STUXNET SALDIRISI VE ABD'NİN SİBER SAVAŞ STRATEJİSİ: ULUSLARARASI HUKUKTA KUVVET KULLANMAKTAN KAÇINMA İLKESİ ÇERÇEVESİNDE BİR DEĞERLENDİRME

Şener ÇELİK*

GİRİŞ

Teknolojik ilerleme, devletlerin savunma ve saldırı maksatlarıyla geliştirdikleri silah sistemlerini gün geçtikçe daha karmaşık hale getirmiştir. Özellikle bilişim teknolojisindeki gelişmeler, bilgisayar sistemlerine ait yazılım ve programların da gerektiğinde bir silah olarak kullanılabileceğini göstermiştir. Söz konusu sistemler, askeri sahadaki köklü değişimler (revolution in military affairs) isimli strateji kuramında belirtildiği gibi, teknolojinin geleceğin savaşma şeklini değiştirebileceğini bugünden kanıtlar mahiyette gözükmektedir. Bilişim sistemlerindeki bu yenilikler, savunma teknolojilerinde büyük bir ilerlemeye neden olurken, aynı zamanda uluslararası hukukta kuvvet kullanımı ve buna bağlı olarak meşru müdafa hakkıyla ilgili yeni soruların ortaya çıkmasına da neden olmuştur.

ABD'nin farklı sahalardaki teknolojik araştırma-geliştirme üstünlüğü, her ne kadar bazı çevreler tarafından eski rekabetçilik düzeyinde olmadığı iddia edilse de, halen bilişim alanında da varlığını muhafaza etmektedir. Bilişim teknolojilerindeki ilerleme, devlet veya devlet-dışı aktörlerin birbir-

* Lisans: Uluslararası İlişkiler, University of London-London School of Economics (2005-2010); Yüksek Lisans: Harp-Harekat Hukuku, Stratejik Araştırmalar Enstitüsü, Harp Akademileri (2010-2013).

lerine karşı zararlı yazılım ve programlarla yapılabilecek saldırıları gündeme getirmiştir. Bu çerçevede, özellikle 11 Eylül sonrası dönemde, düşman devletlere veya devlet-dışı aktörlere karşı kullanılmak üzere, bilgisayar yazılımları ve programlarından oluşan siber silahlar üzerindeki çalışmalar yoğunlaşmıştır. Akabinde, bu silahlarla gerçekleştirilebilecek siber saldırılar ulusal ve uluslararası güvenlik çalışmaları çerçevesinde değerlendirilmeye başlanmıştır. Kuşkusuz bu teknolojik gelişme ABD için yeni ve beklenmedik bir devrim değildir. Savunma ve saldırı amacıyla bilimsel ilerlemelerden faydalanmak, Endüstri Devrimi'nden beri Batı'da gelenekselleşmiş olan bir yönelimdir. ABD'nin ve dünyanın geri kalanının henüz hazırlıklı olmadığı alan ise, genelde teknolojik ilerleme özelde ise bilişim teknolojilerindeki gelişme sayesinde ortaya çıkan siber uzay (cyberspace) fenomeninin yarattığı ulusal ve uluslararası hukuk sorunlarıdır. Bu sorunlar, özellikle ABD'nin bu makalede incelenen İran'ın Natanz kentindeki nükleer yakıt zenginleştirme tesislerine karşı gerçekleştirdiği öne sürülen siber saldırıdan sonra politika yapıcılar ve akademisyenler arasında tartışma konusu olmaya başlamıştır. Söz konusu saldırı, Stuxnet adı verilen bilgisayar programı ile 2009 senesinde gerçekleştirilmiştir. Ancak saldırıyla ilgili verilerin uzun zaman sonra ortaya çıkmış olması, Amerikan kamuoyunun, uluslararası topluluğun ve nihayet konuyla doğrudan ilgili disiplin olan uluslararası hukuk alanında çalışan akademisyenlerin sorunla ilgilenmelerini geciktirmiştir.

Bu makalenin amacı, ABD'nin Stuxnet programıyla gerçekleştirdiği saldırıdan yola çıkarak, siber saldırının uluslararası hukukta ne anlama geldiğini ve nasıl düzenlendiğini araştırmaktır. Temel araştırma sorusu, bir devletin başka bir devlete karşı düzenleyeceği siber saldırı ile uluslararası hukuktaki kuvvet kullanmaktan kaçınma ilkesinin ihlal edilip edilmeyeceği ve bu fiilin meşru müdafa hakkının kullanılmasına cevaz verip vermeyeceğidir. Çalışmanın amacı gereği, siber saldırı incelenirken sadece devletlerin uygulamaları dikkate alınmış, terörizm veya siyasi propaganda amaçlarıyla hareket eden devlet-dışı örgütler, muhalif-aktivist gruplar ve herhangi bir siyasi amacı bulunmayan bilgisayar korsanları tarafından bireysel olarak gerçekleştirilen saldırılar araştırmanın kapsamı dışında tutulmuştur. Araştırmada tipik durum örneklemesi olarak Stuxnet saldırısı ele alınmış, ABD'nin bilişim teknolojilerindeki ve uluslararası sistemdeki başat rolü nedeniyle de

bu ülkenin politikasından yola çıkılarak bir uluslararası hukuk değerlendirmesi yapılmaya çalışılmıştır. Çalışmanın birinci bölümü, teknolojik bir kavramsal çerçeve çizme amacına hizmet edecektir. Bu bölümde, siber silah ve siber saldırı kavramları incelenecek, söz konusu olguların tanımları yapılacaktır. İkinci bölümde, çalışmanın örneklemini oluşturan olay incelenecektir. Stuxnet virüsünün teknik özellikleri, bu virüsle gerçekleştirilen saldırı ve saldırının sonuçları bu bölümün konusu dahilindedir. Üçüncü bölümde, ABD'nin kuvvet kullanmaktan kaçınma ilkesine yaklaşımı çerçevesinde siber saldırı politikası incelenecektir. Politika yapıcı çevreler arasındaki siber silahlarla ilgili birbiriyle çelişen kuvvet kullanma anlayışı bu bölüm kapsamında yorumlanmaya çalışılacaktır. Son bölümde, uluslararası hukukta kuvvet kullanmaktan kaçınma ilkesi ve meşru müdafa hakkı ele alınacak, siber saldırının bir kuvvet kullanımı olarak yorumlanması için gerekli şartlar incelenecektir. Konuyla ilgili önemli uluslararası hukuk belgelerinden biri olan Tallinn Kılavuzu ve muhtemel saldırıların tanımlanmasında kullanılabilecek Schmitt ölçütleri de bu bölümde ele alınacaktır.

