Ekonomi ve Dış Politika Araştırmalar Merkezi

edam

EDAM Siber Politikalar Kağıtları Serisi
2017/2

Siber Savaş:

Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında

Eylül 2017

Dr. Can Kasapoğlu
Savunma Analisti, EDAM

This paper was supported by

Robert Bosch Stiftung

ÖZET

Siber Savaş, günümüzde çok popüler halen gelen, ancak uzmanlar arasında dahi kavramsallaşma sürecini henüz tamamlayamamış bir kavramdır. Örneğin güvenlik bilimleri ve askeri bilimler çalışmalarında "denizaltı harbi nedir" ya da "kimyasal harp nedir" sorularının büyük oranda uzlaşılan yanıtları var iken, aynısını siber harp için söylememiz henüz mümkün değildir. Bahse konu tartışmalar yalnızca stratejik araştırmalar ile de sınırlı kalmamakta. Eğer siber-uzayda ve siber enstrümanlar ile "savaştan" söz edecek isek, siber savaş suçlarının neler olduğunun ve silahlı çatışmalar hukukunun siber-uzaya nasıl uygulanacağının da bilinmesi gerekmektedir. Ayrıca, gerek silahlı çatışmalar hukuku gerekse uluslararası insancıl hukuk açısından "savaş" olgusunun değerlendirilmesi için sivil ve askeri hedef ayrımı, orantılılık prensibi, meşru müdafaa gibi tüm hususların da siber-uzay ve siber enstrümanlar temelinde açıklığa kavuşturulması gerekmektedir. Son olarak, tüm bunların yapılabilmesi için "siber-silah nedir" sorusunun da detaylı biçimde cevaplanması zorunludur.

Siber silahların ne olduğunu tanımladıktan ve siber savaşı hukuki olarak kavramsallaştırdıktan sonra – ki uluslararası toplum bu noktadan çok uzaktadır – bu kez de gündeme siber savaşın önlenmesi gelecektir. Söz konusu amaca ulaşmak için siber silahları kapsayan bir silahsızlanma rejimi (örneğin NPT rejimi veya Avrupa Konvansiyonel Kuvvetler Antlaşması), bu rejimi denetleyecek uluslararası bir mekanizma (Uluslararası Atom Enerjisi Kurumu ya da Kimyasal Silahların Önlenmesi ve Yasaklanması Kurumu gibi) ve bir de verikifasyon yöntemi gerekecektir. Uluslararası toplum, bu sayılanlara da henüz çok uzaktır.

Elbette, bir yandan yukarıda sayılanlara duyulan gereksinim artarken, bir yandan da dünyanın hemen her ülkesinin silahlı kuvvetler teşkilatları siber-uzaya ve siber enstrümanlara uyum sağlamayı –değişik hızlarda– sürdürmektedir. Dünyanın birçok ülkesinde siber komutanlıklar kurulmakta, siber-uzay ve siber enstrümanlar savaşın diğer unsurlarıyla birlikte müşterek harp anlayışıyla kullanılmaktadır.

Bu çalışma, siber harbin stratejik ve uluslararası hukuki kavramsallaştırılması için konuya akademik ve profesyonel ilgi duyan okuyucular için bir giriş ve referans olması amacıyla kaleme alınmıştır. İlk bölümler kapsamında siber savaşın değerlendirilmesinde temel esaslar açıklanmakta, müteakip olarak siber imkan ve kabiliyetlerin harbin karakteristik niteliklerinde neden olabileceği değişiklikler irdelenmektedir. Son olarak siber yeteneklerin gerçek harp ortamında diğer kuvvetler ile müşterek olarak kullanıldığı bir vaka analizinin ardından, sonuç ve öneriler paylaşılmaktadır.

KAVRAMSAL ÇERÇEVE: SİBER SAVAŞIN TANIMLANMASI

Siber yetenekler dünyada toplumların ve bireylerin birbirleriyle üst seviyede 'karşılıklı bağlantılı' ve 'gerçek-zamanlı' iletişim halinde oldukları mevcut durumda, sadece savaş halinde değil, barış zamanında ve savaş-eşiği altında kalan çatışmalarda önemli manipülasyon ve dezenformasyon araçları sağlamaktadır. Günümüzde hemen her çatışmanın ve siyasi sorunun, bir 'YouTube cephesi' bulunması tesadüf değildir[1]. Bilgi harbi yoluyla kitlelerin davranışları ve algılarına nüfuz edilmesi de her dönemde kritik bir hedef olmuştur. Soğuk Savaş sırasında, özellikle 1970'li ve 1980'li yıllarda ABD'ye iltica eden Sovyet ajanlarının ifadeleri, Sovyetler Birliği'nin o dönemdeki istihbarat önceliklerinin arasında siyasal hareketlerin etki altına alınmasının espiyonajdan daha önemli olabildiğini göstermektedir[2]. Dolayısıyla, günümüzde önemli bir yer tutan siber güvenlik sorunlarının, tarih boyunca yaşanan rekabetin bilgisayar ve iletişim teknolojileri ile daha güçlü ve etkin araçlara erişimi olarak betimlenmesi mümkündür. Nitekim, konuya ilişkin çalışmalar, özellikle uluslararası kriz durumlarında sosyal medyada 'bot' adı verilen 'web robotlarının' propaganda ve manipülasyon faaliyetlerinin sistematiklik arz ettiğini ortaya koymaktadır. Bu durumu, 'bilginin silah haline getirilmesi' olarak yorumlayan uzmanlar da mevcuttur[3].

Öte yandan, yukarıda değinilen konuların siber savaş olarak nitelendirilmesi de mümkün değildir. Açıkçası, siber harp kavramının ne olduğunun anlaşılması için, öncelikle 'ne olmadığının' doğru anlatılması gerekmektedir. Zira, popüler kullanımda, siber enstrümanlar kullanılarak icra edilen her uluslararası rekabet faaliyeti 'siber savaş' olarak lanse edilebilmektedir.

Siber suçların ve hatta siber espiyonajın doğrudan siber harp kapsamında değerlendirilmesi gerçekçi olmayacaktır. Gerçekten de, bilgi harbi, propaganda ve hatta demokratik seçim süreçlerine müdahaleler ile dünyanın bir "siber soğuk savaş" dönemine sürükleniyor olması mümkün olsa da, henüz siber-uzayda silahlı çatışmalar hukuku ve askeri bilimler tarafından 'savaş' olarak tanımlanabilecek boyutta bir çatışma yaşanmamıştır. Ayrıca, 'siber harp' kavramının 'siber güvenlik', 'siber saldırı' ya da 'siber espiyonaj' yerine kullanılması da sakıncalıdır, zira siber-uzayda devletler arası ilişkilere dair norm oluşturulması için, hukukçular, diplomatlar, teknik siber uzmanlar, devlet adamları ve güvenlik bilimleri akademiyası arasında terminolojik birliktelik sağlanması önemlidir. Konuya dışarıdan bakanlar, siber ağların yalnızca internetten oluştuğunu düşünebilirler. Oysa ki, siber-uzay, herkesin kullanımına açık olan ve hatta teşvik edilen internetin ötesinde, fiziksel boyutlarda var olan altyapıları ve tesisleri idare eden kapalı kontrol sistemlerini de içermektedir. Söz konusu sistemlere yapılacak siber saldırılar kinetik etkileri dolayısıyla (örneğin genel elektrik kesintileri ya da kritik tesislerde SCADA [supervisory control and data acquisition] sistemlerinin manipüle edilmesi) geniş çaplı can ve mal kaybına neden olabilir. İşte, siber harbe ilişkin tartışmalar da, tam da bu kinetik etkiler dolayısıyla gündeme gelmektedir[4].

1 Rebecca A, Keller. Influence Operations And The Internet: A 21st Century Issue,The US Air War College – Air University, 2010.

2 Deborah Yarsike, Ball. Protecting Falsehoods With a Bodyguard of Lies: Putin's Use of Information Warfare, NATO Defense College, 2017.

3 Ibid.

4 Panayotis, A. Yannakogeorgos, "Keep Cyberwar Narrow", The National Interest, Mayıs 2013, http://nationalinterest.org/commentary/keep-cyber-war-narrow-8459, Erişim tarihi: 31 Ağustos 2017.

SİLAHLI ÇATIŞMALAR HUKUKU VE SİBER SAVAŞ: HUKUKİ KAVRAMSALLAŞTIRMA ÇABALARI

Literatürde siber harbin birçok kez asimetrik bir konsept olarak ele alındığı görülmektedir. Bu yaklaşımlara göre, konvansiyonel olarak zayıf olan tarafın hareket tarzı gibi algılanan siber harp yetenekleri, özellikle aksiyon – reaksiyon dengesini bozan hızı ile dikkat çekmiştir. Ayrıca, bu askeri mücadele biçimi, aktörlerin "silahlı çatışmaya gerek duymadan" hedeflerine ulaşacakları bir strateji olarak takdim edilmiştir. Daha da önemlisi, siber harbe ilişkin birçok tartışma, bilimkurgu dünyasına daha yakın duran anekdotlar üzerinden sürdürülmüştür[5].

