısı'nda onanan yeni "Siber Savunma Kavramı" ile pekiştirilmiştir.[20] Böylece NATO, Yükselen Güvenlik Tehditleri Bölümü

20. Bkz. "Defending the Networks: The NATO Policy on Cyber Defence", NATO, http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf, (Erişim tarihi: 19 Aralık 2016). Bu hususta Kenneth Geers'ın "Stratejik Siber Güvenlik" başlığıyla kaleme aldığı, bilgisayar güvenliğinin "teknik bir disiplin"den nasıl "stratejik bir konsept"e dönüştüğünü anlattığı, 2011 tarihli NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCD COE) yayını geniş kapsamlı ve detaylı bilgiler sunmaktadır. Bkz. Kenneth Geers, *Strategic Cyber Security*, (NATO-CCD COE Publications, Tallinn: 2011).

(ESCD), Ulusal Siber Güvenlik İttifakı (NCSA), Komuta Kontrol ve Danışmanlık Ajansı (NC3A), Müttefik Transformasyon Komutanlığı (ACT), Siber Savunma Mükemmeliyet Merkezi (CCD COE) bünyesindeki siber savunma çalışmalarını daha etkin ve etkili biçimde yürütmeye başlamıştır. Ayrıca 2012 Nisan'ında NATO Savunma Planlama Süreci'ne siber savunma da entegre edilmeye başlanmış; Mayıs ayındaki Chicago Zirvesi'nde İttifak liderleri, NATO'nun tüm ağını, merkezileştirilmiş bir koruma sağlama ve iyileştirmelerin uyarlanması maksadıyla NCIRC çatısı altında bir araya getirerek, NATO'nun siber savunmasının geliştirilmesi hususundaki bağlılıklarını teyit etmişlerdir. Yine söz konusu reformların bir parçası olarak 2012 Temmuz'unda NATO Muhabere ve Bilgi Ajansı (NCIA) kurulmuştur.

NATO 21. yüzyılda siyasi, ekonomik ve bilişim güvenliğine zarar verebilen siber saldırıları "öncelikli risk arz eden tehdit" olarak tanımlamış, akabinde de birlik içerisinde ortak bir mücadele zemini yaratabilmek amacıyla üye ülkelerin teknik ve politik altyapısını güçlendirmek için gerekli çalışmaları başlatmıştır.

Yukarıda kısaca değinilen gelişmelerden görüleceği üzere NATO ve üye devletler söz konusu tehditle mücadele etmek amacıyla sistemli bir planlama içerisine girmişler, siber savunma bütçesini hızla artırırken teknik altyapıyı güçlendirmek için de önemli girişimlerde bulunmuşlardır. Ancak bütün bunların haricinde İttifak'ın belki de en fazla tartıştığı hususlardan birisi siber savunma politikalarına "ortak savunma sistemi"ni devreye sokacak "yasal düzenlemeler" ile hukuki bir nitelik kazandırmak olmuştur. Tartışmaların odağında siber saldırıların bir "savaş gerekçesi" olarak telaffuz edilmesi, böylece savunma ve caydırıcılık misyonlarının gerektiğinde devreye sokulması hususu yer almıştır. Başka bir ifadeyle tartışma 4 Nisan 1949 tarihli kuruluş anlaşmasında, "Bir üyeye yapılan herhangi bir saldırı tüm üyelere yapılmış kabul edilir" şeklindeki 5. madde çerçevesinde siber saldırılara mukabelede bulunabilmek adına uluslararası hukukun öngördüğü politik ve teknik kabiliyetlerin kullanılması üzerinde yaşanmıştır.

Peki, Soğuk Savaş esnasında kabul edilen askeri saldırıların günümüzde siber saldırılar olarak genişletilmesi ve herhangi bir üyenin olası bir siber saldırıya uğraması halinde anlaşmanın bu maddesinin uygulanması mümkün müdür? NATO Siber Güvenlik Başkanı Süleyman Anıl'ın Bilişim 2011 Etkinliği esnasında dile getirdiği "Siber uzayda soğuk savaş çıkabilir"[21] sözlerinden hareketle siber dünyanın yeni bir çatışma alanı olduğunu kabul etsek dahi bu yeni tür savaşa dair bazı temel soruların cevaplandırılması ve bu yönde bir uzlaşının sağlanması gerekmektedir.

Örneğin;

- Zaman, mekan ve sınır tanımayan siber saldırıları, öncesinde ve sonrasında "kim" ve "nasıl" tespit edecektir? Eylem ve fail arasındaki "hukuki ilişki" ne şekilde kurulacak, delillendirilecek ve ispat edilecektir? Bu konudaki süreç zamansal ve metodolojik olarak ne şekilde işleyecektir? Bunun da ötesinde saldırıyı yapan kişi ya da grupla bunları yönlendiren devlet arasındaki sorumluluk ilişkisi ya da illiyet bağı "ne şekilde" kurulacaktır?
- Kişi veya örgütün herhangi bir devletle ilişkisi söz konusu ise bu durum o ülkenin hükümetine nasıl bağlanacaktır? Şayet saldırıyı gerçekleştirenler üye ülkelerden birinin ya da saldırı ile hiçbir bağlantısı olmayan üçüncü bir ülkenin internet şebekelerini kullanmış ve bu da tespit edilmiş ise bu durumda eylemin gerçekleştiği ülke nasıl dışarıda bırakılacak ya da tam tersi bir durumda ülkenin hükümeti hangi koşullar altında sorumlu tutulacaktır?

21. "NATO Siber Güvenlik Başkanı Anıl: Yeni Soğuk Savaş Siber Alanda Olabilir", *Bilişim Dergi*si, Sayı 138, s. 78-81.