I. KAVRAMSAL ÇERÇEVE: SİBER SALDIRI VE SİBER SİLAHLAR

Siber saldırı, askeri literatürde, devletlerin ulusal hukuk metinlerinde ve uluslararası hukuk kaynaklarında açıkça tanımlanmış ve üzerinde mutlak bir uzlaşı sağlanmış bir kavram değildir. Bu nedenle söz konusu fiilin farklı tanımları bulunmaktadır. Literatürdeki en kapsamlı tanımlardan biri olan ABD Ulusal Araştırma Konseyi Bilgisayar Bilimler ve Telekomünikasyon Kurulu (Computer Science and Telecommunications Board of the National Research Council) Baş Bilim Uzmanı Herbert Lin'in açıklamasına göre, siber saldırı, düşmanın bilgisayar sistemlerini ve ağlarını veya bu sistem ve ağlarda bulunan ya da bunlardan geçen bilgiyi ve/veya programları değiştirmek, bozmak, yanıltmak, geriletmek veya ortadan kaldırmak için yapılan kasıtlı hareket ve harekatlardır[1]. Bu saldırıların gerçekleştiği siber ortam, devletler, devlet-dışı örgütler, özel kurumlar ve hatta kişiler arasında

[1] Herbert S. **Lin**, "Offensive Cyber Operations and the Use of Force", **Journal of National Security Law & Policy**, Vol.4, No.63 (2010), p.63.

meydana gelebilecek siber savaşların gerçekleşeceği yirmibirinci yüzyılın yeni savaş alanı (domain) olarak kabul edilmektedir. Bilişim teknolojilerindeki devrim ve internetin verdiği çevrimiçi erişim imkanı, bütün bu aktörlere yeni saldırı/savunma araçları ve stratejileri sunduğu gibi, aynı zamanda hepsini farklı derecelerde yaralanabilir kılmıştır. Geleneksel kabule göre, bilgisayarlar ve bilgisayar ağları üzerinden yürütülen siber saldırı asimetrik bir savaştır. Özellikle ABD'ye karşı konvansiyonel alanda silah üstünlüğü olmayan aktörlerin, bu ülkenin askeri kabiliyetlerini tehdit etmek için siber saldırı yöntemlerini kullanmaya kararlı oldukları bilinmektedir[2]. Ancak, yukarıda belirtildiği gibi, devlet-dışı aktörlerin siber faaliyetleri bu çalışmanın kapsamı dışında olduğundan, burada asimetrik savaş çerçevesinde bir değerlendirme yapılamayacaktır.

ABD Ulusal Bilimler Akademisi (National Academy of Sciences, NAS) tarafından yapılan tanıma göre ise, siber saldırı, düşman bilgisayar sistemlerini veya ağlarını ya da bilişim ve/veya programlarını değiştirmek, yok etmek, yanıltmak veya geriletmek için yapılan, uzun bir zaman dilimi içine yayılmış olabilen kasıtlı hareketlerdir[3]. NAS, sözünü ettiği 'düşman

---

2 William J. **Lynn III**., "Defending a New Domain: The Pentagon's Cyberstrategy", **Foreign Affairs** Vol.89, No.5 (2010), p.98.

3 William A. **Owens**, Kenneth W. **Dam**, Herbert S. **Lin**, (ed.), **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities**, Committee on Offensive Information Warfare, National Research Council, The National Academies Press, Washington, DC (2009), p.10. Siber savaş, ABD'nin uluslararası sistemdeki teknolojik üstünlüğü ve politik etkisi nedeniyle genel olarak bu ülkedeki akademik çevreler tarafından yayınlanan bilimsel eserler kapsamında incelenmektedir. Bu eserlerde ifade edilen geleneksel yaklaşımlara alternatif olarak Çin akademik çevrelerinin görüşleri hakkında ayrıntılı bir araştırma örneği için bkz.: Li **Zhang**, "A Chinese Perspective on Cyber War", **International Review of the Red Cross**, Vol.94, Issue 886, (June 2012), pp. 801-807. Aynı konuda bir konferans bildirisi için bkz.: Su **Sheng**, Wang **Yingkun**, Long **Yuy**i, Li **Yong**, Jiang **Yu**, **Cyber Attack Impact on Power System Blackout**, IET Conference on Reliability of Transmission and Distribution Networks, (22-24 Nov.2011). Siber savaş operasyonlarının farklı ülkelerdeki gelişimi hakkında bir değerlendirme için bkz.: Şeyda **Türkay**, "Siber Savaş Hukuku ve Uygulanma Sorunsalı", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. LXXI, S. 1, s.1177-1228, (2013).

bilgisayarları veya ağları'nın mutlaka düşmanın kendi mülkiyetinde olmasına ya da düşman tarafından işletilmesine gerek olmadığını, düşmanın herhangi bir şekilde desteklediği veya kullandığı bilgisayarların veya ağların da 'düşman' bilgisayarı olarak kabul edilebileceğini savunmuştur[4]. Böylece NAS, düşmanın kendi mülkiyetinde olmayan fakat 'desteklediği' veya 'kullandığı' bilgisayarların veya ağların da - bir siber saldırının bu kaynaklardan düzenlenmesi durumunda - düşmana ait olarak kabul edilmesi gerekeceği şeklinde bir varsayım geliştirmiştir.