Silahlı çatışmalar hukukuna dahil olan temel antlaşmalar arasında henüz siber saldırılar ve siber silahlara ilişkin özel ve norm teşkil eden bir unsur yoktur. Ancak, insancıl hukuk kapsamında siber çatışmayı kapsayan daha genel yorumlar yapıldığı, günümüzdeki ve gelecekteki 'siber silahların' da bu hukuki değerlendirmeler kapsamında ele alındığı bilinmektedir.

Siber harp olgusunun popüler tartışmaların ötesinde, hukuki ve teknik olarak tanımlanarak konuya ilişkin uluslararası bir konsensüs oluşturulması büyük önem arz etmektedir. Bu bağlamda, siber harbin gerçekleşmesi için bilinen askeri imkanlarla oluşturulabilecek bir yıkıma neden olma kriterleri ve silahlı çatışmalar hukukunun siber saldırılar karşısında ne derecede uygulanabileceğine ilişkin bazı çalışmalar olsa da, uluslararası toplumun halen katetmesi gereken uzun bir yol vardır.

Özellikle devlet düzeyindeki aktörlerin, siber alanda / siber enstrümanlar ile yaşanan bir çatışmanın kontrolsüz tırmanmasına engel olmak amacıyla gerekli uluslararası mekanizmaları inşa etmesi büyük önem arz etmektedir. Örneğin, bir siber saldırı karşısında verilecek meşru yanıtın sınırlarının ve şartlarının belirlenmesi kritik bir husustur. Bu çerçevede, düşmanca bir siber eylemin, boyutları, failleri ya da sonuçları açısından, hangi koşullarda Birleşmiş Milletler Sözleşmesi 51. Madde kapsamında meşru müdafaa hakkı doğuracağına ilişkin hukuki bir anlayışın oluşturulması zaruridir. Bu noktada, kritik ulusal altyapıya yönelik kinetik etki doğuran saldırılar bir kriter olarak alınacak ise, o halde kritik ulusal altyapının ve kinetik etkinin de ayrıca tanımlanması gerekecektir. Ayrıca, birçok siber saldırı devlet sponsorluğunda, vekaleten (proxy) biçimde gerçekleşmektedir[6]. Dolayısıyla, meşru yanıtın hangi durumlarda ve hangi uluslararası hukuki gerekçeler ile kaynak ülkeye yönelebileceği de ayrı bir tartışma konusudur. Son olarak, siber saldırıların klasik bir silahlı saldırı sayılmasına ilişkin kriterler berrak biçimde belirlense dahi, saldırının sivil hedeflere mi askeri hedeflere mi yöneldiğinin net biçimde anlaşılması gerekecektir. Zira, bir silahlı saldırıyı değerlendirirken önemli hukuki çerçevelerden biri de hedefin niteliklerdir[7].

SİBER SAVAŞ SIRASINDA SİVİL VE ASKERİ HEDEF AYRIMI İMKANSIZ MI?

Son olarak, yukarıda belirtilen sorunsallar aşılsa dahi, askeri hedeflere yönelen bir siber saldırının beklenen sonuçları oluştururken sivillere – istemeden de olsa – verebileceği zarar (collateral damage) nasıl ölçülecektir? Günümüzde akıllı mühimmatlara ve gelişmiş muharebe ağlarına sahip silahlı kuvvetler, bu tür kaygıları teknoloji-yoğun harekatlar ile bir yere kadar aşabilmektedir. Ancak siber silahlar için böyle bir avantaj her durumda söz konusu olmayabilir.

5 Paul, Cornish. David, Livingstone. and Claire Yorke. On Cyber Warfare, Chatham House, Londra, 2010, p.vii.

6 Sinan, Ulgen. Governing Cyberspace: A Road Map for Transatlantic Leadership, Carnegie Europe, 2016, pp.60-64.

7 Ibid.

Söz gelimi, bir ülkede internet ağlarının ve servislerinin çökertilmesi muhakkak sivillerin zarar görmesine neden olacaktır[8]. Yine, siber silahların özgün nitelikleri dolayısıyla, ofansif tarafın askeri planlayıcılarının muhtemel sonuçları önceden kestirmesi zordur. Sadece söz konusu nitelik dahi, siber enstrümanlara ilişkin kitle imha silahlarına ya da konvansiyonel yeteneklere yönelik silahsızlanma girişimlerine benzer inisiyatiflerin gündeme gelmesine neden olmaktadır.

SİBER SİLAHLARIN KONTROLÜ VE SİBER SİLAHSIZLANMA MÜMKÜN MÜ?

Bu noktada, silahsızlanma ve silahlanmanın sınırlandırılmasına ilişkin uluslararası ilişkiler ve uluslararası hukuk çerçevelerinin 'siber silahlara' teşmil edilip edilemeyeceğinin anlaşılması büyük önem taşımaktadır. Zira, siber silahların nasıl ve hangi parametrelerde sınırlandırılacağı / sınırlandırılabileceği tek bir yapıya sıkışmış değildir. Siber silahların sınırlandırılmasına ilişkin bağlam, nükleer silahlara mı yoksa konvansiyonel silahlara mı daha çok benzeyecektir? Ya da daha farklı bir gereksinimden mi hareket edilecektir? Bu sorulara uluslararası toplum tarafından verilecek yanıtlar siber savaş olgusunun geleceğini de belirleyecektir.

Silahsızlanma ve silahlanmanın önlenmesi / sınırlandırılması rejimleri nedenleri ve sonuçları bağlamında birbirlerinden farklılık göstermektedir. Bu tip düzenlemeler, silahlanmaya nitelik ve nicelik açısından sınırlandırmalar getirebilir (örn. Avrupa Konvansiyonel Kuvvetler Antlaşması), bazı tür ve nitelikte silahların kullanılmasını yasaklayabilir (örn. Ottawa Sözleşmesi), bazı silahlara ilişkin deneme faaliyetlerini sınırlandırabilir (örn. Kısmi Nükleer Deneme Yasağı Antlaşması), ya da bazı silahların üretimi ve stoklanmasını engelleyebilir (örn. Kimyasal Silahların Yasaklanması Sözleşmesi). Sayılan tüm bu rejimler silahlı çatışmalar hukukundan farklılık arz etmektedir. Zira, bu tip düzenlemelerin amacı, savaş zamanında devlet davranışlarının düzenlenmesi değil, bizatihi çatışma durumunun ve tırmanmanın engellenmesidir[9].

Peki ofansif siber yeteneklere ilişkin bir sınırlandırma – eğer yapılacak ise – hangi koşullara ve parametrelere göre düzenlenmelidir? Silahsızlanma ve silahlanmanın sınırlandırılmasına ilişkin düzenlemeler belirli kategorik sonuçlara ulaşmak için yapılır. Bu kapsamda devletler arasında askeri dengesizliklerin minimize edilmesi, tahmin edilebilirliğin yükseltilmesi, yeni silahlar geliştirilmesinin mümkün olduğunca önüne geçilmesi, silahlanmaya ayrılan harcamaların kısıtlanması ya da silahlı çatışma olması durumunda geri dönülemez ve vahim derecede hasarların engellenmesi gibi motivasyonlardan söz edilebilir[10]. Elbette bu noktada, taarruzi (ofansif) siber silahın ne olduğunun tanımlanması ve hatta mümkünse kategorize edilmesi büyük önem taşımaktadır.

Kimi uzmanlar, 'siber silahların' hedef bilgisayar sistemlerine doğrudan erişime gerek duymayan (örn: internette yayılan virüsler), hedef bilgisayar sistemlerine doğrudan erişerek etki gösteren (, örn: SCADA sistemlerine nüfuz edebilen ve dolaylı kinetik etki oluşturan siber-ajanlar) olmak üzere iki ana kategoride ele alınabileceğini düşünmektedir. Bu yaklaşıma göre, olası bir siber silahsızlanma ya da silahlanma kontrolü rejimine tabi olacak unsurlar ikinci kategoride bulunacaklar arasından belirlenecektir[11].

Siber silahların herhangi bir uluslararası kontrol rejimine tabi olmaları için, askeri ve siyasi çevreler tarafından tıpkı kitle imha silahları ya da balistik füzeler gibi 'stratejik silahlar' çerçevesinde değerlendirilmesi önem arz etmektedir. Konuya ilişkin çalışmalar, askeri amaçla kullanılan siber yeteneklerin 'stratejik silahlar' seg-

8 Ibid.

9 Louise, Arimatsu. "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations", 4th International Conference on Cyber Conflict, NATO CCDCOE, 2012.