- Potansiyel saldırıların güvenlik çıkarlarına zarar verme riskinin derecesi ve saldırı sonrası verdiği zarar nasıl hesaplanacaktır?
- Hangi tür siber saldırılar, 5. madde kapsamında değerlendirilerek acil bir durum oluşturacak ya da meşru müdafaa gerektirecek diğer saldırı türleri ile eş sayılacaktır?
- Saldırılara cevap verebilmek için nasıl bir silah ya da teknoloji sistemine sahip olmak gerekecektir?
- Savunma bütçelerini dramatik bir şekilde azaltan üye devletler siber savaşın maliyetini karşılamaya ve bu yönde yatırım yapmaya rıza gösterecekler midir?
- Siber savunma kapasiteleri ve yetenekleri dahi gelişmemiş bazı üye devletler savaş tehdidine karşı ne şekilde etkili bir caydırıcılık sergileyecek ya da gerekli önleyici faaliyetleri hangi oranda gerçekleştirebileceklerdir? Siber savaşa karşı nasıl bir misilleme yapılması gerekecektir? Askeri güç kullanımı ya da siyasi ve ekonomik bir yaptırım, uluslararası hukuka nasıl bağlanacaktır? Tespit edilen siber saldırıya "nasıl", "ne zaman" ve "hangi orantıda" güç kullanılarak karşılık verilecektir?
- Bu saldırılara karşı yapılacak mukabelenin şekli ve sınırları nasıl çizilecektir? Uluslararası hukukta askeri kuvvet kullanılmasını gerektiren "zararla karşılık" uygulamasına başvurmanın önüne nasıl geçilecektir?
- Üye devletler ortak savunmada "birlikte duruş" sergileseler dahi bazı üye devletlerin kötü seyreden ikili ilişkileri karar alma sürecini nasıl etkileyecektir?
- Siber saldırıları önleme, tespit etme ve karşılık verme aşamasında üye devletlerin ulusal yasaları ve düzenlemelerinin müdahale etme sürecini zora sokma ihtimali dahi söz konusu iken bilgi paylaşımı ve ortaklık aşamasında uluslararası iş birliği ne şekilde sağlanabilecektir?
- Tespit edilmiş ancak henüz saldırı seviyesine ulaşmamış siber savaş tehditlerine karşı kime, ne şekilde bir cevap verilecektir?

Kuşkusuz yukarıda zikredilen soruların net olarak cevaplanması en azından şimdilik zor gözükmektedir. Bunun birinci nedeni İttifak'ın mevcut durumda klasik olarak tanımlanan tehditler çerçevesinde karşılaştığı sorunların çözümünde dahi uzlaşı sağlayamayan görüntüsüdür. İkinci nedeni ise NATO'nun geniş bir yelpazede sınır tanımayan tehditlerle karşı karşıya olmasıdır. Zira altı farklı bölgede istikrarı ve güveni tesis etmeye çalışan NATO'dan terörizmle mücadele, iç savaş, ekonomik kriz, savunma planlaması, genişleme süreci, toprak bütünlüğü koruma, askeri harekatlar, KİS, korsanlık, uyuşturucu ve insan kaçakçılığı, balistik füze, siber saldırı, enerji ve çevre güvenliği gibi birçok meseleye çözüm ve katkı sağlaması beklenmektedir.

Askeri, siyasi ve güvenlik meselelerine bakarak NATO'nun yakın dönem içerisinde siber saldırılara karşı ortak savunma sistemini siyasi söylem ve hukuki beyanatların ötesinde fiiliyatta devreye sokması henüz ihtimal dahilinde gözükmemektedir. Açıkçası böyle bir kararın mevcut şartlar altında başarı ile uygulanması son derece zayıf bir olasılıktır. Zira üye devletlerin böyle bir kararı fiiliyata geçirmeden önce üzerinde durmaları gereken çok daha önemli hususlar vardır. Mesela üye devletlerin tamamında siber bilinç ve direnç geliştirilmeli ve siber saldırılara karşı koyacak güçlü bir altyapı ivedilikle inşa edilmelidir.

Eğer İttifak'ın siber savaşa karşı mücadelede başarılı olması bekleniyorsa bu sadece ABD, İngiltere, Almanya ve Fransa gibi sınırlı sayıda ülkenin üst düzey bilişim teknolojisine bel bağlanarak yapılmamalıdır. Ayrıca siber saldırıları önlemenin siber savaşa karşılık vermekten çok daha önemli olduğu gerçeği en baştan kabul edilmelidir. Bu da üye devletlerin yüksek teknolojik donanımlarına, istihbarat kapasitelerine ve analiz becerilerine bağlıdır. Özellikle NATO'nun istihbarat yetenekleri bakımından üye devletlere bağımlı olduğu düşünülürse güçlendirilmiş bir

istihbarat ağının "siber savunma politikası" çerçevesinde daha etkin bir bilgi paylaşımı ve iş birliği sağlayacağı aşikardır.

Tarihsel arka plana bakıldığında Türkiye ilk ciddi siber saldırıyı 5 Ağustos 2008 tarihinde deneyimlemiştir.

Yukarıdaki hususlara ilaveten belirtmek gerekir ki 2014 yılının Şubat ayında İttifak'ın Savunma Bakanları NATO'yu kolektif savunma, müttefiklere yardım, modern yönetişim, sanayi ile ilişkiler ve yasal hususlarla bağlantılı olarak "yeni ve güçlendirilmiş bir siber savunma politikası" geliştirmek üzere görevlendirmiştir. Kuzey Atlantik Konseyi (NAC) Nisan 2014'te "Savunma Politikası ve Planlama Komisyonu/Siber Savunma" bölümünün ismini "Siber Savunma Komisyonu" olarak yeniden adlandırmıştır. NATO ağına ve kullanıcılarına artırılmış koruma sağlayan NCIRC Mayıs 2014 itibarıyla tam operasyonel yeterliliğe ulaşmıştır. Müttefikler Eylül 2014'te gerçekleşen Galler Zirvesi'nde yeni siber savunma politikasını onarlarken, yeni eylem planını da tasdik etmişlerdir. Ayrıca İttifak üyeleri gelişen siber tehditler karşısında mevzubahis politika ve uygulamanın gerek siyasi ve gerekse teknik düzeylerde gözden geçirilerek sürekli geliştirilip güncellenmesi gerektiği üzerinde mutabık kalmışlardır. 17 Eylül 2014 tarihinde NATO siber tehdit ve sorunlarla başa çıkabilmek amacıyla özel sektörle daha yakın ve güçlendirilmiş iş birliğinin tesisine yönelik olarak bir inisiyatif başlatmıştır. Bu çerçevede İttifak liderlerince Galler Zirvesi'nde kabul edilen NATO Endüstri Siber Ortaklığı (NICP) Belçika'nın Mons şehrinde düzenlenen, bin 500 endüstri lideri ve politika belirleyicilerin siber işbirliğini tartışmak üzere bir araya geldiği iki günlük konferansta sunularak tanıtılmıştır.