Siber saldırının hangi tür yazılım ve donanımlar ile gerçekleştirileceği konusunda, bir başka deyişle ne gibi zararlı bilişim unsurlarının siber saldırı silahı olarak nitelenebileceği hakkında literatürde kesin mutabakat sağlanmış değildir. Bunun bir nedeni, muhtemelen, bilişim alanındaki gelişmelerin olağanüstü hızı ve 'silah' olarak sınıflandırılabilecek yazılım ve programların konvansiyonel silah sistemlerine göre resmi şekilde açıkça tasnif edilmiş olmamasıdır. Gerçekten de, aşağıda incelenecek Stuxnet virüsü hariç, muhtemelen bugün devletlerin kuvvet kullanımı kapsamında başvurabileceği ve müstakil olarak siber saldırı silahı olarak geliştirilmiş bir yazılım veya program yoktur. En azından resmi olarak böyle bir unsurun varlığı açıklanmamıştır. Bu tip yazılım ve programlar, bugüne kadar daha çok örgütlü olmayan, kurumsal bir kimlikten yoksun, hiyerarşik bir emir-komuta düzeni içinde yer almayan ve genellikle politik muhalif-aktivist kimliğiyle hareket eden bireysel girişimlerin ürünü olarak dikkat çekmişlerdir. Öte yandan, bilişim sistemlerine verebilecekleri zararlar dikkate alındığında, belirli yazılım ve programların siber saldırı silahı olarak nitelenebileceği de muhakkaktır. Genel olarak bilgisayar sistemlerine ve ağlarına ciddi zarar verebilecek bütün yazılım veya programların bu sınıflandırma içinde yer aldığı varsayılmaktadır. Botnet, DoS saldırısı, mantık bombası, Truva atı, virüs ve solucan, bir siber saldırıda kullanılan zararlı yazılımlar ve programlar olarak kabul edilmektedir[5].

---

[4] a.g.e., p.11.

[5] Botnet (robot network), robot ağ adı verilen programların ifade eder. Botnet, bir veya birden fazla bilgisayarı uzaktan kontrol altına alan programa verilen isimdir. Bu tip saldırı altında olan bilgisayar kullanıcıları genellikle donanıma zararlı bir

Siber silahın tanımı konusunda bir uzlaşıya varmak adına, bu silahları neden olabilecekleri zarara göre sınıflandırmak yerinde ve işlevsel bir yöntemdir. Bu yaklaşıma göre, siber silahlar bir etki spektrumu üzerinde düşük ve yüksek potansiyele sahip yazılım ve programlar olarak değerlendirilirler[6]. Düşük potansiyele sahip siber silahlar, bir sistemi dışarıdan etkileyebilen ancak bu sistemin içine girmeyi ve onu içeriden yönetmeyi başaramayan zararlı yazılımlardır (malicious software - malware)[7]. Yüksek potansiyele sahip siber silahlar ise, bu sistemlerin içine girerek 'akıllı unsur' (intelligent agent) şeklinde çalışan ve otonom şekilde hareket ederek sistemin normal faaliyet sürecine zarar veren zararlı yazılımlardır[8].

---

yazılım yüklendiğinden haberdar olmazlar. DoS (Denial of Service) saldırısı, 'hizmet engelleme' kelimelerinin birleşimiyle tanımlanan bir eylemdir. DoS saldırılarında kullanılan yazılımlar, belirli ağ kaynaklarına yetkili erişimi engelleyen programlardır. Mantık bombası (logic bomb), belli bir programın içine kasıtlı olarak zararlı bir kod yerleştirilmesi işlemine verilen isimdir. Mnatık bombası genellikle hedef alınan bilgisayar veya ağlardaki bilgileri yok etmek veya kulanılamaz duruma getirmek için kullanılır. Truva atı (Trojan horse), kullanıcıların çalıştırmak istedikleri program gibi davranan yazılımlara verilen isimdir. Mantık bombasına benzer bir sistemle çalışır. Virüs, hedef bilgisayar veya ağlara zarar vermek için yazılan bir uygulamadır (application). Virüsler bilgisayar dosyalarına girerek kendi kendisini çoğaltabilirler. Solucan (worm) ise kendi kendisini yayabilen virüs programıdır. Bu programlar genel olarak, ağlara karşı DoS saldırısı gerçekleştirmek veya virüs sokmak için 'arka kapı' (back door) olarak bilinen sistem açıkları yaratmak için kullanılırlar. Bu bilişim kavramlarının açıklandığı oldukça anlaşılabilir dille yazılmış bir çalışma için bkz.: Anthony F. **Sinopoli Cyberwar and International Law: An English School Perspective,** Yüksek Lisans Tezi, Government and International Affairs, University of South Florida (2012), pp.27-31. Zararlı programların türleri ve tanımları hakkında resmi bir tasnif çalışması için bkz.: United States General Accounting Office, **Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems**, (March 2004).

6 Thomas **Rid** ve Peter **McBurney**, "Cyber-Weapons", **Rusi Journal**, (February-March, 2012), p.8.

7 a.g.e., p.8.

8 a.g.e., p.8. Yüksek potansiyele sahip zararlı yazılımlar hakkında yönetici özeti mahiyetinde bir çalışma için bkz.: Dale **Peterson** "Offensive Cyber Weapons:

İtalyan bilişim uzmanı Stefano Mele, siber saldırı silahının tanımını yapmadan önce üç unsurun incelenmesini gerekli görerek, bunların, saldırıda kullanılan yazılım ve donanımın muhteviyatı (context), amaç (purpose) ve araçlar (mean/tool) olduğunu öne sürmüştür[9]. Buna göre bir siber saldırı silahı, 'ulus veya ulus-dışı aktörler tarafından, bir çatışma sırasında saldırılan hedefin hassas bilişim sistemlerine veya altyapısına ya da insanlarına, dolaylı da olsa zarar vermek veya doğrudan bilişim sistemlerini tahrip etmek, ya da bu sistemlere karşı sabotaj düzenlemek amaçlarıyla kullanılan bir bilgisayar işlemi, ekipmanı veya aracıdır.'[10]. King's College'dan güvenlik uzmanı Thomas Rid ve bilgisayar bilimleri uzmanı Peter McBurney de, siber silahı tanımlarken, silah kavramının ontolojik açıklamasından yola çıkmışlardır. Buna göre siber silah, yapılara, sistemlere veya canlılara fiziksel, işlevsel veya psikolojik zarar vermek üzere tasarlanan veya kullanılan bir bilgisayar kodudur[11].