10 Ibid.

11 Kristine M. Rogers, Resistance is not Futile: The Case Against a Cyber Arms Treaty, Air War College, 2010, pp.4-5.

mentinde değerlendirilmesi için birinci ve en önemli koşulun bir ülkenin kritik ulusal altyapısına 'felaket düzeyinde' (catastrophic) bir zarar vermesi olduğunu belirtmektedirler. Bugüne kadar, siber silahların bir devletin mevcudiyetini ortadan kaldırabilecek, nükleer silahlara denk bir yıkıcılık geliştirdiğini gösteren somut kanıtlar olmamıştır[12]. Öte yandan, özellikle kritik ulusal altyapılarını ve ekonomilerini büyük oranda bilgisayar ağlarına taşıyan ülkeler için böyle bir tehdit ihmal edilebilir düzeyde de değildir. Ayrıca, nükleer silah rejimi bu silahların kullanılmaması üzerine kurulu iken; siber yetenekler barış durumlarında dahi kullanılabilmektedir. Dahası, siber saldırı altında olan bir devlet, kendisine saldıran aktörü tespit edemeyebilir. Nükleer taarruz için böyle bir durum neredeyse yoktur. Dolayısıyla ofansif siber yetenekler, sıklıkla başvurulabilen unsurlardır[13].

'Attribution', yani saldırının kaynağının tespit edilmesi hususlarında ise ofansif siber yeteneklerin biyolojik silahlar ile kıyaslanması daha gerçekçi olacaktır. Zira, biyolojik saldırı altında olan bir ülkenin, karşı karşıya kaldığı tehdidin bir salgın mı yoksa bir biyolojik harp faaliyeti mi olduğunu anlaması bazı durumlarda vakit alabilecektir. Dahası tıpkı kimi biyo-ajanların inkübasyon süreleri dolayısıyla bir süre gizlenerek daha sonra yıkıcı etkilerini gösterebilmesi gibi, bir siber-ajan da bilgisayar sistemleri içinde 'inkübasyon benzeri' bir süreç geçirebilir.

Şurası kesindir ki, 'siber silahlar', aynı kimyasal ve biyolojik silahlar gibi sivil ve askeri amaçlar için yararlanılabilecek, çift-kullanımlı (dual-use) teknolojilere dayanmaktadır. Ayrıca, nükleer silahlar günümüz itibariyle devletlerin tekelinde iken, en son IŞİD tehdidi ve El Kaide'ye bağlı grupların terör trendleri, kimyasal silahların devlet-dışı gruplar tarafından da kullanılabildiğini göstermektedir. Siber silahlar için de böyle bir durum söz konusudur. Birçok devlet-dışı grup siber yeteneklere sahiptir.

Ancak, kimyasal silahlarla ilgili silahsızlanma ve silahların kontrolü rejimleri örnek gösterilse de, yine de siber silahların sınırlandırılmasında önemli bir hukuki zorluk bulunmaktadır. Zira, kötü amaçlı yazılımlar (malware) bir sisteme zarar vermek için kullanılacağı gibi, sistemin açıklarını ya da ihtiva ettiği verileri ve bilgileri öğrenmek amacıyla espiyonaj faaliyetleri için de kullanılabilir (spyware). Ancak, bahse konu casus yazılımlar, ardından gelebilecek yıkıcı kötü amaçlı yazılımlara da zemin hazırlarlar. Bu bağlamda, ünlü Stuxnet yazılımına katkıda bulunan Duqu casus yazılımı iyi bir örnektir[14]. Daha açık bir ifadeyle, söz gelimi, dolaylı kinetik etki sahibi Stuxnet bir siber-silahsızlanma sözleşmesine konu olacak ise, Duqu casus yazılımını bu bağlamda nereye koymak gerekecektir?

Altı çizilmelidir ki, uzmanların siber silahlarla ilgili herhangi bir kontrol rejiminde öngördükleri en büyük zorluk, tarafların düzenlemeye uymadıklarının (non-compliance) belirlenmesi olacaktır. Zira, devletlerin, bilgisayar sistemlerini tarayacak bir verifikasyon rejimine sıcak bakmayacakları açıktır. Böylelikle, denetleyici ve yaptırım gücünü haiz bir uluslararası mekanizmanın olmadığı, verifikasyon rejiminin bulunmadığı ya da sınırlı olduğu bir siber silahların sınırlandırılması konsensüsüne varılsa dahi, ortaya çıkacak durum Biyolojik Silahların Yasaklanması Sözleşmesi ile hayli benzeşecektir, yani kontrol mekanizmaları etkisiz kalacaktır[15].

Son olarak vurgulanmalıdır ki, silahların sınırlandırılması ve silahsızlanma rejimleri, uluslararası hukuki mülahazalar kadar, hatta daha fazla, siyasi-askeri değerlendirmelere dayanırlar. Örneğin, Soğuk Savaş sonrasında Rusya Federasyonu'nun ve ABD'nin kimyasal silahlara daha fazla ihtiyaç duymadıklarına ilişkin stratejik değerlendirmeleri Kimyasal Silahların Yasaklanması Sözleşmesi'ni ve ilgili silahların kontrolü

12 Ayrıntılı bilgi için bkz. Andrew, F. Krepinevich, Cyber Warfare: A 'Nuclear Option'?, CSBA, 2012.

13 Ibid.

14 Louise, Arimatsu. "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations", 4th International Conference on Cyber Conflict, NATO CCDCOE, 2012.

15 Ibid.

rejimini beraberinde getirmiştir[16]. Dolayısıyla izlenmesi gereken esas parametre, böyle bir oydaşmanın uluslararası toplumun önemli ve yükselen siber aktörlerinde bulunup bulunmadığıdır.

Nitekim 2011 yılında Rusya Federasyonu, Çin Halk Cumhuriyeti, Tacikistan ve Özbekistan'ın BM nezdindeki bir girişimi, Washington ve Moskova arasındaki görüş ayırılıkları nedeniyle sonuca ulaşmamıştır. Burada dikkat çekici husus, bir siber kontrol rejiminin otoriter devletler tarafından internet ve bilgi akışına yönelik sansür aracı olarak kullanılmasından duyulan endişedir. Bir diğer konu da, ABD gibi teknolojik üstünlüğü elinde bulunduran aktörlerin bu yeteneklerinin uluslararası mekanizmalar tarafından sınırlandırılması ve kontrol edilmesinden imtina etmeleridir. Söz konusu engeller aşılmadan, siber savaş kapasitesine ilişkin somut adımlardan bahsetmek zordur.

Elbette, siber-uzayda bir silahlanma yarışına engel olunmasına yönelik gereksinimler her geçen gün artarken, bir yandan da bir yandan da dünyanın önde gelen silahlı kuvvetleri siber-uzaya ve siber enstrümanlara uyum sağlamayı –değişik hızlarda– sürdürmektedir.

Bu çerçevede, birçok ülkede siber komutanlıklar kurulmakta, siber-uzay ve siber enstrümanlar savaşın diğer unsurlarıyla birlikte müşterek harp anlayışıyla kullanılmaktadır. Türk Silahlı Kuvvetleri de 2013 yılında bünyesindeki Siber Savunma Merkezi'ni bir Siber Komutanlık'a dönüştürerek önemli bir adım atmıştır. NATO standartlarında görev yapan bahse konu komutanlığın kuruluşu, Silahlı Kuvvetler'in Muhabere ve Elektronik Bilgi Sistemleri (MEBS) kapasitesinin geliştirilmesi ve milli siber savunma çözümleri açısından önemli bir gelişmedir[17].

Ayrıca, bu çalışmanın ileriki bölümlerinde açıklanacağı üzere, siber yetenekler ve elektronik harp günümüzde birbirinden ayrılmaz askeri görevlerdir. Bu bağlamda da, TSK'nın ve Türk Savunma Sanayiinin son dönemdeki atılımları dikkat çekicidir. 2017 yılı başında ASELSAN ile imzalanan protokolün üç yıllık sürede elektronik harp yeteneklerinde ciddi artış sağlaması hedeflenmektedir[18].