10 Şubat 2016 tarihinde ise NATO ve Avrupa Birliği (AB), müşterek olarak siber saldırılara karşı koruma ve cevap verme amacıyla "Siber Savunmaya İlişkin Teknik Anlaşma"yı imzalamışlardır. Bu kapsamda NATO Siber Olaylara Mukabele Yeteneği (NCIRC) ile AB'nin Bilgisayar Olaylarına Acil Müdahale Timi (CERT-EU) arasında bilgi ve tecrübe paylaşımı hususunda teknik bir çerçeve belirlenmiştir. 14 Haziran 2016 tarihinde gerçekleşen Varşova Zirvesi'nde İttifak Savunma Bakanları halihazırdaki harekat alanları olan "kara", "deniz" ve "hava"ya ilaveten "siber-uzay"ı, harbin yeni boyutu olarak tanıma hususunda mutabakata varmışlardır. Günümüzdeki kriz ve çatışmalardaki "siber boyut" göz önünde bulundurulduğunda şüphesiz bu kararla temel amaç ve görevi savunma olan NATO'nun misyon ve operasyonlarını daha güçlü icra etmesini sağlayacağı öngörülmüştür. Keza 8-9 Temmuz 2016 tarihleri arasında gerçekleşen Varşova Zirvesi'nde de Müttefikler, "siber uzayı" NATO'nun yeni askeri harekat alanı olarak resmen kabul etmişler, bilahare siber savunma maksadıyla öncelikle kendi ulusal ağları ve altyapılarını geliştirmeyi ve siber saldırılara süratle karşı koyma kabiliyet ve yeteneklerini artırma yükümlülüklerini yerine getireceklerini taahhüt etmişlerdir. Başka bir yönüyle bu taahhüt aynı zamanda NATO'nun interneti bir savaş alanı olarak tanımasını dolayısıyla İttifak'ın siber saldırılara karşı konvansiyonel silahlarla mukabelede bulunmasının da önünü açmıştır.

Sonuç itibarıyla 2016 Varşova Zirvesi'nde NATO'nun gündemi belki de hiç olmadığı kadar yoğun olmuştur. İttifak üyeleri siber savunma kapasitelerini artırmak ve siber savaşla mücadele politikalarını birbirlerine eklemlemek amacıyla görüşmeler yapmış ve birtakım yeni kararlar almışlardır.[22]

22. "Cyber Defence Pledge", NATO, 08 Temmuz 2016, http://www.nato.int/cps/en/natohq/official_texts_133177.htm, (Erişim tarihi: 19 Aralık 2016).

Bahse konu olan bu kararlar başlıklar halinde şu şekildedir:

- Siber savunma NATO'nun kolektif savunma anlayışının önemli bir parçası olmuştur.
- NATO siber uzay alanında da uluslararası hukuk kurallarının geçerli olduğunu kabul etmiştir.
- NATO hava, kara ve denizin ardından harbin yeni boyutu olarak siber uzayı kabul etmiştir.
- Müttefik ülkeler NATO'nun ve birbirlerinin ağıyla uyumlu olacak şekilde kendi ulusal iletişim ağlarını korumakla mükelleflerdir.
- NATO siber eğitim, öğretim ve tatbikat imkan ve kabiliyetlerini geliştirecektir.
- Müttefik ülkeler siber saldırıları önlemek, etkilerini hafifletmek ve olası zararları karşılamak amacıyla bilgi paylaşımı ve karşılıklı yardımlaşmayı pekiştirme taahhüdünde bulunmuşlardır.
- NATO ve AB siber savunma iş birliği hususunda teknik anlaşma imzalamışlardır.
- NATO Endüstri Siber Ortaklığı (NICP) çerçevesinde endüstri ile daha yakın ve yoğun iş birliği sağlanacaktır.

TÜRKİYE'NİN SİBER TEHDİTLERE KARŞI HAZIRLIK DURUMU

Günümüz toplum ve devletlerinin karşılaştıkları yeni güvenlik sorunlarından birisi olan "siber tehditler" mutlak korunmanın da mümkün olmadığı bir alanı temsil etmektedir. Bunda teknolojinin çok hızlı ilerleme kaydetmesi ve adeta herkese açık bir yarış alanı olmasının getirdiği sınır tanımazlığı kadar; güvenliğin sağlanabilmesinin çok aktörlü paydaşlar arasında yoğun bir iş birliği, görev ve sorumluluk paylaşımını gerektirmesi başrolü oynamaktadır. Üstelik bu paydaşlar çoğu zaman ulusal sınırları aşan bir niteliğe sahip olabilmektedir. Bu nedenle siber güvenliğin sağlanmasında "sıfır risk" yerine, "yönetilebilirlik" sınırları içerisinde bu riskleri minimalize etme çabaları öne çıkmaktadır.

Bu tehditlerden bağımsız olmayan Türkiye de siber güvenliğin ulusal düzeyde sağlanması teknik sorumluluğunu, görev alanları bakımından öncelikle Ulaştırma, Denizcilik ve Haberleşme Bakanlığına (UDHB) vermiştir. Ayrıca Emniyet Genel Müdürlüğü ve Milli İstihbarat Teşkilatı gibi güvenlik ve istihbarat kuruluşlarının da bu anlamda kendi görev alanları bakımından sorumluluk ve görevleri olduğu gibi başta savunma sanayii ile ilgili olanlar olmak üzere stratejik nitelikteki diğer kurum ve kuruluşlar da faaliyet alanları bakımından gerekli önlemleri almak durumundadırlar. UDHB siber güvenliğin sağlanmasında ana koordinasyonu sağlama ve ulusal düzeyde strateji ve eylem planları hazırlayarak bunların uygulamasını icra ve takip etmede birincil sorumluluğa sahiptir.

Tarihsel arka plana bakıldığında Türkiye ilk ciddi siber saldırıyı 5 Ağustos 2008 tarihinde deneyimlemiştir. Günde yaklaşık 1 milyon varillik ham petrolü Hazar Denizi'nden Türkiye'nin Akdeniz kıyılarına ulaştıran 1.768 kilometrelik Bakü-Tiflis-Ceyhan (BTC) boru hattı üzerinde Erzincan'ın Refahiye ilçesi yakınlarında bir patlama meydana gelmiştir. Her ne kadar ilk kertede sabotajdan şüphelenilmiş, saldırıyı PKK üstlenmiş ve hatta müteakiben yürütülen soruşturmada "teknik arıza" gerekçesine dayandırılmışsa da hakikatte patlamanın sofistike bir siber saldırı nedeniyle vuku bulduğu öne sürülmüştür. Saldırının büyüklüğü ve yol açtığı zarar noktasından yaklaşıldığında Amerikan Deniz Harp Akademisi (*U.S. Naval War College*) Profesörü Derek Reveron'a göre BTC patlaması siber savaşın tarihini değiştirir nitelikte tekrardan yazmıştır.[23] Başka bir örnek mahiyetinde 3 Temmuz 2012 tarihinde hackerlar tarafından Dışişleri Bakanlığı-