Mele ile Rid ve McBurney'nin tanımları, siber saldırı silahının ne olduğu veya olmadığı hakkında yetkin bir çerçeve oluşturmaktadırlar. Buna karşın, her iki tanım da dikkatli okunduğunda önemli eksikliklere sahip görünmektedirler. Mele'nin tanımında siber silahın 'bir çatışma ortamında' kullanılan yazılım ve donanımları ifade ettiği vurgusu vardır. Bu ifadeden barış zamanında kullanılan zararlı bir programın saldırı silahı kapsamına girmeyecebileceği gibi bir sonuç çıkarılabilir. Oysa, aşağıda incelenecek olan Stuxnet saldırısında görüleceği gibi, bugüne kadar vuku bulan en önemli siber saldırılar iki devletin silahlı bir çatışma halinde oldukları durumlarda değil, normal barış koşullarında gerçekleşmişlerdir. Rid ve McBurney ise tanımlarını oldukça geniş ve soyut bir çerçeveye yerleştirerek, siber saldırı silahının bir 'yapı'ya veya 'sistem'e zarar vermek amacıyla tasarlanıp kullanılan yazılım ve programlar olarak betimlemiş, ancak bu

---

Construction, Development, and Employment", **The Journal of Strategic Studies**, Vol.36, No.1, (2013), pp.120-124.

9 Stefano **Mele**, **Cyber-Weapons: Legal and Strategic Aspects**, Italian Institute of Strategic Studies "Niccolò Machiavelli", Rome, (June 2013), p.10.

10 a.g.e., p.10.

11 **Rid** ve **McBurney**, p.7.

hedef alınan yapı ve sistemlerin neler olduğu konusunda daha ileri bir açıklamaya girişmemişlerdir. Yapı ve sistemden kastedilen nedir? Bu kavramlar sadece hedef ülkenin stratejik önemi haiz kamusal alanında faaliyet gösteren resmi kurumlarını mı ifade etmektedir, yoksa özel teşebbüse ait kurumları da kapsamakta mıdır? Silah, yazarların iddia ettiği gibi, esasta sadece bir 'yazılım' olan bir tür 'bilgisayar kodu' ise, bu durumda söz konusu kodun üzerinde bulunduğu 'donanım'ın da silah kapsamına girmesi gerekmez mi? Mele ile Rid ve McBurney'nin açıklamaları, bu ve benzeri sorulara ayrıntılı cevaplar vermez. Yine de, yukarıda belirtildiği gibi, siber silah tanımını mevcut şartlarda en yetkin şekilde yaptıkları kabul edilebilir.

II. STUXNET VİRÜSÜ VE SALDIRISI

Bilişim teknolojilerinde olağanüstü bir ilerlemenin kaydedildiği son on yıl içinde kuvvet kullanma fiili kapsamında en azından üç önemli siber saldırı eyleminin gerçekleştiği bilinmektedir. Bunlardan ilk ikisi Rusya tarafından 2007'de Estonya'ya karşı, 2008'de ise Gürcistan'a karşı girişildiği iddia edilen harekatlar; üçüncüsü ise, ABD tarafından 2009'da İran'a karşı düzenlendiği öne sürülen saldırıdır[12]. Bugün bilişim ve uluslararası hukuk çevrelerinde en çok tartışılan saldırı işte bu sonuncusudur. Kullanılan virüsün adıyla 'Stuxnet saldırısı' olarak bilinen bu harekatın 2009'da ABD tarafından İran'ın Natanz nükleer yakıt zenginleştirme tesislerine karşı düzenlendiğine inanılmaktadır[13].

---

12 Herbert **Lin**, "Cyber Conflict and İnternational Humanitarian Law", **International Review of the Red Cross**, Vol.94, No.886 (Summer 2012), p.519. Estonya ve Gürcistan'da gerçekleştirilen siber saldırılarla ilgili bir rapor için bkz.: William C. **Ashmore**, **Impact of Alleged Russian Cyber Attacks,** School of Advanced Military Studies, Fort Leavenworth. (2009). Kritik altyapılara yönelik siber saldırılar ve güvenlik önlemleri hakkında bir inceleme için bkz.: Gary **Mcgraw** "Cyber War is Inevitable (Unless We Build Security In)" **The Journal of Strategic Studies**, Vol.36, No.1(2013), pp.109-119.

13 ABD Stuxnet'le bir ilgisi olduğunu doğrulayan resmi bir açıklama yapmamış, ancak bu virüsün yazılması ve saldırı amacıyla kullanılmasında bir rolü olduğunu da hiçbir zaman yalanlamamıştır. Savunma Bakan Yardımcısı William Lynn, CNBC'den Melissa Lee'nin "ABD Stuxnet'in geliştirilmesinde herhangi bir

Virüsün varlığı ve saldırı hakkında ayrıntılı bilgiye aslında saldırıdan yaklaşık bir sene sonra ulaşılabilmiştir. 2010 yılının Mayıs ayında Minsk'de bulunan Virusblokada isimli Ukrayna bilişim şirketi, Microsoft Windows işletim sistmlerinde zararlı etki gösterme olasılığı bulunan bir virüs programı keşfetmiştir[14]. Programın o güne kadar rastlanılan tüm zararlı yazılımlardan daha karmaşık bir yapıya sahip olduğunun farkedilmesi üzerine, İsrail anti-virüs program yazılım şirketi Kaspersky ve Amerikan yazılım şirketi Microsoft ile birlikte virüsün kaynağını bulmak üzere ortak bir araştırma başlatılımış, araştırmaya daha sonra Amerikan bilişim güvenlik şirketi Symantec de dahil olmuştur[15]. Bulgulara göre, İran'ın Natanz nükleer yakıt zenginleştirme tesislerindeki bilgisayar ağına karşı düzenlenen virüs saldırısı iki ayrı tarihte gerçekleştirilmiş olup, birinci saldırı 22 Haziran 2009'da yerel saatle 16.30'da, ikinci saldırı ise 7 Temmuz 2009 tarihinde yerel saatle 17.00'de meydana gelmiştir[16]. Virüs üzerinde çalışan uzmanlar, saldırının hedefinin tesislerdeki Alman Siemens şirketi tarafından üretilmiş olan 'Simatic WinCC Step7' isimli denetleme kontrol ve veri toplama sistemi

---

şekilde yer aldı mı?" sorusunu son derece politik bir cevapla geçiştirerek önce sorumluluğun başka ülkelerde olabileceğini ima etmiş, ardından bunun şu anda cevaplandırabileceği bir soru olmadığını açıklamıştır. Ancak bilişim çevreleri, Stuxnet'in teknik özelliklerini göz önünde bulundurarak, programın ABD tarafından geliştirilip saldırının da yine bu ülke tarafından düzenlendiğine kesin gözüyle bakmaktadırlar.

Lynn'ın röportajı için bkz.: http://www.youtube.com/watch?v=_9Gt2Ek4inM.