Sayılan tüm olumlu gelişmelere karşın, Türkiye'nin siber harp konusunda halen katetmesi gereken önemli mesafeler de bulunmaktadır. Öncelikle konuya ilişkin akademiya, kamu, özel sektör ve düşünce kuruluşlarının düzenli ve etkin işbirliğini sağlayacak mekanizmalarım kurulması ve konsept üretilmesi kritik bir zarurettir. İkincisi ve daha önemlisi, dünyada süregelen ofansif siber yetenekler tartışmasının Türkiye'de –yeterince– yapılmıyor olması, siber askeri modernizasyonunun gelişim yönüyle ilgili daha yoğun bir entelektüel çabanın gerektiğini göstermektedir. Üçüncü olarak, özellikle Türkiye'nin yakın çevresinde hava savunma kapasitelerindeki artış, siber ve elektromanyetik kapasitenin ciddi biçimde geliştirilerek derin taarruz yeteneklerine entegre edilmesinin yaşamsal önemi olduğunu göstermektedir. Savunma modernizasyonunda bu yönde daha geniş kapsamlı adımlara ihtiyaç duyulmaktadır. Belirtilenlere ek olarak, siber çatışmanın 'savaş eşiği altında' gri bir alanda vuku bulduğu unutulmamalıdır. Ülkemizde çeşitli kurumlara bağlı sürdürülen çabalar ile ile siber-elektromanyetik askeri gelişmelerin eşgüdümünün sağlanması ve savaş eşiği altında kalan durumlar için gerekli vizyonun oluşturulması kritiktir.

SİBER SAVAŞ: MEŞRU HEDEF NASIL TANIMLANMALI?

Siber harbin icrasına ilişkin silahlı çatışmalar hukuku konusunda önemli bir nokta da, 'meşru hedefi' kimlerin ve nelerin teşkil edeceğidir. Tarih boyunca siviller ile askeri personel ayrımı keskin parametrelere

16 Ibid.

17 Hurriyet, http://www.hurriyet.com.tr/turk-ordusunun-yeni-kuvveti-siber-savunma-40113652, Erişim tarihi: 10 Eylül 2017.

18 Sabah, http://www.sabah.com.tr/ekonomi/2017/03/02/aselsan-ile-tsk-elektronik-harp-anlasmasi-imzalandi, Erişim tarihi: 10 Eylül 2017.

dayanmıştır. Elbette, askerlerin üniforma kullanmaları ve askeri tesislerin ayırıcı işaretlere sahip olması bu konuda ilk emareyi oluşturmuştur. Yine tarih boyunca, 'harp sahası' olgusu, sivillerin ve sivil yerleşimlerin kesin olarak çatışma bölgelerinden ayrılabilmelerine olanak sağlamıştır. Öte yandan, sivil ve askeri hedefler arasındaki ayrım giderek bulanıklaşmaktadır. Özellikle İkinci Dünya Savaşı ile birlikte gelişen trendler, sivillerin askeri harekatlardan korunmasında ciddi zorluklar olduğunu ve söz konusu zorlukların yükseldiğini göstermektedir[19]. - 21. Yüzyılın çatışmalarının ise, meskun mahalde harp şeklinde tezahür eden, hibrid nitelikli bir profil sergilemesi sivilleri doğrudan bir çevresel unsur haline getirmiştir. Konu siber harp olunca, sivil ve askeri hedef ayrımı yapılması oldukça güçtür. Esasen, bazı uzmanlar siber savaşın harp tarihi boyunca sivil ve askerler arasındaki ayrımın tamamen ortadan kalkacağı bir eşik olacağını değerlendirmektedir[20].

Bu noktada sorulması ve uluslararası toplum tarafından anlamlı bir konsensüs ile yanıtlanması gereken soru şudur: herhangi bir siber saldırı savaş nedeni sayılabilir mi ve askeri mukabeleyi meşru kılabilir mi?

Bu konuda kuşkulu olan birçok uzman, siber saldırıların – henüz – sınırlı hasar verme yeteneğine sahip olması ve verilen hasarların sıklet merkezinin çoğunlukla ekonomik hedefler ya da sonuçlar olması dolayısıyla salt askeri bir çerçevede değerlendirilemeyeceğini öne sürmektedir. Konuya daha farklı yaklaşanlar ise siber saldırıların dolaylı kinetik etkilerinin, örneğin genel elektrik kesintilerinin, can kaybına neden olabileceği ve bir ülkede hayatın akışına ve asayişe vahim zarar verebileceği için bir silahlı saldırı gibi değerlendirilebileceğini düşünmektedir[21]. Bahse konu bakış açısına göre, doğrudan kinetik etki ile (örneğin elektrik altyapısının balistik füzelerle tahrip edilmesi ile) dolaylı kinetik etkiler arasında (elektrik altyapısının ofansif siber yetenekler ile akamete uğratılması) arasında son kertede ortaya çıkacak durum açısından pek fark olmayacaktır. Siber savaşın – ya da gelecekte yaşanabilecek olası siber savaşların – silahlı çatışmalar hukuku için oluşturduğu bir diğer engel de coğrafya ve coğrafyaya bağlı devletin egemenlik alanı kavramlarını bir ölçüde anlamsızlaştırmasıdır. Uluslararası ilişkilerde modern devletlerin egemenlikleri ile siyasi coğrafyaları ve sınırları arasında organik bir ilişki vardır. Öte yandan, devletin egemenlik haklarını kullanacağı coğrafya bugüne dek, doğal olarak, hava sahası, karasuları gibi fiziksel niteliklere göre tanımlanmıştır[22]. Peki, bir bilgisayar ağını hedef alan virüs, coğrafi olarak bir devletin siyasal egemenlik haklarına tecavüz etmiş sayılabilir mi? Zira, BM Sözleşmesi'nin 2. Maddesi, devletlerin toprak bütünlüklerine, ülke topraklarına ve işbu topraklar üzerindeki egemenlik haklarına ve bağımsızlıklarına yönelik eylemleri yasaklamaktadır. O halde, yukarıdaki örnekte bahsettiğimiz siber-ajan, BM Sözleşmesi'nin ilgili maddesi kapsamında bir ihlalin sebebi olarak değerlendirilebilir mi? Eğer gerçekten de siber enstrümanlar –tıpkı konvansiyonel silahlar ve kitle imha silahları gibi– BM Sözleşmesi'nin ülke egemenliğinin ve bağımsızlığının temel parametrelerine yönelik bir bir tehdit olarak algılanır ise bu enstrümanlara yönelik silahsızlanma ve silahlanmanın sınırlandırılması rejimileri daha sağlam bir temele dayanacaktır[23].

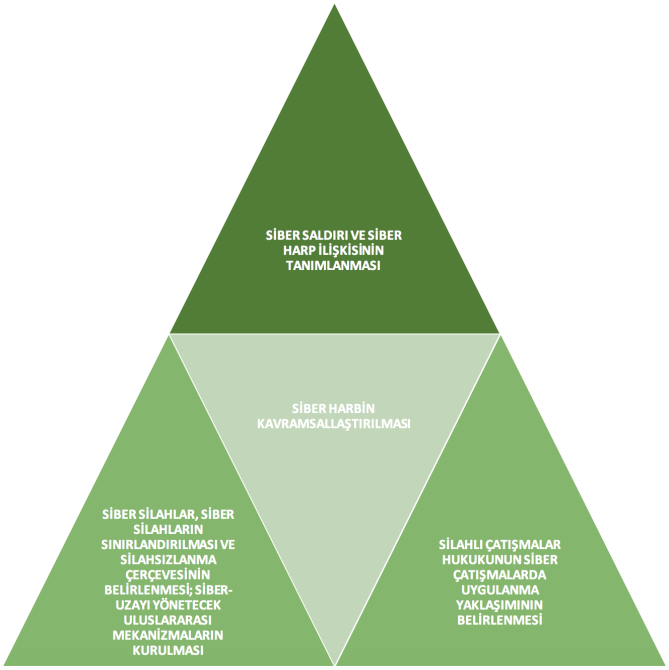
19 Claire Oakes, Finkelstein ve Kevin H. Govern, "Introduction: Cyber and the Changing Face of War", University of Pennsylvania Law School, Faculty Scholarship Paper 1566, 2015.

20 Ibid.

21 Claire Oakes, Finkelstein ve Kevin H. Govern, "Introduction: Cyber and the Changing Face of War", University of Pennsylvania Law School, Faculty Scholarship Paper 1566, 2015.

22 Claire Oakes, Finkelstein ve Kevin H. Govern, "Introduction: Cyber and the Changing Face of War", University of Pennsylvania Law School, Faculty Scholarship Paper 1566, 2015.

23 Ibid.



Siber savaşın bir askeri mesele olarak ele alınmasında elzem olan bir diğer husus da doktrin oluşturulmasıdır. Zira literatürde askeri doktrin, bir silahlı kuvvetler için "inanç sistemi" anlamına gelmektedir. Askeri doktrinler, silahlı kuvvetler teşkilatlarının nasıl savaşacağını, harp ve harekat ortamını nasıl algılayacaklarını, kurumsal ve stratejik kültür kodlarını, konseptleri ve kavramları belirlerler. Bu çerçevede askeri doktrinler, teknik, taktik, operasyonel, stratejik sorulara yanıt vermek ve on binlerce personelin eşgüdüm ile düşünmesi ve hareket etmesi amacıyla hazırlanır[24].