23. "Siber savaşın miladı", *Milliyet*, 10 Aralık 2014, http://www.milliyet.com.tr/siber-savasin-miladi/dunya/detay/1982549/default.htm

nın internet sitesine siber saldırılar düzenlenmiş, Bakanlığın sınav başvurularına ilişkin bilgilerine erişimin haricinde yabancı misyonlarda çalışanlara ait kimlik bilgilerinin internet ortamında yayınlanması söz konusu olmuştur.[24] Yine Aralık 2015'te Türkiye tam 2 hafta boyunca yoğun siber saldırılara maruz kalmıştır. Öyle ki dönemin ODTÜ Rektörü Ahmet Acar 14 Aralık'ta "uluslararası literatüre geçecek düzeyde, dünya üzerinde yaşanmış en yoğun saldırılardan birisinin gerçekleştiğini"; yurt içinde ve dışında 5 ayrı noktada konuşlanan 6 adet ".tr" alan adı sunucusuna DDoS saldırılarının düzenlendiğini açıklamıştır.[25] Ayrıca söz konusu konjonktürde Türkiye-Rusya arasındaki gerginliğe dayandırılarak Rus hackerlar tarafından yapıldığı iddia edilen, bankalar başta olmak üzere e-Devlet gibi kritik bazı kamu kurumlarının internet sitelerine yöneltilen siber saldırılar neticesinde kredi kartı ödemeleri ve diğer bankacılık işlemlerinin yanı sıra internet üzerinden gerçekleştirilen muhtelif uygulamalarda da aksaklıklara tanık olunmuştur.[26] Şüphesiz Türkiye bu türden siber saldırılara anında müdahale edilmesi ve önleyici tedbirler alınması hususunda önemli adımlar atmıştır. Örneğin 2008 yılında TÜBİTAK tarafından 8 kamu kurum ve kuruluşunun katılımıyla gerçekleşen "ulusal seviyedeki ilk siber güvenlik tatbikatı" BOME 2008 Bilgi Sistem Güvenliği Tatbikatı'na ilaveten TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Araştırmalar Merkezi (BİLGEM) ve BTK iş birliğiyle 2011 ve 2013 yıllarında "Ulusal Siber Güvenlik Tatbikatı" düzenlendiğinin altı çizilmelidir.[27]

Bu aşamada Türkiye'nin siber güvenlik alanındaki ilk ciddi atılımının da TÜBİTAK BİLGEM bünyesinde "Ağ Güvenliği Grubu"nun teşekkül ettirilmesiyle başladığı not düşülmelidir. 1997 yılında kurulan Ağ Güvenliği Grubu'nun adı, müteakiben "Bilişim Sistemleri Güvenliği" (BSG) ve 2012 Temmuz itibarıyla müstakil bir yapıya büründürülerek "Siber Güvenlik Enstitüsü" (SGE)[28] olarak değiştirilmiştir. Kuşkusuz Türkiye Ağ Güvenliği Grubu ve halefleri nezdinde yürütülen çalışmalar ve projeler sayesinde ulusal siber güvenliğin sağlanmasına yönelik önemli bir bilgi birikimi elde etmiştir.

Örneğin 2001'de Genelkurmay Başkanlığının desteğiyle "Ortak Kriter Test Merkezi" (OKTEM) kurulması projesi gerçekleştirilmiş, ilerleyen süre zarfında "Haberleşme Güvenliği" (COMSEC) testleri kabiliyetler arasına eklenirken 2006 sonrası özellikle "Yan Kanal Analizi" (*Side Channel Analysis*) ve "Tersine Mühendislik" (*Reverse Engineering*) konularında uzmanlık kazanılmıştır. Keza Türkiye'nin bilgi toplumu olması ve bilgi teknolojilerinden etkin olarak istifade edilmesi amacıyla Devlet Planlama Teşkilatı Bilgi Toplumu Dairesi Başkanlığının 2005 yılında başlattığı "Bilgi Toplumu Stratejisi" projesi önemli getiriler sunmuştur. Proje kapsamında Ağ Güvenliği Grubu tarafından yürütülmek suretiyle kamu kurum ve kuruluşların bilgi sistemlerinin güvenliğini sağlamak, olası güvenlik problemlerini minimize etmek, ilgili ihtiyaçları karşılamak ve kurumsal bilgi güvenliği bilincini tesis etmek gayesiyle "Bilgi Sistemleri Güvenlik Programı" başlatılmıştır. Programın önemli hedeflerinden birisi Türkiye'nin, bilgisayar ortamlarında yaşanabilecek bilgi güvenliği sorunlarına doğru, zamanında ve sağlıklı müdahaleyi gerçekleştirebilme imkan ve kabiliyetleri açısından gerek duyulan altyapının tesisi olmuştur ki bu amaca binaen "Türkiye Bilgisayar Olayla-

24. "Dışişleri İnternet Sitesine Siber Saldırı", TRT Haber, 03 Temmuz 2012.

25. "Savunmamız Sağlamdı", *Hürriyet*, 25 Aralık 2015.

26. "Bankalara Siber Saldırı Bugün De Devam Ediyor", *Hürriyet*, 25 Aralık 2015.

27. "Siber Güvenlik Tatbikatları", TÜBİTAK BİLGEM, http://sge.bilgem.tubitak.gov.tr/tr/siber-guvenlik-tatbikatlari, (Erişim tarihi: 19 Aralık 2016).

28. "Siber güvenlik" alanında Ar-Ge faaliyetleri yürüten TSK başta olmak üzere kamu kurum ve kuruluşları ile özel sektöre çözüme yönelik projeler gerçekleştiren SGE'nin etkinlikleri; (i) İleri Siber Güvenlik Araştırma-Geliştirme Çalışmaları, (ii) Siber Güvenlik Stratejisi Belirleme Çalışmaları ve (iii) Siber Güvenlik Çözüm Projeleri şeklinde üç temel başlık altında toplanmaktadır. Detaylı bilgi için bkz. "Tarihçe", TÜBİTAK BİLGEM, Siber Güvenlik Enstitüsü, http://sge.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce, (Erişim tarihi: 19 Aralık 2016).

rına Müdahale Ekibi (TR-BOME)"[29] teşekkül ettirilmiştir. Stratejik nitelikli kamu kurum ve kuruluşlarında BOME yapılanmasının kurulabilmesi için TR-BOME gerekli eğitim, koordinasyon ve danışmanlık faaliyetleri icra etmekle mükellef kılınmıştır. Bu çerçevede 2008 yılından itibaren gerçekleştirilen ulusal düzeydeki tatbikatlarla ilgili kurumların "bilgi güvenliği" sorunlarına hızla çözüm üretebilme kabiliyeti kazanabilmeleri konusunda muhtelif projeler hayata geçirilmiştir.