14 Sean **Collins**, Stephen **McCombie**, "Stuxnet: The Emergence Of a New Cyber Weapon And Its Implications" **Journal of Policing, Intelligence and Counter Terrorism**,Vol.7, No.1(April 2012), p.84.

15 a.g.e., s.85. Virüs Symantec tarafından önce 'W32.Temphid' olarak isimlendirilmiş, daha sonra bu isim 'W32.Stuxnet' olarak değiştirilmiştir. Stuxnet adı, bir yazılım nesnesi olan '.stub' ve 'sürücü dosyası' anlamındaki 'mrxnet.sys' kelimelerinin birleşiminden oluşmaktadır. Stuxnet, keşfedildiği tarihe kadar görülmemiş seviyede kompleks yazılım özelliklerine sahip bir programdır. Virüsü benzerlerinden ayıran özelliklerinin incelendiği bir rapor için bkz.: Thomas M. **Chen**, **Stuxnet, The Real Start of Cyber Warfare?,** IEEE Network (November/ December 2010), p.2-3.

16 http://www.wired.com/threatlevel/2011/07/stuxnet-timeline/

(Supervisory Control and Data Acquisition, SCADA) adlı program olduğunu bulmuşlardır[17]. SCADA, enerji üretim ve dağıtımının kontrolü, su, doğal gaz, kanalizasyon sistemleri gibi kritik altyapıların kontrol edilmesi ve izlenmesinde kullanılmaktadır[18]. ABD resmi makamları veya yetkilileri, yukarıdaki dipnotta belirtildiği üzere, saldırıda kendilerinin bir rolü olduğuna veya olmadığına dair bir açıklama yapmamışlardır. İran hükümeti adına resmi açıklama yapan Buşer Nükleer Güç Tesisleri yöneticisi Mahmud Caferi, tesislere karşı bir siber saldırı düzenlendiğini onaylamış, ancak muhtemelen siyasi prestij kaygıları nedeniyle, bu saldırının önemli bir hasara neden olmadığını belirtmiştir[19]. Bunun gerçeği yansıtmadığı ise, aşağıda görüleceği gibi, konuyla ilgili uzmanların araştırmaları sonucunda ortaya çıkmıştır.

Stuxnet basitçe bir bilgisayar virüsü olarak anılsa da, esasen uzaktaki bilgisayar sistemlerine nüfuz etmesi ve bunları kontrol altına alması için tasarlanmış son derece kompleks bir bilgisayar programıdır[20]. Programın

---

17 http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/ Virüsün SCADA sistemi üzerindeki etkileri hakkında ayrıntılı bir değerlendirmenin yapıldığı konferans bildirisi için bkz.: Stamatis **Karnouskos**, **Stuxnet Worm Impact on Industrial Cyber-Physical System Security**, IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society, (2011). http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6109934. Saldırının hedef alınan sistemleri ne şekilde etkilediği hakkında Uluslararası Güvenlik ve Bilim Enstitüsü'nün (Institute for Science and International Security, ISIS) raporu için bkz.: David **Albright**, Paul **Brannan**, Christina **Walrond**, **Stuxnet Malware and Natanz: Update of ISIS Report** (December 22, 2010). http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/. Santrifüjlerin nasıl devre dışı bırakıldığıyla ilgili teknik bir rapor için bkz.: Ralph **Langner**, **To Kill a Centrifuge A Technical Analysis of What Stuxnet's Creators Tried to Achieve**, The Langner Group, (November 2013).

18 Mehmet **Kara**, Soner **Çelikkol**, **4. Ağ ve Bilgi Güvenliği Sempozyumu Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği**, Atılım Üniversitesi, 25-26 Kasım 2011.

19 http://www.bbc.co.uk/news/world-middle-east-11414483

20 James P. **Farwell**, Rafal **Rohozinski**, "Stuxnet and The Future of Cyber War", **Survival** Vol.53, No.1 (February–March 2011), p.24. Stuxnet'in sınıflandırıl-

nasıl çalıştığı ve nüfuz ettiği bilgisayar sistemlerinde ne gibi bir etki gösterdiğini bütün teknik ayrıntılarıyla incelemek bu makalenin kapsamı dışında kalan bilişim teknolojileriyle ilgili bir ihtisas konusudur. Ancak, bir devlete karşı kuvvet kullanma fiili olarak yorumlanıp yorumlanamayacağına karar verebilmek adına, kuşkusuz virüsün nükleer yakıt zenginleştirme süreci üzerinde nasıl bir tesir bıraktığının anlaşılabilmesi şarttır. Stuxnet, hedef aldığı Simatic WinCC Step7 yazılımına yönelik ele geçirme işlemini iki aşamada gerçekleştirmiştir. Birinci aşamada, virüs, uranyum-235 ayrıştırması ve konsantrasyonu için gerekli olan santrifüjün yaratılmasında kullanılan motorların hızını belirleyen Programlanabilen Mantık Kontrolörleri'ni (Programmable Logic Controller, PLC) kontrol altına almıştır[21]. PLC'ler esasen, endüstriyel üretim sektörlerindeki elektromekanik süreçlerin otomasyonunda kullanılan sayısal bilgisayarlardır. Virüs, ikinci aşamada, söz konusu PLC'lerin ürettiği santrifüjleri besleyen elektrik akımlarının frekansını sürekli olarak alçaltıp yükselterek değiştirmeye zorlamış, böylece zenginleştirme sürecinin kesintiye uğramasına neden olmuştur[22]. Stuxnet, bu frekans değiştirme işlemini olağanüstü bir hızda - her 100 milisaniyede sisteme bir komut göndererek - gerçekleştirmiştir[23]. Bu işlevi göz önüne

---

masıyla ilgili bir görüş için bkz.: Ryan **Jenkins**, "Is Stuxnet Physical? Does It matter?" **Journal of Military Ethics**, Vol.12, No.1(2013), pp.68-79. Programla ilgili çevrimiçi olarak yayınlanan ayrıntılı bir teknik rapor için bkz.: John **Richardson**, **Stuxnet as Cyberwarfare: Applying The Law of War to The Virtual Battlefield**.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888

21 a.g.e., p.24. Programın nasıl çalıştığı ve sistemi ne şekilde enfekte ettiğiyle ilgili ayrıntılı bir rapor için bkz.: Nicolas **Falliere**, Liam O **Murchu**, Eric **Chien**, **W32.Stuxnet Dossier** Symantec Security Response, Symantec (February 2011).