Peki, siber-uzay askeri fonksiyonları olan bir operasyonel harekat ortamı olarak tanımlanacak ise– ki NATO son olarak böyle bir adım atmıştır– bir siber harp doktrini hangi unsurları içerecektir? Burada sorduğumuz soru, değişik ülkelerin siber savaşa yönelik farklı bakış açılarının ötesine geçmektedir. Söz gelimi, dünyanın hemen her milli güvenlik dokümanı bir tehdit tanımı ve sıralaması yapmak durumundadır. Dolayısıyla, hangi ülke tarafından hazırlanırsa hazırlansın, bir siber harp doktrini birtakım elzem unsurları içermek zorundadır.

Literatürdeki çalışmalar bu konuda üç ana hususun üzerinde durmaktadır. Bunlardan ilki, siber saldırının failinin nasıl bulunacağı ve nasıl algılanacağına ilişkindir (attribution problem). Zira, günümüzde birçok devlet, siber saldırılar için vekil gruplar kullanmaktadır. Bu noktada, bir siber saldırı karşısında mukabelenin kime yapılacağının belirlenmesi büyük önem arz etmektedir[25]. Türk okuyucular için daha çarpıcı bir örnek vermek gerekirse, 1990'lı yılların sonunda Türkiye Cumhuriyeti, PKK terör örgütü ile mücadelede yeni bir konsept geliştirerek sorunun 'vekaleten harp' boyutuna odaklanmış ve Hafız Esad yönetimindeki Suriye Baas rejimi üzerinde, BM Sözleşmesi 51. maddeden doğan meşru müdafaa hakkını saklı tuttuğunu belirterek, doğrudan savaş tehdidi yoluyla baskı kurmuştur. 21. yüzyılda, vekaleten bir siber saldırı ile karşılaşan herhangi bir devletin, siber saldırıyı gerçekleştiren devlet-dışı vekil unsura mı, sponsor devlete mi mukabele edeceği çok kritik bir noktadır.

İkinci olarak, bir siber saldırının sonuçlarına ilişkin 'hasar tespitin' ve ofansif bir siber müdahalenin düşmana verdiği 'zayiata' ilişkin muharebe hasar kıymetlendirmesinin nasıl yapılacağı, bir siber harp doktrininin mutlaka ele alması gereken bir konudur. Bu noktada, dolaylı etkilerin ölçülmesi en büyük zorluğu teşkil etmektedir.[26]

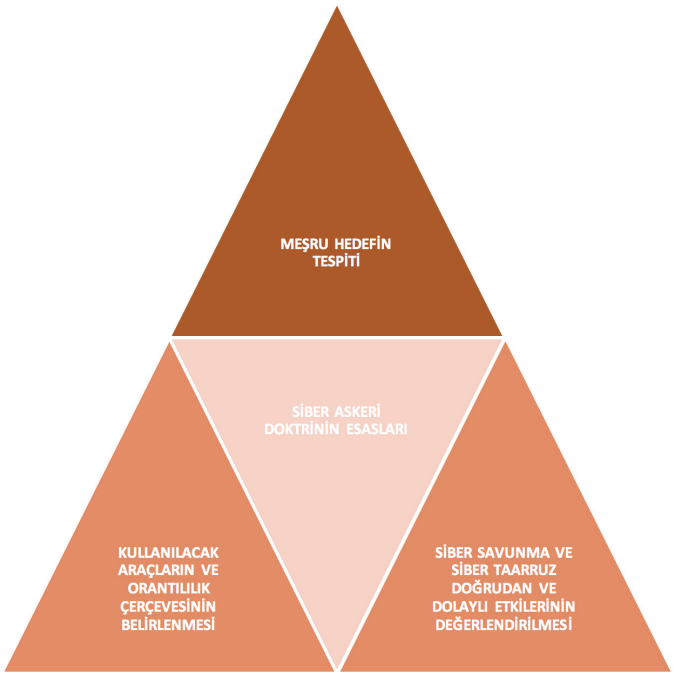
Üçüncü ve son olarak, orantılılık prensibi de dikkate alınmak suretiyle, bir siber saldırıya nasıl ve hangi enstrümanlar ile karşılık verileceği, bir siber askeri doktrinin yanıtlaması gereken bir diğer ana unsurdur[27]. Söz konusu husus, bir devletin siber harp tehdidine karşı ne ölçüde müşterek ve bütüncül bir yanıt vereceğini de gösterir niteliktedir.

24 Askeri doktrinlerin gelişimi üzerine ayrıntılı bir çalışma için, bkz: Aaron P. Jackson, The Roots of Military Doctrine: Change and Continuity in Understanding the Practice of Warfare, US Army Combined Arms Center, Forth Leavenworth, Kansas, 2013.

25 Jarno, Limnell ve Charly Salonius-Pasternak, Challenge for NATO: Cyber Article 5, Center for Asymmetric Threat Studies (CATS), 2016, p.2.

26 Ibid.

27 Ibid.



Yukarıda aktarılanlara karşın, siber harp olgusunu modern uluslararası ilişkiler ve silahlı çatışmalar hukuku çerçevesinde tanımlamak için ciddi bir zorluk bulunmaktadır. Hemen tüm siber saldırılar, savaş eşiğinin altında vuku bulmaktadır ve saldırgan devletle ilişkilendirilmelerinde ciddi problemler vardır[28]. Siber savaşa bütüncül bir bakış açısı getiren ve bu yeni olgunun harbin diğer unsurlarından ayrı düşünülmemesi gerektiğini öne süren uzmanlar ise siber saldırı ve siber savaş durumlarının, elektromanyetik spektruma bağlı siber boyut ile kısıtlı kalmayacağını, fiziksel coğrafi boyutlara da sirayet edeceğini belirtmektedirler. Bu varsayımın en önemli argümanı, Rusya'nın son dönemde eski Sovyet coğrafyasına yönelik müdahalelerinde (son olarak Ukrayna'da) siber araçları genel tırmandırma stratejisinin bir parçası olarak kullanmış ve halen kullanıyor olmasıdır. Bu çerçevede, Moskova'nın özel ve örtülü operasyonlar için 'harp sahasını' önce siber imkanlar ile 'hazırladığına' dikkat çekilmektedir[29].

Siber harbin kavramsallaştırılması hususunda dikkat çekilen bir diğer nokta da siber savaş (cyber war) ve siber çatışma (cyber conflict) kavramlarına ilişkin farklı yaklaşımların olabileceğidir. Bu noktada siber savaş fikrini benimseyen uzmanlara yönelik temel eleştiri, askeri ya da askeri-istihbari kurumlarca icra edilen tüm siber faaliyetlerin bir harp faaliyeti gibi değerlendirilmesindeki sakıncalardır. Bu anlayışa göre, siber harbi ayrı bir unsur olarak ele almak yerine, bilgisayar ve ağ teknolojilerine dayanan tüm silahlı kuvvetler teşkilatları için savaşın, her boyut ile, 'siberleşmiş' olduğunun doğru anlaşılması gerekmektedir. Bu anlayışa göre, siber boyutun fiziksel dört boyut ile (kara-hava-deniz / okyanus -uzay) etkileşimi sonucunda ortaya çıkan tablo, silahlı çatışmanın da giderek 'siberleştiğini' göstermektedir[30].

SİBER SAVAŞ VE ASKERİ İTTİFAKLAR: NATO ÖRNEĞİ

Harp, sadece askeri teknoloji ve teknikten ibaret olmayıp, uluslararası hukuk ve uluslararası ilişkilerin önemli bir unsurudur. Siber harpten söz edilecek ise, sivil ve askeri hedef ayrımı, BM Sözleşmesi kapsamında meşru müdafaa hakkı gibi hususların yanı sıra, askeri ittifaklardan ve siber saldırılar karşısında casus foederis'in, yani bir ittifakın hangi koşullar altında askeri seçenekleri ile harekete geçirileceğine ilişkin çerçevenin de analiz edilmesi gerekmektedir. NATO'nun kurucu antlaşmasının (Washington Antlaşması ya da Kuzey Atlantik Antlaşması) 5. maddesi casus foederis olgusunun günümüzdeki en somut ve caydırıcı örneklerinden birini teşkil etmektedir[31].

28 Kubo, Macak. "From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law", 9th International Conference on Cyber Conflict, CCDCOE, 2017.

29 Jen, Weedon. "Beyon 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine", Cyber War in Perspective: Russian Aggression against Ukraine, Kenneth Geers [ed.], NATO CCDCOE, Tallinn, 2015.

30 Peter, Dombrowski ve Chris C. Demchak. "Cyber War Cybered Conflict and the Maritime Domain", Naval War College Review, https://www.researchgate.net/profile/Peter_Dombrowski/publication/288670392_Cyber_War_Cybered_Conflict_and_the_Maritime_Domain/links/5682f34208aebccc4e0e1a3d/Cyber-War-Cybered-Conflict-and-the-Maritime-Domain.pdf?origin=publication_detail, Erişim tarihi: 30 Ağustos, 2017.