Ulusal düzeyde bilgi güvenliği ve siber savunmaya yönelik çalışmalar kapsamında ayrıca TSK bünyesinde 2012 yılında "Siber Savunma Merkezi Başkanlığı" kurulmuş olup bu Başkanlık 2013 Ağustos'ta Genelkurmay Karargahı yerleşkesinde bulunan "Siber Savunma Komutanlığı"na dönüştürülmüştür. Keza 2013 yılında siber alanda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerinin azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde "Ulusal Siber Olaylara Müdahale Merkezi" (USOM, TR-CERT) faaliyete geçirilmiştir.[30]

Yine söz konusu çalışmaların bir parçası olarak TSK'nın bilgi sistemleri güvenliği ve siber savunma konusunda anında harekete geçilebilmesi ve olası saldırıların etkilerinin azaltılması maksadıyla "TSK Siber Savunma Merkezi Projesi" (SSMP) geliştirilmiştir. Proje kapsamında "Siber Savunma Merkezi"nin kurulması, bilahare bu merkezin gereksinimlerini karşılamak üzere "Siber Savunma Harekat Merkezi"nin teşekkülü kararlaştırılmıştır. Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. 'nin (STM) ana/alt yüklenici olduğu SSMP siber saldırılar karşısında eş zamanlı ve etkili karşılık verilebilmesi amacıyla tasarlanmış önemli bir proje olup halihazırda "ihale teklif değerlendirme aşaması"ndadır.[31] Ayrıca güncel bir gelişme mahiyetinde siber güvenlikte mükemmeliyet merkezi olmayı hedefleyen HAVELSAN'ın bünyesinde faaliyet göstermek üzere "Siber Savunma Teknoloji Merkezi" (SİSATEM) 23 Mart 2016 tarihinde hizmete açılmıştır.[32]

Siber tehditlerden bağımsız olmayan Türkiye siber güvenliğin ulusal düzeyde sağlanması teknik sorumluluğunu, görev alanları bakımından öncelikle Ulaştırma, Denizcilik ve Haberleşme Bakanlığına (UDHB) vermiştir.

Burada bir parantez açıp 2016 Mayıs'ında STM nezdinde kurulan "Siber Füzyon Merkezi"nin (SFM) de kritik teknoloji ve bilgi varlıklarını koruyan proaktif ve koruyucu faaliyetlerde bulunduğunu bilgi teknolojileri operasyonları ile siber tehdit istihbaratından gelen bilgi akışı ve güvenlik fonksiyonlarını yönetip koordine ettiği vurgulanmalıdır. Görev tanımı ve alanı itibarıyla SFM "Siber Operasyon (Harekat) Merkezi" (SOM), "Siber İstihbarat Merkezi" (SİM) ve "Zararlı Yazılım Analiz Laboratuvarı" şeklinde üç ana unsurdan oluşmakta, böylece hem harekat etkinliğini hem de siber tehdit istihbaratının zamanında dağıtılmasıyla saldırıları önleyerek yahut etkisini azaltarak güvenlik seviyesini artırmaktadır.[33]

29. Bilgisayar güvenlik sorunlarıyla ilgili ulusal danışma noktası olan TR-BOME Koordinasyon Merkezi, TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) Bilişim Sistemleri Güvenliği bölümü bünyesinde faaliyetlerine sürdürmektedir. TR-BOME ve BOME KM hakkında ayrıntılı bilgi için bkz. TÜBİTAK UEKAE, TR-BOME, https://www.bilgiguvenligi.gov.tr/cert/index.php, (Erişim tarihi: 19 Aralık 2016).

30. Ulusal Siber Olaylara Müdahale Merkezi ve faaliyetleri hakkında bkz. USOM, https://www.usom.gov.tr/index.html, (Erişim tarihi: 19 Aralık 2016).

31. "TSK Siber Savunma Merkezi Projesi" (Son güncelleme tarihi: 17 Eylül 2015), Savunma Sanayii Müsteşarlığı, http://www.ssm.gov.tr/anasayfa/projeler/Sayfalar/proje.aspx?projeID=276, (Erişim tarihi: 19 Aralık 2016).

32. "Siber Savunma Teknoloji Merkezi Açıldı", TSKGV, http://www.tskgv.org.tr/siber-savunma-teknoloji-merkezi-acildi/, (Erişim tarihi: 19 Aralık 2016).

33. STM, Siber Füzyon Merkezi, https://www.stm.com.tr/tr/urunler/siber-fuzyon-merkezi, (Erişim tarihi: 19 Aralık 2016).

Türkiye'nin siber güvenliğinin sağlanmasında bundan sonra izleyeceği politikaları yansıtması bakımından "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" (USGSEP) önemli ipuçları sunmaktadır. Söz konusu planın temel stratejik anlayışı siber güvenliğin, milli güvenliğin bir ana düstur ve unsuru olarak görülmesidir. Bu konuda toplumun tüm kesimlerinde farkındalık ve bilinç düzeyinin yükseltilerek; teknik, hukuki ve diğer alanlarda gerekli hazırlıkların tamamlanması ve altyapı ögelerinin güçlendirilmesi hedeflenmektedir. Bu çerçevede ana hedeflerin yanı sıra bunları konsolide edecek lojistik ve destekleyici nitelikte alt eylem maddeleri belirlenmiştir. Bunların ne şekilde hayata geçirileceği, icrası ve denetimin yöntem ve usullerinin belirlenmesinin gereğine ilişkin hükümler yine bu belgede derç edilmiştir.