22 http://www.symantec.com/connect/blogs/stuxnet-breakthrough

23 Ralph **Langner**, "Stuxnet: Dissecting a Cyberwarfare Weapon", **Journal IEEE Security and Privacy**, Vol.9, Issue3 (May/June 2011), p.50. Langner'e göre, virüs Siemens sistemi üzerinde bir 'kesme kodu' (interrupt handler) gibi davranmıştır. Bir bilgisayardaki işlemci herhangi bir işlemi yürütürken kesme kodu algıladığında yürütülen işlem durdurulmakta ve başka bir işlemin yapılmasına olanak verilmektedir. Stuxnet'in bu özelliği sayesinde zenginleştirme sürecini bütünüyle durdurmadığı, fakat sistemdeki elektrik frekanslarını sürekli değiştirmek suretiyle

alındığında, virüsün uranyum zenginleştirme sürecini veya tesislerini bütünüyle sabote etmek değil, tesislerdeki çalışmayı sekteye uğratmak maskadıyla geliştirildiği ve sisteme yüklendiği anlaşılmaktadır. Natanz'daki SCADA sisteminin internet üzerinden bir ağ bağlantısına sahip olmadığı dikkate alındığında, virüsün bir USB hafıza ünitesi veya taşınabilir bir bilgisayar ile Simatic WinCC Step7'ye bulaştırıldığı kesin gibidir[24]. Natanz ve diğer tesislerdeki mevcut olan teknik sorunlar nedeniyle Stuxnet saldırısının uranyum zenginleştirme programı üzerindeki kesin etkisini hesaplayabilmek zordur[25]. Ancak saldırı sonucunda 1000 adet santrifüjün zarar gördüğü, bunların 600'ünün değiştirildiği bilinmektedir[26].

III. ABD'NİN SİBER SALDIRI STRATEJİSİ ÇERÇEVESİNDE KUVVET KULLANMA YAKLAŞIMI

11 Eylül terör saldırılarından sonra ABD'deki politika yapıcı çevrelerin belirlediği siber savaş stratejisi savunma kadar saldırı anlayışını da yansıtmıştır. Saldırı anlayışını yansıtan en önemli resmi belge, Başkan Barack Obama tarafından Ekim 2012'de imzalanarak yürürlüğe giren 20 numaralı

---

santrifüjlerin normal çalışmasını aralıklarla kesip yeniden başlattığı anlaşılmaktadır.

24 Stamatis **Karnouskos**, **Stuxnet Worm Impact on Industrial Cyber-Physical System Security,** p.4491. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.259.7495

25 **Stuxnet: Targeting Iran's Nuclear Programme**, IISS Strategic Comments, (30 Mar 2011). http://www.tandfonline.com/doi/abs/10.1080/13567888.2011.575612#preview

26 Emilio **Iasiello**, **Cyber Attack: A Dull Tool to Shape Foreign Policy,** 5th International Conference on Cyber Conflict. (2013). Stuxnet'in yarattığı etkiyle ilgili bir değerlendirme için bkz.: Jon R. **Lindsay**, "Stuxnet and The Limits of Cyber Warfare" **Security Studies**, Vol.22, pp.365-404 (2013). ISIS'e göre, saldırının gerçekleştiği 2009 senesinde Natanz'daki santrifüj sayısı yaklaşık 8.000'dir. Ancak tesislerde oluşan zararı tespit edebilmek için toplam santrifüj / zarar gören santrifüj oranına başvurmanın ne derecede güvenilir bir hesaplama yöntemi olacağı hakkında bir yorum yapmak güçtür. En azından bu çalışma kapsamında hukuki bir sonuca ulaşmak için böyle bir hesaplamaya dayanarak fiilin yarattığı zararı tespit edebilmek mümkün gözükmemektedir.

Başkanlık Politika Yönetmeliği'dir (Presidential Policy Directive-20, PPD-20). Yönetmelikte, Saldırıcı Siber Etki Harekatları (Offensive Cyber Effects Operations, OCEO) olarak tanımlanan siber saldırıların ABD'ye dünya çapındaki ulusal amaçlarına ulaşabilmesi için 'eşsiz ve alışılmadık' bir kabiliyet kazandıracağı vurgulanarak, bu saldırıların düşmana 'hiçbir uyarı yapılmadan' gerçekleştirileceği açıklanmıştır[27]. PPD-20, düşmana verilecek zararın ayrıntısına girmemiştir. Ancak belgede söz konusu zararın 'hafif'ten (subtle) 'ciddi'ye (severe) uzanan bir 'çeşitlilik' (range) içinde olacağının belirtilmesi, OCEO ile hedeflenen amacın - aynı Stuxnet saldırısında olduğu gibi - düşmanın maddi altyapısını veya üretim süreçlerini yok etmeye yönelik bir eylem gerçekleştirmek olduğunu göstermektedir. Yönetmelik, lafzı açısından değerlendirildiğinde, ABD'nin siber saldırı ile gerçekleştirebileceği bir kuvvet kullanma fiilini uluslararası hukukun öngördüğü evrensel normlara sadık şekilde yürüteceği şüpheli gözükmektedir. ABD'de hükümetin politikasına yakın çevreler de ülkenin bir siber tehdit altında olduğunu öne sürerek, kendilerine yönelik siber saldırıyı önemli bir tehlike olarak görmekte, bu nedenle aynı sistem ve yöntemlerle gerçekleştirilecek bir önalıcı saldırının (pre-emptive attack) meşru müdafa olarak yorumlanacağını savunmaktadırlar[28]. Amerikalı hukukçu Stewart Baker, ABD Hava Kuvvetleri'nden emekli Tuğgeneral Richard Dunlap'la birlikte kaleme

---

27 **Presidential Policy Directive/PPD-20**, (2012) p.9.