31 NATO, http://www.nato.int/cps/en/natohq/topics_67656.htm, Erişim tarihi: 31 Ağustos, 2017.

Peki NATO'nun ittifak üyesi devletlerden birine yönelik bir saldırı karşısında 5. maddeyi işletmesi mümkün müdür? 2014 Galler ve nihayet 2016 Varşova zirvelerinin sonucunda Kuzey Atlantik İttifakı bugün resmi olarak siber savunmanın (cyber defense) NATO'nun kolektif savunma görevlerinin bir parçası olduğunu belirtmektedir. Dahası, NATO, uluslararası hukukun siber-uzayı da kapsayacak şekilde uygulanabileceğini vurgulamaktadır[32]. Son olarak, Varşova Zirvesi'nde siber-uzayın operasyonel bir alan olduğunun belirtilmesi[33], ittifakın siber yeteneklerinin siyasi-askeri istikameti ile ilgili önemli bir fikir vermektedir.

NATO Genel Sekreteri Jens Stoltenberg, 2016 yılında Savunma Bakanları buluşması kapsamındaki basın toplantısında Der Speigel muhabirinin ittifak üyelerinden biri ya da birkaçına yönelik bir siber saldırı karşısında 5. maddenin işletilip işletilemeyeceğine ilişkin sorusuna, böyle bir saldırının söz konusu kolektif savunma şartını tetikleyebileceğini ancak her siber saldırıya karşı 5. maddenin işletilmesi gibi bir zorunluluğun olmadığını belirten bir yanıt vermiştir[34]. Esasen bu 'muğlak' yaklaşımın, hem ittifakın siber tehditler karşısındaki adaptasyon sürecini hem de mukabele seçeneklerinde esneklik tercihini ortaya koyduğu söylenebilir. Zira, henüz gelişme aşamasında olan siber çatışma ortamının konvansiyonel ve hatta nükleer silahları da içeren bir tırmanmaya neden olması uluslararası toplum için korkutucu bir durumdur. Nitekim, Genel Sekreter Stoltenberg, yukarıda sözü edilen basın toplantısı sırasında yöneltilen sorular arasında olan Rusya Federasyonu'nun ABD başkanlık seçimlerine müdahalesine yönelik soruya, NATO'nun siber yeteneklerinin herhangi bir ülkeyi hedef almadığını ifade eden ve içinde 'Rusya' sözcüğü hiç geçmeyen bir yanıt vermeyi tercih etmiştir[35].

Yine de, NATO'nun Siber Savunma Mükemmeliyet Merkezi (Tallinn – Estonya) tarafından düzenlenen son siber konferansta (CyCon 2017) ağırlık kazanan görüşler, Estonya'da 2007 yılında meydana gelen siber saldırılar benzeri bir saldırının yaşanması durumunda, 5. madde yolunu da açık bırakacak şekilde, çok daha sert bir yanıt verileceği yönünde olmuştur.[36] Henüz diplomatik retorik düzeyinde olsa da, siber tehditler karşısında ve daha önce vuku bulmuş bir olayı ölçek olarak alarak, kolektif savunma maddesi imasının yapılması dahi NATO ve siber harbin geleceğine ilişkin önemli bir fikir vermektedir. Elbette, mükemmeliyet merkezlerinin ürettiği görüşler ve analizler Kuzey Atlantik İttifakı için bağlayıcılık oluşturmamaktadır. Buna karşın, bahse konu analitik girdilerin, Kuzey Atlantik Konseyi'nin ve NATO üyesi ülkeleri yöneten elitlerin bakış açıları üzerinde de kimi durumlarda ciddi etki sahibi olabildiği unutulmamalıdır.

32 NATO, http://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en, Erişim tarihi: 31 Ağustos, 2017.

33 Ibid.

34 Genel Sekterer Stoltenberg'in yanıtı için: "We have decided that a cyber attack can trigger Article 5, meaning that a cyber attack can trigger collective defence, because we regard cyber attacks as something that can cause a lot of damage and can be very dangerous. As I said, it's hard to imagine a conflict without a cyber dimension. So, yes, cyber can trigger Article 5, but the same time I think it's also important to understand that cyber is not something that always triggers Article 5". http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en, Erişim tarihi: 31 Ağustos 2017.

35 Genel Sekreter Stoltenberg'in yanıtı için bkz: "So our cyber capabilities, our cyber defence is not directed against any particular adversary. It is something we developed, something we strengthen to be able to respond to attacks from any direction. So I will not name any particular, but I'll just underline that we are stepping up our efforts to be able to defend our own networks, both at headquarters but also when we do operations and missions.It's extremely important to have networks that are working but also help and assist allies that may be under attack. We have developed small teams which we can send out and assist. And of course in the different scenarios which we can imagine related to hybrid attacks, cyber will be an important dimension related to hybrid, and therefore we have to be able to support allies which may come under cyber attack. That's also an area where we see a great potential for enhanced cooperation with the European Union, and we have just agreed on arrangements with the European Union on technical measures related to cyber defence". http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en, Erişim tarihi: 31 Ağustos 2017.

36 DefenseNews, https://www.defensenews.com/2017/05/31/nato-might-trigger-article-5-for-certain-cyberattacks/, Erişim tarihi: 31 Ağustos 2017.

SİBER SAVAŞIN COĞRAFYASI: SİBER-UZAYIN JEOPOLİTİK NİTELİKLERİ

Siber-uzay, toplumlar üzerinde harbin diğer boyutlarıyla kıyaslanamayacak ölçüde bir etki alanına sahiptir. Ayrıca, savaşın bilinen diğer boyutlarının aksine, siber-uzayın fiziksel olarak tek bir devlet tarafından coğrafi kontrolü mümkün olmadığı gibi, siber ortamda çatışma diğer boyutlara nazaran çok daha hızlı vuku bulmaktadır[37]. Daha da önemlisi, bir aktörün teknolojik kapasitesi arttıkça, kara-deniz-hava-uzay sistem ve platformları siber-uzaya daha çok bağımlı hale gelir. Dolayısıyla siber-uzayda yaşanacak bir zafiyet, özellikle gelişmiş devletler açısından, harbin diğer boyutlarında ciddi olumsuz sonuçlar doğurabilecektir[38].

Siber-uzay esasen harbin diğer dört boyutunda 'bir biçimde' vardır. Daha açık bir ifadeyle, örneğin, denizde seyir halindeki savaş gemilerinin sensörlerinden ya da havada bulunan platformlardan yapılan bilgi iletimleri ve karada konuşlu data kompleksleri siber-uzayı tamamlayan unsurlardır. Harbin dördüncü boyutu olan uzay ile siber-uzay arasında ise daha özel bir ilişki bulunmaktadır. Zira her iki boyut da telekomünikasyon ve ağ teknolojileri ile doğrudan ilgilidir. Ayrıca, uzayda icra edilen operasyonlar siber-uzaydaki yeteneklere, siber-uzayda icra edilen operasyonlar ve siber elektromanyetik faaliyetler de uzay boyutundan gelen desteğe bağımlıdır[39].

Askeri olarak bakıldığında, siber-uzayın, harbin diğer boyutları olan kara-hava-deniz-uzay dörtlüsüne göre önemli farklılıkları bulunmaktadır. Öncelikle siber-uzay, savaşın tarihsel ve doğal boyutlarının aksine, bilinen fizik kuralları ile tanımlanabilecek nitelikte değildir. Tabi ki, harbin fiziksel olarak nitelendirilebilen boyutlarında yaşanan olayların sosyal ve politik sonuçları da olmaktadır. Bununla birlikte, harp sahasındaki olayların kinetik etkileri (örn. bir balistik füze harp başlığının karadaki bir hedefi vurması, uçaksavar ateşi ile bir hava platformunun vurulması, bir denizaltının bir su-üstü platformunu vurması, yörüngedeki bir askeri uydunun vurulması, yeraltındaki bir tünelin topçu unsurları ile vurulması vb.) yine fiziki harp sahası ya da sahalarının fiziki olarak tanımlanabilen nitelikleri ile sınırlıdır. Siber-elektromanyetik askeri faaliyetlerin birçoğu ise hesaplanması çok zor ve çok boyutlu etki alanlarına ulaşabilir[40]. Örneğin bir bilgisayar virüsü, hedef ülkenin sistemlerini etkiledikten sonra, dünyanın çeşitli yerlerinde esasen hedef alınmamış olan ülkelere de sirayet edebilir. Bu nedenle, uluslararası hukuki incelemede belirtildiği üzere, siber-uzayda 'etkili menzil' ya da istenmeyen hasar olasılığı hesaplanması çok komplikedir. Zira, siber-uzay, bilginin kullanımı, insanlar arası etkileşim sağlanması ve inter-komünikasyon için oluşturulmuş bir alandır. Söz konusu alan, telekomünikasyon sistemleri aracılığıyla, elektromanyetik spektrum ile birlikte mevcudiyetini sürdürmektedir. Daha açık bir ifadeyle, bahse konu telekomünikasyon sistemleri, elektromanyetik spektrumu kullanarak, küresel bir ağ örmek suretiyle siber-uzayı oluşturur[41].