USGSEP'de belirlenen ana hedefler doğrultusunda aşağıdaki somut adımlar öngörülmüştür:[34]

- Bilgi teknolojilerine dayalı verileri ihtiva eden, bunların akışını sağlayan ve her türlü işlem ve hizmet kapasitesine sahip sistemlerin gizlilik ve güvenliğinin sağlanması
- Siber güvenliğe risk ve tehdit teşkil eden teşebbüs ve olayların önlenmesi, vuku bulması halinde zararın asgari seviyede tutulmasına gayret gösterilmesi ve oluşan zafiyetlerin en kısa sürede giderilerek hizmet sunan sistemin normal akışına döndürülmesi, suçun teşekkülü halinde hukuki ve idari kovuşturma ya da soruşturmaların takibinin sağlanması
- Siber güvenliğin sağlanmasında gerekli olan teknik unsur ya da teknoloji ürünlerinin gizliliğin sağlanabilmesi açısından mümkün olduğu kadar yerli üretime dayandırılması, kâbili mümkün olmadığı takdirde ithal edilen teknolojik ürünlerde azami ihtiyatın sağlanması

USGSEP'de öngörülen ve dikkat çeken diğer bir husus ise bu belgenin "statik" değil, "dinamik" bir vizyona sahip olmasıdır. Zira belgede hızla gelişen teknoloji, değişken ve çeşitlenen risk ve tehditlerin oluşturduğu yeni ihtiyaç ve koşullar karşısında kendini güncelleme konusunda bir esneklik tanınmıştır. Bu bağlamda kamu ve özel sektördeki değişen ihtiyaçlar karşısında ortaya çıkan yeni taleplere ivedilikle cevap verilmesini ve bu konuda paydaşlar arasında ulusal düzeyde "eş güdüm" sağlanmasını mümkün kılacak güncellemelerin gerçekleştirilmesi hedeflenmiştir. Planın ihtiva ettiği hedeflere ulaşılması için öngörülen zaman dilimindeki nihai sürenin sonu olan 2019 yılına gelindiğinde gerçekleştirilememiş ya da eksik kalmış eylemlerin bir sonraki eylem planına dahil edilmesi kararlaştırılmıştır. Özetle mevzubahis belgedeki stratejik amaçlara ulaşmak gayesiyle 2016-2019 döneminde gerçekleştirilmesi planlanan stratejik eylemler ise sırasıyla şu başlıklar altında gruplanmıştır: (i) Siber Savunmanın Güçlendirilmesi ve Kritik Altyapıların Korunması; (ii) Siber Suçlarla Mücadele; (iii) Farkındalık ve İnsan Kaynağı Geliştirme; (iv) Siber Güvenlik Ekosisteminin Geliştirilmesi; (v) Siber Güvenliğin Milli Güvenliğe Entegrasyonu.[35]

Son gelişmeler ışığında 20 Ekim 2012 tarihli ve 28447 sayılı *Resmi Gazete*'de yayımlanan Bakanlar Kurulu Kararı (2012/3842) üzerine "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar"ın yürürlüğe konulduğu da ayrıca hatırlanmalıdır. Zira Karar uyarınca UDHB'nin başkanlığında "Siber Güvenlik Kurulu" (SGK) teşekkül ettirilmiş, bu kapsamda SGK kamu kurum ve kuruluşlarının fiziksel ve siber saldırılara karşı daha güvenli bir ağ üzerinden haberleşmeleri amacıyla birtakım çalışmalar gerçekleştir-

34. "2016-2019 Ulusal Siber Güvenlik Stratejisi", Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, s. 9 http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf, (Erişim tarihi: 19 Aralık 2016).

35. "2016-2019 Ulusal Siber Güvenlik Stratejisi", Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, s. 15.

miştir.[36] Mevzubahis çalışmalar neticesinde kamu kurum ve kuruluşları arasındaki iletişim ve veri iletiminin yeni güvenli bir altyapı sağlanıncaya kadar, örneğin siber güvenlik risklerinin azaltılması, e-Devlet uygulamalarının güvenli ortak kullanımı ve halihazırda internet üzerinden gerçekleştirilen bulut uygulamalarının internetten bağımsız sanal ağ üzerinden yapılması maksadıyla "Kamu Sanal Ağı" (KamuNet) oluşturulması kararı alınmıştır. Nitekim 3 Aralık 2016 tarihli ve 29907 sayılı *Resmi Gazete*'de yayımlanan Başbakanlık Genelgesi (2016/28) ile birlikte kamu kurum ve kuruluşlarının KamuNet'e dahil edildiği duyurulmuştur.[37]

Ana hatlarıyla özetlemek gerekir ise Türkiye her zamankinden daha yüksek siber güvenlik riskleriyle karşı karşıyadır. Türkiye'ye yönelik siber saldırıların türü, kaynağı, sayısı ve hedefi hızla çeşitlenip artmaktadır ki bu hakikat yakın zaman önce Başbakan Binali Yıldırım tarafından da çarpıcı bir şekilde dile getirilmiştir. 2016 Aralık'ında 33. Ulusal Bilişim Kurultayı'nda konuşan Başbakan Yıldırım, 2017 senesini "Bilişimde Gelişim Yılı" ilan ettiğini kaydederken internet kullanımında yüzde 56'lara ulaşıldığını, siber güvenlik meselesinin ise ülke güvenliği meselesine dönüştüğünü ancak bu konuda daha fazla mesafe alınması icap ettiğini söylemiştir. Konuşmasında veri merkezi, internet değişim noktaları, bilişim sektöründe insan kaynağı, stratejik bakış ihtiyacı gibi kritik konulara temas eden Yıldırım, bilhassa yazılımların yüzde 95'inin dışarıdan geldiğini hatırlatarak yazılım ve donanımlarda yerlilik ve millilik oranının ehemmiyetine vurgu yapmıştır. Ayrıca 15 Temmuz sonrasında siber saldırılardaki çarpıcı artışa dikkat çekmiş, 8-14 Temmuz'da 183 saldırı gerçekleşirken bu rakamın 5-11 Ağustos arasında 407'ye, 11-17 Ağustos tarihlerinde ise 700 küsura çıktığını deklare etmiştir. Başbakan geniş çaplı ve büyük saldırılar karşısında tedbir alındığını, halihazırda 528 kurumda siber olaylara müdahale ekibi bulunduğunu ancak buna rağmen mevzunun salt siber güvenlik boyutuyla değil, siber caydırıcılık yönüyle de ele alınması gerektiğini açıklamıştır.[38]

SONUÇ

Küresel güvenlik ortamı "konvansiyonel" ve "asimetrik" savaşa ait taktik ve teknikleri bir arada kullanan devlet ve devlet-dışı aktörler sayesinde gittikçe daha "belirsiz" ve "istikrarsız" bir çehreye bürünmektedir. Bu bağlamda "siber-uzay" devletlerin gerek saldırı ve gerekse savunma imkan ve kabiliyetleri açısından kritik bir alana işaret etmektedir. Aslına bakılırsa bu alan birey güvenliğinden devlet güvenliğine uzanan geniş bir yelpazedeki bütün alt ve üst yapıları ihtiva etmektedir. Öyle ki silahlı kuvvetlerin envanterindeki askeri makine ve teçhizattan sivil kullanım amaçlı iletişim ve haberleşme araçlarına, akıllı ev ve bina teknolojilerinden otomasyon sistemlerinin çalışma, performans ve işlevselliklerine değin birçok husus doğrudan siber-uzayı ilgilendirmektedir.