28 Mike **McConnell**, "Mike Mcconnell on How to Win the Cyber-War We're Losing", Washington Post (28 February 2010). http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html. Aslında istihbarat topluluğu önümüzdeki iki yıl içinde (2013 yılı itibarıyla) Rusya ve Çin gibi büyük devletler tarafından ABD'ye yönelik önemli bir siber saldırı gerçekleşme olasılığının uzak olduğunu kabul etmektedir. Tehdit olarak görülen, yalıtılmış devletler ve devlet-dışı aktörlerdir. Burada yalıtılmış devletlerin hangileri olduğu açıklanmamışsa da, bu tanımla İran ve Kuzey Kore gibi uluslararası sitemdeki statüko karşıtı revizyonist aktörlerin kast edildiği muhakkaktır. Siber saldırıyla ilgili Ulusal İstihbarat Direktörü tarafından hazırlanan ayrıntılı bir rapor için bkz.: James R. **Clapper**, **Statement for The Record Worldwide Threat Assessment Of The US Intelligence Community,** Senate Select Committee On Intelligence (2013). Önalıcı saldırı (pre-emptive attack) ve önleyici saldırı (preventive attack) kavramları ve aralarındaki fark üçüncü bölümde açıklanacaktır.

aldıkları makalesinde, hükümet içindeki uzmanların siber savaş konusunda hukuki sorularla uğraşarak ordunun siber ortamda savaşmasını imkansız hale getirdiklerinden yakınmıştır[29]. Stewart, kendi tezini savunurken İkinci Dünya Savaşı'nda Britanya Başbakanı olan Stanley Baldwin'in Almanya'nın bombalanmasıyla ilgili kuvvet kullanımı hakkında yaptığı açıklamasına atıfta bulunmuştur. Baldwin, yaptığı ünlü konuşmasında, en iyi savunmanın saldırı olduğunu belirterek, "Kendi kadınlarınızı ve çocuklarınızı korumak istiyorsanız düşmanın öldürdüğünden daha fazla kadını ve çocuğu daha hızlı şekilde öldürmelisiniz" şeklinde uluslararası hukukta kuvvet kullanmaktan kaçınma normlarının sınırlarını zorlayan bir strateji izlenmesini önermiştir[30]. Stewart Baker gibi tanınmış bir hukukçunun bir siber saldırıya engel olabilmek adına kadınların ve çocukların ölümüyle sonuçlanabilecek önleyici bir siber saldırıyı meşru görmesi, kuşkusuz kanunlarla ve etik değerlerle bağdaşan bir yaklaşım olarak kabul edilemez. Bu yaklaşım, ABD'de uluslararası hukuka mesafeli duran politik ve akademik çevreler arasında bile fazla taraftar bulmayacak kadar aşırılıkçı bir düşünceyi ifade etmektedir. Ancak Amerikan karar alma mekanizmasıyla çok yakın ilişkileri olan Baker gibi bir hukukçunun, sınırlı bir ölçüde de olsa, devletin resmi görüşünü yansıtıyor olabileceği unutulmamalıdır. ABD, siber saldırıda kuvvet kullanımıyla ilgili kararlarını Baker gibi aşırılıkçı reelpolitik yanlılarına danışarak vermeyecekse bile, ülkenin bir siber tehdit altında olduğu yönündeki algı ve PPD-20'nin söylemi dikkate alındığında, devletin stratejik ve politik amaçlarına ulaşmak için uygun gördüğü durumlarda siber saldırıya başvurmayı bir seçenek olarak değerlendireceği anlaşılmaktadır.

Esasen PPD-20'nin lafzı ve Baker gibi uluslararası hukukta kuvvet kullanmaktan kaçınma ilkesini ihlal etmeye eğilimli kişilerin dile getirdikleri sert söylemler, ABD'nin siber güvenlikle ilgili resmi devlet belgelerinde açıklanan stratejiden uzak bir duruşu ifade etmektedirler. Devletin resmi

---

29 Stewart A. **Baker**, Charles J. **Dunlap** Jr., "What Is the Role of Lawyers in Cyberwarfare?"http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/

30 Keith **Middlemas** and John **Barnes**, **Baldwin: A Biography**, Littlehampton Book Services Ltd., Worthing, 1969, p.735.

siber kuvvet kullanma politikası - ne kadar samimi olduğu bilinmese de - kuvvet kullanmaktan kaçınmak doğrultusunda bir anlayışı yansıtan barışçı bir retorik çerçevesinde yapılandırılmıştır. 2003 yılında hükümet tarafından yayınlanan Siber Uzayın Güvenliği için Ulusal Strateji (The National Strategy to Secure Cyberspace) adlı belge, özellikle Amerikan vatandaşlarının içinde yaşadığı, sahip olduğu ve kullandığı siber uzayın güvenli tutulması gibi rasyonel bir politika önermiştir. Belgede, ABD'nin stratejik hedeflerinin, Amerika'nın hassas altyapısına yönelik saldırıları önlemek, siber saldırıya karşı ulusal zaafiyeti azaltmak ve son olarak, hasarı ve toparlanma zamanını en aza indirmek olduğu açıklanmıştır[31]. Ocak 2008'de de Bush yönetimi, Kapsamlı Ulusal Siber Güvenlik Girişimi'ni (Comprehensive National Cybersecurity Initiative, CNCI) hayata geçirmiştir. CNCI'da açıklanan amaçlar, bilgisayar ağlarına sızılmasına karşı savunma geliştirmek, karşı-istihbarat sayesinde tüm tehditlere karşı ABD'yi savunmak ve gelecekte siber güvenliği eğitim, koordinasyon ve araştırma faaliyetleri ile güçlendirmektir[32]. 2009'da Beyaz Saray tarafından yayınlanan Siber Uzay Politika Değerlendirme (Cyberspace Policy Review) belgesinde ise, bilişim ve iletişim ağları hakkında ABD'nin ulusal hukuk düzenlemeleri kadar uluslararası hukukun da geçerli olduğu açıklanmıştır[33]. Bu belge, ABD'nin siber savaşta uluslararası hukuka saygılı olacağının belirtildiği önemli ve ender resmi yazılı kaynaklardan biridir. Savunma Bakanlığı'nın Temmuz 2011'de yayınladığı Siber Uzayda Harekat Stratejisi'nde de (Strategy for Operating in Cyberspace) ABD devlet sistemi dahilinde 15.000 ağ ve 7 milyon bilgisayar bulunduğu belirtilerek siber uzaya olan bağımlılık vurgulanmıştır[34]. Bu ağların ve bilgisayarların güvenliğinin sağlanması için de siber tehditlerin keşfedilmesi, ortaya çıkarılması, analiz edilmesi ve azaltılması gerektiğine dikkat çekilmiştir[35].

---

31 **The National Strategy to Secure Cyberspace**, (February 2003), p. viii.

32 **Comprehensive National Cybersecurity Initiative**, (Ocak 2008), s.1-2.