Elbette, yukarıda anılan özgün niteliklerinden ötürü, siber-uzayda caydırıcılık sağlanması da geleneksel bakış açısıyla kavranılması zor bir hususdur. Özellikle Soğuk Savaş dönemine ait caydırıcılık teorilerinin savunma yetenekleri, tehdidin inanılırlığı, askeri-siyasi mesajın gereken etkinlikte iletilmesi gibi temel bileşenleri, günümüz siber parametreleri için değişime uğramak durumundadır[42].

37 The United States Army War College, Strategic Cyberspace Operations Guide, June 2016. pp.6-7.

38 Ibid.

39 The US Department of Army, FM 3-38 Cyber Electromagnetic Activities, 2014.

40 The US Department of Army, FM 3-38 Cyber Electromagnetic Activities, 2014.

41 Ibid.

42 Amir, Lupovici. "Cyber Warfare and Deterrence: Trends and Challenges in Research", Military and Strategic Affairs, Vol.3 No.3, Aralık 2011.

SİBER HARBİN GELECEĞİ: BİLİMKURGU MU TEKNOLOJİK DEVRİM Mİ?

Özellikle son dönemde elektronik ağ tabanlı iletişimde yaşanan devrim niteliğindeki ilerlemeler, muharebe ağlarının (battle network) da benzer biçimde gelişmeler yaşamasına neden olmuştur. Birinci Dünya Savaşı sırasında telefon ve telsiz hatlarının kullanılmaya başlamasıyla deniz ve kara unsurları ile uzak mesafelerde iletişim kurulması, kimi uzmanlar tarafından ilk muharebe ağı teşkili kabul edilmektedir. Modern muharebe ağları, komuta-kontrol sistemleri, hedef tespit sensörleri & diğer keşif-gözetleme-istihbarat imkanları, silah sistemleri ve platformları ile tüm bu unsurları birbirine bağlayan elektronik komünikasyona dayalı muhabere yeteneklerinin toplamından oluşmaktadır[43]. Muhabere imkan ve kabiliyetlerinde yaşanan elektronik devrim, askeri coğrafya anlayışında önemli değişiklikleri de beraberinde getirmiştir. Bir tür olarak 'insanın' savaşmaya başladığı ilk dönemde, sevk ve idare merkezi ile muharip unsurlar arasındaki mesafe, 'insan sesinin ulaşabileceği ya da gözünün görebileceği' mesafe olmak durumunda idi. Bugün bu mesafe devrimsel bir noktaya vardığı gibi, ağ-merkezli harp anlayışı, silah sistemlerine normal şartlarda tespit edemeyecekleri hedeflere angaje olma imkanı da tanımaktadır. Dolayısıyla, özellikle İkinci Dünya Savaşı'ndan itibaren artan bir hızla, bir muharebe ağları rekabeti (battle networks competition) yaşandığı, önümüzdeki dönemde de bu trendin büyük bir ivme ile yükselerek devam edeceği belirtilmektedir[44].

Siber yetenekler çağında, ağ-merkezli harbin temel prensipleri olan bilgi üstünlüğünün kazanılması, harbe iştirak eden dost birlikler arasında bilgi paylaşımının ve ortak durumsal farkındalığın üst düzeye çıkarılması, harekatın lineer düzlemin dışına çıkarılması ve senkronizasyonun etkin kullanımı gibi hususların giderek önem kazanacağı bir gerçektir[45]. Dahası, bilgi üstünlüğünün kazanılması, yani harp sahasına ilişkin mümkün olan en doğru ve en fazla bilgiyi en hızlı biçimde elde ederek dost kuvvetler ile paylaşmak bunu yaparken de düşmanın aynı olanaklardan mümkün olduğunca mahrum kalmasını sağlamak, siber çağda daha önemli bir kuvvet çarpanı haline gelmektedir[46].

Aşağıda aktarılacağı üzere, ağ-merkezli harbin bileşenleri de hem nicel hem de teknolojik nitelik bakımdan büyük bir ivme göstermektedir.

Savunma Sanayii devi Raytheon'un yaptığı bir çalışma, geleceğin savaşlarında ve ABD'nin üçüncü 'offset stratejisinde' belirleyici olacak teknolojik trendler arasında, başlıca, yapay zeka, insan-makine etkileşimini yükseltecek yenilikler, akıllı üretim teknolojileri, mikro-drone'lar, elektromanyetik silahlar, siber harp, küçük & akıllı mühimmatlar ve atomaltı parçacıklara ilişkin bilimsel çalışmaların bulunacağını belirtmektedir[47].

Bilgisayar ve robotik teknoloji alanında yaşanan gelişmeler, geleceğin harp ortamında otomatik sistemlerin yerini tedrici olarak otonom sistemlere bırakacağını göstermektedir. Otonom sistemler, otomatik sistemlerin aksine, tek bir davranış paterni ile değil, bir dizi hareket tarzı seçenekleri ve durum analizleri ile hareket edecektir. Bu durumda, esasen yazılımlara dayalı olan 'robotların nasıl düşündüğü' sorunsalı da geleceğin harp ortamında hem stratejik hem de askeri-etik konularının önemli bir parçası olacaktır[48].

Özetle, siber yeteneklerde yaşanan gelişmelerin askeri strateji ve konseptlerin platform-merkezli yaklaşım-

43 John, Stillion ve Bryan, Clark. What it Takes to Win: Succeeding in 21st Century Battle Network Competitions, CSBA, 2015.

44 Ibid.

45 Richard, L. Folks, Network Centric Warfare In The Age Of Cyberspace Operations, U.S. Army War College, 2011.

46 Ibid.

47 Raytheon, http://www.raytheon.com/news/rtnwcm/groups/corporate/documents/content/rtn_303213.pdf, Erişim tarihi: 28 Mart 2017.

48 M.I, Cummings, Artificial Intelligence and the Future Warfare, Chatham House, Londra, 2017.

lardan ağ-merkezli yaklaşımlara geçişini hızlandıracağı görülmektedir. Geleceğin harp ve harekat ortamında siber kapasitede üstünlük sağlayan tarafın, doğal olarak bilgi üstünlüğünü ve ağ-merkezli yeteneklerde avantajlı konumu sağlayacağı açıktır. İsrail'in Suriye Baas rejiminin nükleer programını akamete uğratmak maksadıyla 2007 yılında gerçekleştirdiği 'Meyve Bahçesi Harekatı*' –Mivtza Bustan*– siber-elektromanyetik faaliyetlerin ağ-merkezi harekatlarda taarruzi olarak kullanımına ilişkin dikkat çekici bir örnek teşkil etmektedir. Harekat kapsamında, Suriye'nin Kuzey Kore'nin yardımıyla yürüttüğü ve askeri amaçlı olduğu yönünde kuvvetli şüpheler bulunan bir nükleer tesis, el-Kibar, İsrail Hava Kuvvetleri tarafından imha edilmiştir[49]. Hatta harekata katılan bazı İsrail uçaklarının yakıt tanklarının da Türkiye topraklarına bırakıldığı bildirilmektedir[50].

Konuya ilişkin açık-kaynaklı yayınlar , İsrail F-15 ve F-16'larının Suriye hava savunma kompleksini aşmak için entegre bilgi harbi, elektronik harp[51] ve siber harp yeteneklerinden yararlandığını belirtmektedir[52]. Buna göre, BAE Systems'in kontratını kazandığı ve Suter adı verilen projeler dizisi, düşman bilgisayar ağlarına sızmak ve radarlarını manipüle etmek gibi görevler için tasarlanmıştır ve 2000'li yılların başında Nellis Hava Üssü'nde denemeleri başlamıştır[53]. Suter, ABD Hava Kuvvetleri için geliştirlen, ağ-merkezli istihbarat-keşif-gözetleme-hedef tespit hassas mühimmata dayalı taarruz kompleksi olan NCCT (Network-Centric Collaborative Targeting) ile eş zamanlı olarak yürütülmektedir[54].

Konuya ilişkin teknik değerlendirmeler, Suter'in bir jammer'dan çok bir 'hacker' olduğunu ortaya koymaktadır ve özü itibariyle bilgisayarlara ilişkin 'hacking' teknoloji ve konseptleri ile elektronik espiyonaj faaliyetlerinin birleştirilmesi sonucu hayata geçirildiği belirtilmektedir[55]. Ayrıca, İsrail'in, kendi 'Suter-benzeri' sistemlerini 2006 İkinci Lübnan Savaşı'ndan itibaren kullandığı ve 2007 Meyve Bahçesi Harekatı sırasında da bu sistemlerden faydalandığı, ek olarak Suriye hava savunma sistemlerinin durumuna ilişkin ABD'den anlık data desteği de aldığı belirtilmektedir[56].