Dolayısıyla "kavram" ve "kapsam" itibarıyla siber güvenlik ekseriyetle zihinlerde çağrıştırdığı bağımsız hackerların yönelttiği tehditten çok daha farklı ve endişe verici bir mahiyete haizdir. Örneğin bazı ülkelerde yüksek otoriteler tarafından belirli bir amaç ve hedefe istinaden istihdam edilen hackerlar vardır ki bunlar söz konusu devletin çıkar ve menfaatlerine en uygun şekilde hizmet edebilecek üstün teknik bilgiyle donatılmış-

36. Siber Güvenlik Kurulu'na üye kurumlar şu şekildedir: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB); Dışişleri Bakanlığı; İçişleri Bakanlığı; Milli Savunma Bakanlığı (MSB); Kamu Düzeni ve Güvenliği Müsteşarlığı (KDGM); Milli İstihbarat Teşkilatı (MİT); Genelkurmay Başkanlığı; Bilgi Teknolojileri ve İletişim Kurumu (BTK); Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK); Mali Suçları Araştırma Kurulu ve Telekomünikasyon İletişim Başkanlığı (TİB). "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", *Resmi Gazete*, http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf, (Erişim tarihi: 19 Aralık 2016).

37. "Kamu Kurum ve Kuruluşlarının KamuNet'e Dâhil Edilmesi ile İlgili 2016/28 Sayılı Başbakanlık Genelgesi", *Resmi Gazete*, http://www.resmigazete.gov.tr/main.aspx?home= http://www.resmigazete.gov.tr/eskiler/2016/12/20161203.htm&main=http://www.resmigazete.gov.tr/eskiler/2016/12/20161203.htm, (Erişim tarihi: 19 Aralık 2016).

38. "Başbakan Yıldırım: Siber Saldırılarda Caydırıcılık Geliştirilecek", *Habertürk*, 22 Kasım 2016; "Başbakan Yıldırım: 2017'yi 'Bilişimde Gelişim Yılı' İlan Ediyorum!", *Habertürk*, 8 Aralık 2016.

lardır. Sadece bu boyutuyla ele alındığında dahi "bağımsız hackerlar" ile "herhangi bir devletin hesabına çalışan hackerlar"ın nasıl ayırt edilebileceği sorunsalı karşımıza çıkmaktadır. Böylesine açık uçlu, her türlü enstrüman ve seçeneği kullanmanın mübah olduğu bir savaşta devletlerin birbirlerini nasıl ve hangi bakımdan suçlayabileceklerini önceden kestirmek oldukça zordur.

Nitekim bugün siber güvenliğin artık ulusal ve hatta küresel güvenlik meselesi haline dönüştüğü müşahede edilmektedir. Öte yandan bilgisayar güvenliğinin de teknik bir disiplinden stratejik bir konsepte evrildiğine şahit olunmaktadır. Bu anlamda dünyanın çok etkili fakat aynı zamanda o ölçüde korunmasız, müdafaası zor bir alan olan internete artan orandaki bağımlılığı siber saldırganların yıkıcı/engelleyici imkan ve kabiliyetleriyle birleşerek ulusal ve uluslararası güvenliğe gittikçe daha büyük tehditler yöneltmektedir. Bilgisayar ve işletim sistemlerinin gücü ve direnci virüsler, solucanlar, klavye kaydediciler, scamler, casus yazılımlar, reklam yazılımları (*adware*) gibi tüm kötü amaçlı ve zararlı yazılımlarla her geçen gün artan oranda sınanmaktadır. Diğer bir ifadeyle başlangıçta kişisel/kurumsal verilerin korunması gibi internet ortamından kaynaklı mahremiyet hassasiyetine dair bireysel/grup kaygılarına vurgu yapılırken halihazırda ulusal, bölgesel ve küresel güvenlik endişelerini gidermeye yönelik siber savunma planlamalarından bahsedilmektedir.

Bu yönüyle "siber güvenlik" meselesi acaba sadece "teknik bir konu" olmakla mı sınırlıdır? Elbette ki "hayır!" Şayet bu şekilde olsaydı başarı ölçümlemesi yapmak muhtemelen çok daha kolay olabilirdi. En basitinden tarihsel seyrinde "yalnız kurt" timsali bağımsız hackerların yerini artık günümüzün küresel siber suçluları ve siber orduları devralmıştır. Peki, siber ordularda "ideal komutan" için nasıl bir profil tahayyül edilmelidir? Ayrıca siber silahlanmanın "maliyeti", "yayılımı" ve "kontrolü" hususlarında çözümü ziyadesiyle zor gözüken problemlerle karşı karşıya olunduğu da yadsınamaz bir hakikattir.

Nükleer silahlar gibi siber saldırılar için de karşılıklı toplu yıkımdan bahsetmek mümkün müdür? Caydırıcılık bir çözüm aracı olabilir mi? Eğer olacaksa "caydırıcılık" nasıl sağlanacaktır? Ağır yaptırım ve cezalar getirmek mi, yoksa hizmet dışı bırakarak diğer bir ifadeyle suç fırsatlarını azaltarak önleme mi tercih edilmelidir? Siyasi araçların devreye sokulması, siber saldırıların azaltılmasında ne ölçüde etkili olabilir? Siber saldırıların, keza siber caydırıcılığın doğrudan ve dolaylı etkisi nasıl hesap edilecektir? Bu açıdan bakıldığında toplam etki analizinin (doğrudan ve dolaylı) yapılması oldukça zor gözükmektedir. Kaldı ki burada siber saldırıların yol açtığı ekonomik, sosyal vb. maliyetleri de hesaba katmak gerekmektedir.

Özetle siber uzay siyasi, askeri, ekonomik, hukuki, adli ve teknik boyutlarıyla cevaplardan ziyade henüz yanıtlanamayan soru ve sorunlarla dolu bir alana işaret etmektedir. Kuşkusuz stratejik zorluklar, stratejik çözümler gerektirmektedir ki bu minvalde stratejik siber savunma da "bütüncül" ve "entegre" bir güvenlik yaklaşımının inşasına ihtiyaç duymaktadır. Bu bağlamda siber saldırılara karşı sadece devletler ile kamu kurum ve kuruluşlarından müteşekkil ortaklarla değil hassaten özel sektörle endüstriyel iş birliği yapılması gerektiği de aşikardır. Bu perspektiften yaklaşıldığında devletler, bölgesel/uluslararası örgütler ve özel sektör arasında tesis edilecek güçlü bir ilişki siber mücadeledeki eş güdümlü iş birliğini bir üst seviyeye taşıyacaktır. Ayrıca teknolojik inovasyon ve uzmanlık kazanımı için bilgi paylaşımı, tatbikat, mesleki ve teknik açılardan personelin eğitim ve öğretim uygulamalarına ağırlık verilmesi gereğinin altı çizilmelidir.

Mevzu Türkiye açısından değerlendirildiğinde Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın hazırlanması, Siber Savunma ve Füzyon Merkezleri'nin açılması, Ulusal Siber Güvenlik Tatbikatları düzenlenmesi veyahut kamu kurum ve kuruluşlarının KamuNET'e dahil edilmesi siber güvenlik ve savunma alanındaki farkındalığın gittikçe arttığının bir göstergesi ve kanıtıdır. Bu

bilince rağmen Türkiye'deki siber güvenlik personelinin sayısı ve yetkinliğindeki gelişim hızı/düzeyi karşılaşılan tehdit çeşitliliği ve seviyesiyle mukayese edildiğinde oldukça düşük seyretmektedir. Neticede kritik altyapıların ve akıllı sistemlerin buluştuğu alanda risk daha fazla yükselmektedir. Ulusal ölçekte haberleşme, enerji, finans, su gibi kritik altyapıların bilişim sistemlerini analiz etmek suretiyle muhtemel tehditleri ortaya koyan siber güvenlik odaklı çalışmalar daha fazla yürütülmelidir. Keza siber-uzay kaynaklı tehditlere karşı gerekli önlemlerin alınması noktasında ilgili kamu kurumları ve özel sektör arasındaki eş güdüm ve koordinasyon kadar konuya ilişkin mevzuat hükümlerinin düzenleyiciliği ve denetimine de hassasiyetle dikkat edilmelidir.

Kısaca Türkiye sadece mevcut risk ve tehditleri yönetebilecek şekilde siber saldırılara karşı önleyici yahut etkilerini azaltacak tedbirler almakla değil, aynı zamanda geleceğin siber-uzay trendini ön görebilecek teknolojik altyapıya ve entelektüel birikime sahip olmakla da mükelleftir. Mevzubahis trend bağlamında özellikle iki hususun altı çizilmelidir. Birincisi, Robot Çağı'na doğru hızla ilerlediğimiz, ikincisi ise savunma ve güvenlik sistemleri söz konusu olduğunda en kritik bileşenler olarak karşımıza yazılımların çıktığıdır. Dolayısıyla hazır alım suretiyle yurtdışından tedarik edilen sistemlerde siber güvenlik tedbirlerinin alınması çok elzemdir. Türkiye'nin bu konudaki farkındalığına binaen satın almak istediği savunma ve güvenlik sistemlerinde artık siber tedbirleri ister olarak şartnamelerde kayıt düşmesi, ziyadesiyle önemlidir. Zira unutulmamalıdır ki İHA'lar, savaş uçakları, gemiler, yolcu uçakları, büyük tankerler gibi sıralayabileceğimiz askeri ve sivil kullanım amaçlı tüm araç ve teçhizatlar, yazılım ve kodlamalar içermektedir. Nitekim Leon Panetta'nın "Siber Pearl Harbor" benzetmesi ya da Cengiz Karaağaç'ın "İnsansız 11 Eylül saldırıları" tabiri aslında teröristlerin bilfiil harekata müdahil olmalarına gerek duymaksızın yazılımlar vasıtasıyla yakın gelecekte vukû bulması kaçınılmaz gözüken, bu nedenle gerekli tedbirlerin ivedilikle alınmasına işaret eden stratejik sürprize dayalı terör eylemleri açısından dikkat çekicidir.

Sonuç olarak Türkiye devlet ve devlet-dışı aktörler üzerinden siber-uzay alanındaki trendi okurken "operatif", "saldırgan" ve "savunmacı" şeklinde üç temel alana eğilmek durumundadır. Mevzubahis alanlardaki trendlerin ise; propaganda stratejisi, hedef kitle, istihbarat toplama, bilgi paylaşımı ve güvenliği, finansman, endüstriyel casusluk, suç ve terörizm bağlantısı, devlet ve devlet-dışı aktörler arasındaki ilişki ağı gibi muhtelif parametreler üzerinden tespit ve teşhis edilerek yakından izlenmesi gerekmektedir.

Netice itibarıyla siber-uzay sunduğu büyük fırsat ve kolaylıklarla günümüzün vazgeçilmez bir fenomeni haline geldiği kadar yarattığı tehdit ve risklerle adeta bir "kıyamet silahı" olma potansiyelini de bünyesinde taşımaktadır. Bu yönüyle artık bilim-kurgu filmlerinin fantastik senaryolarının ötesine geçmiş, yaşanan deneyimlerle günlük hayatın bir gerçeği haline gelmiştir. Görülen o ki çağımızın yeni rekabet ve savaş alanları da bu kompleks ve münteşir cephede olacaktır.

Elinizdeki çalışma siber-uzayı bireyin ve devletin güvenliğine ilişkin tehdit algılamalarından öteye taşımakta, küresel güvenlik ortamındaki belirsizlik ve istikrarsızlığı tetikleyici başat ögelerden birisi olarak yansıtmaktadır. Bu minvalde siber-uzay alanındaki gelişmelerin günümüzde ulaştığı noktayı, bireysel ve kolektif güvenlik sorunlarına etkisi, tehdit algısının boyutu, savaş alanının sui generis karakteristiği, mücadelenin çehresi ve seyrine odaklanarak güncel vakalar üzerinden izah etmektedir. Çalışmada siber güvenlik alanının, ulusal ve global ölçekli teknolojik ve kriminolojik bir sorundan, stratejik bir meseleye evriminin serencamına da yer verilmektedir. Ayrıca yeni siber tehdit alanları ve türleri karşısında ulusal ve uluslararası/uluslarüstü düzeyde yerel ve uluslararası aktörlerin alabileceği her türlü güvenlik önlemleri, iş birliği ve koordinasyon mekanizmalarıyla birlikte hukuki ve diğer caydırıcı unsur ve uygulamaların neler olabileceği de tartışılmaktadır.

SETA

ANKARA • İSTANBUL • WASHINGTON D.C. • KAHİRE

www.setav.org