SONUÇ

Siber yeteneklerin geleceğin harp ortamında ciddi bir oyun değiştirici olacağı kesin görünse de, henüz silahlı çatışmalar hukuku tarafından tam anlamıyla karşılanabilecek bir siber savaş eşiğinin geçildiğini söylemek mümkün görünmemektedir. Aynı şekilde, ofansif siber yeteneklere ilişkin düzenleyici bir uluslararası mekanizmanın kurulması ve bir verifikasyon rejimi oluşturulması hususlarında da iyimser olmak güçtür. Zira, hemen hiçbir ülke kendi enformasyon ve bilgisayar altyapısını uluslararası kontrole açmak konusunda istekli olmayacaktır. Ayrıca, siber silahsızlanma konusunda bugüne kadar bazı adımların, Rusya Federasyonu ve Çin Halk Cumhuriyeti gibi otoriter rejimlerden gelmesi, güven yaratıcı önlemler adı altında internette bireysel özgürlüklerin de tehlikeye atıldığı paketlerin gündeme gelebileceğiyle ilgili ciddi şüphelere neden olmaktadır. Belirtilenlere ek olarak, başta ABD olmak üzere, teknolojik yetenekler konusunda önemli üstünlükler yakalamış ülkelerin bahse konu imkan ve kabiliyetlerini bir uluslararası pazarlık konusu yapmaları pek mümkün görünmemektedir.

49 IISS, Nuclear Programmes in the Middle East: In the Shadow of Iran, http://www.iiss.org/-/media/Silos/StrategicDossiers/Nuclear-Programmes-in-the-Middle-East--In-the-shadow-of-Iran/ME-06-Chapter-04-Syria-etc/ME-06-Chapter-04-Syria-etc.pdf, Erşim tarihi: 27 Mart 2017.

50 IHS Jane's, Access Denial- Syria's Air Defence Network, 2014.

51 Ibid.

52 Kenneth, Geers. Pandemonium: Nation States, Natıonal Security, And The Internet, The Tallinn Papers, CCD-COE, 2014, p.7.

53 Clay, Wilson. Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues, Congressional Research Service, 2007, p.7.

54 Exhibit R-2, RDT&E Budget Item Justification: PB 2016 Air Force, http://www.globalsecurity.org/military/library/budget/fy2016/usaf-peds/0305221f_7_pb_2016.pdf, Erişim tarihi: 27 Mart 2017.

55 Daha ayrıntılı değerlendirme için bkz: http://www.airforce-technology.com/features/feature1625/, Erişim tarihi: 27 Mart 2017.

56 Ibid.

Öte yandan, siber-uzayda yaşanacak çatışmalar için uluslararası hukuki norm oluşturulması ve hatta uluslararası bir mekanizma kurulması önemlidir. Bunların başarılamaması halinde ciddi sorunlarla karşılaşılabilir, zira siber teknolojilerin önümüzdeki yıllar içinde 'kritik kütleye' ulaşacağı değerlendirilmektedir. Söz konusu 'kritik kütle' aşaması ve sonrasında hem siber-elektromanyetik teknolojilerde gelişmişlik seviyesi ülkelerin milli güç kapasitesi açısından oyun değiştirici bir kuvvet çarpanı haline gelecektir, hem de kinetik etkiler ve ikincil hasar kapasitesi kontrolden çıkan boyutlara ulaşabilecektir.

Bu çerçevede sadece 'silahların' değil, 'hedeflerin' de yukarıda özetlenen trendleri beslediği not edilmelidir. Teknolojik gelişmişlik seviyesi yükseldikçe, ülkelerin ekonomik yaşamları, kritik ulusal altyapıları ve sosyal etkileşimleri giderek daha çok dijitalize olmakta, bilgisayar ağlarına ve telekomünikasyon imkanlarına daha çok bağımlı duruma gelmektedir. Dolayısıyla ofansif siber yeteneklerin 'hedef seçenekleri' her geçen gün daha çok genişlemektedir. Daha da kritik olmak üzere, gerek bilimsel araştırmalar ve sivil amaçlar için gerekse KBRN alanında (kimyasal-biyolojik-radyolojik-nükleer) askeri programlar için kullanılan tesis altyapıları da giderek SCADA sistemlerine daha çok dayanmaktadır. Bu nedenle, ofansif siber yeteneklerin sınırlandırılması ve siber-uzayda çatışma durumlarına dair norm oluşturulması girişimlerinin daha önce aktarılan 'kritik kütle' aşamasının sonuca ulaşmasından önce başarılması ciddi bir gereksinimdir.

Baş döndürücü gelişmelerin yaşandığı bu dönemde, Türk karar vericilere yönelik siber siyasa üretiminde tavsiye olarak birkaç noktanın altını çizmekte yarar görülmektedir. İlk ve en önemli parametre zamanlamadır. Siber teknoloji yarışına günümüzde gerekli yatırımı yapan ulusların, 2020'li yıllarda yatırımlarının karşılığını uluslararası rekabetin –barış ve savaş dönemlerini kapsayan– her alanında fazlasıyla alacağı, 2010'lu yıllarda bahse konu yatırımları gerçekleştirmeyen devletlerin ise milli güç kapasitelerinde ciddi bir erozyonla karşılaşacağı mütalaa edilmektedir. Söz konusu yatırımlar için ön şartlar ise: doktrin, beşeri sermaye, kurumlar arası koordinasyon ve eşgüdüm ile bilimsel, inovatif düşüncedir. İkinci olarak, siber-uzaya ilişkin uluslararası hukuki norm oluşturma sürecinde mutlaka aktif olunması ve diplomatik pozisyonun belirlenmesi çok önemlidir. Zira, siber-uzayda oyunun kuralları henüz belirlenme aşamasındadır. Üçüncü olarak, Türkiye'ye yönelik gerek diğer devletlerden gerekse terör örgütlerinden kaynaklanabilecek risk ve tehdit değerlendirmelerinde siber boyutun üzerinde hassasiyetle durulması yaşamsal önemdedir. Belirtilen milli güvenlik analizlerinde temel amaç 'hayal gücü eksikliğinden' kaynaklanabilecek stratejik sürpriz faktörlerini minimize etmek olmalıdır. Son olarak, ülkemizde bulunan akademik kaynakların ve düşünce kuruluşlarının siber çatışma ve siber teknoloji sahalarında araştırma yapmalarını ve tartışmalarını teşvik edecek bir ortamın oluşturulması zaruridir.

Daha geniş çerçeveli siber çatışma durumundan, daha dar bir çerçevede siber harp boyutuna inildiğinde, bu çalışmanın temel bulgusu, savaşın diğer unsurları ve teknolojik gelişmeler ile müştereklik niteliklerinin ön plana çıkacağıdır. Bu çerçevede, siber harp ve elektronik harp, siber harp ve uzay teknolojileri, hatta siber harp ve biyolojik harp gibi kombinasyonlar üzerinde durmak, geleceğe ilişkin tahminlerde daha gerçekçi bir vizyon sunabilir

Günümüzde ve geleceğin harp ortamında, özellikle A2/AD (Anti-Access / Area Denial) olarak adlandırılan kompleks savunmalara karşı ağ-merkezli müşterek harekat icrası açısından siber-elektromanyetik yetenekler kritik olacaktır. Dolayısıyla bu çalışma, geleceğin savaşlarının sıklet merkezinin, C4ISR (komuta-kontrol-muhabere-bilgisayar-istihbarat-gözetleme-keşif) ağları, askeri uydu haberleşme yetenekleri, siber-elektromanyetik imkan ve kabiliyetler ile bilgi harbi kapasitesi, hassas-güdümlü taarruzi sistemler etrafında şekilleneceğini öngörmektedir. Büyük olasılıkla temel görevler, bahse konu sistemlerin düşman penetrasyonundan korunması ve düşmanın benzer sistemlerinin akamete uğratılması olacaktır.

Son olarak, özellikle Batı'nın ve NATO'nun, klasik anlamda 'savaş eşiğinin altında' tanımladığı çatışma ortamlarına ilişkin yeni bir paradigma geliştirmesi zaruri görünmektedir. Zira, bahse konu alan, eğer tam anlamıyla gerçekleşecek ise, siber savaşın harp sahası olacaktır.

Ekonomi ve Dış Politika Araştırmalar Merkezi

edam

EDAM Siber Politikalar Kağıtları Serisi 2017/2

Eylül 2017

Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında

Dr. Can Kasapoğlu
Savunma Analisti, EDAM