33 **Cyberspace Policy Review**, (2009), p.10.

34 **Strategy for Operating in Cyberspace**, (2011) p.1.

35 a.g.e., p.7.

Yukarıda açıklanan her bir resmi devlet belgesinin yazılış amacı ve lafzı dikkate alındığında, PPD-20 ile çelişir gibi görünen iki hususun ön plana çıktığı görülmektedir. Birincisi, ABD'nin siber güvenlik konusunda saldırgan değil savunmacı bir politika izleyeceğidir. Sözü edilen belgelerin hepsi siber saldırılara karşı 'savunma' faaliyetlerini düzenlemek amacıyla kaleme alınmış olup, hiçbirinde PPD-20'ye paralel bir 'saldırı' ifadesi yoktur. İkincisi, politika yapıcılarının siber savaş düzenlemeleri çerçevesinde ABD'nin uluslararası hukuka uyacağını belirtmeleridir. Beyaz Saray ve Savunma Bakanlığı tarafından yayınlanan belgelerde dile getirilen amaç, hedef ve yöntemler, ABD'nin uluslararası antlaşmalara ve örf-adet hukukuna uyacağı yönündedir. Bu değerlendirmeler dikkate alındığında, ABD'nin siber saldırıyı söz konusu resmi belgelerde öngörüldüğü gibi 'savunma amaçlı bir tedbir' olarak mı yoksa PPD-20'de vurgulandığı gibi 'saldırı amaçlı bir silah' olarak mı kabul ettiği önemli bir tartışma konusudur. Yukarıda incelenen Stuxnet saldırısı ve Stewart Baker gibi hukukçuların açıklamaları göz önünde tutulduğunda, ABD'nin siber silahları saldırı amacıyla kullanmayı -en azından belirli durumlarda- gerçekçi bir seçenek olarak elinde tutmak istediği görülmektedir. Siber saldırının özellikle ABD'de stratejik ve politik açıdan nasıl ele alındığına ilişkin daha derin bir inceleme bu makalenin kapsamı dışında olup, konunun uluslararası hukuktan çok uluslararası ilişkiler ve uluslararası güvenlik alanlarında yapılacak başka bir çalışmada değerlendirilmesi uygundur. Bu makale açısından önem taşıyan, bir siber saldırının kuvvet kullanmaktan kaçınma ilkesinin ihlali anlamına gelip gelmeyeceğidir ki, bu sorunun cevabı üçüncü bölümde tartışılacaktır.

IV. ULUSLARARASI HUKUKTA KUVVET KULLANMA

Bir egemen devletin başka bir egemen devlet üzerinde kuvvet kullanması, özellikle ulus-devlete dayalı uluslararası sistemin temellerinin atıldığı 1648 Westphalia Antlaşmaları'ndan sonra farklı uluslararası antlaşma, mutabakat ve konferanslarda ele alınmış ve yasaklanmıştır. Konuyla ilgili antlaşmalar incelendiğinde, bu uzun tarihsel sürecin 1. Dünya Savaşı'ndan sonraki bölümünün önem taşıdığı görülmektedir. 1919'da kurulan Milletler Cemiyeti, devletler arasındaki anlaşmazlıkların çözümü için savaşa başvu-

rulmasını kısıtlamıştır. Cemiyet'in kurucu metni olan Milletler Cemiyeti Sözleşmesi'nin 11. maddesine göre "Cemiyet Üyeleri, hakemlerin kararından ya da Konsey'in raporundan sonra üç aylık bir süre geçinceye kadar, hiçbir durumda savaşa başvurmamayı da kabul ederler."[36]. 1928'de 62 ülke tarafından imzalanan Briand-Kellogg Paktı ise uluslararası anlaşmazlıklarda savaş yolunun tercih edilmesinden vazgeçildiğini ilan etmiştir. Antlaşmanın 2. maddesine göre, "İmzacı devletler niteliği ve kaynağı ne olursa olsun, aralarındaki her türlü antlaşmazlık ve çekişmelerde barış yollarından başka bir yol izlememeyi esas aldıklarını kabul ve ilan ederler."[37]. Briand-Kellogg Paktı kuvvet kullanmaktan kaçınma ilkesini ilk defa bu kadar yalın biçimde dile getirmesi açısından önem taşıyan bir uluslararası hukuk düzenlemesidir.

Kuvvet kullanmanın yasaklanması hakkında Briand-Kellogg Paktı haricinde çeşitli siyasi ve diplomatik girişimler olmuşsa da, 2. Dünya Savaşı'nın sonuna kadar uluslararası açıdan hukuki bağlayıcılık teşkil eden bir antlaşma yürürlüğe girmemiştir. Birleşmiş Milletler'in (BM) 24 Ekim 1945'te kurulmasından dört ay önce, 26 Haziran 1945 tarihinde, halen kuvvet kullanımını düzenleyen asli antlaşma olan BM Sözleşmesi 50 devlet tarafından imzalanarak hayata geçirilmiş, takip eden yıllarda diğer devletler tarafından da imzalanarak kabul edilmiştir. BM Sözleşmesi'nin 2(4). maddesi, bugün kuvvet kullanmaktan kaçınma ilkesini *jus cogens* olarak düzenlemiş en önemli uluslararası hukuk normunu oluşturmaktadır. Söz

---

[36] Milletler Cemiyeti Sözleşmesi, uluslararası ilişkilerde kuvvet kullanmaktan kaçınılması amacıyla esasen hakemlik müessesesi üzerinde önemle durmuştur. Sözleşme'nin 13. maddesinin 1. fıkrasında "Cemiyet Üyeleri, aralarında, hakemlikle çözüme elverişli saydıkları bir anlaşmazlık çıkarsa ve bu anlaşmazlık diplomasi yoluyla istekleri karşılar bir biçimde çözülemezse, bu sorunun tümüyle hakemliğe sunulacağını kabul ederler."denmek suretiyle, olası çatışmaların çözümü için bir arabuluculuk mekanizması oluşturulmuştur. Aynı maddenin 3. fıkrası uyarınca, anlaşmazlığın sunulacağı hakemlik mercii, tarafların gösterdikleri ya da daha önce yapılmış sözleşmelerde öngörülen hakemlik mahkemesi olacaktır. Milletler Cemiyeti Sözleşmesi'nin 11. ve 13. maddeleri ve Sözleşme'nin tamamı için bkz.: http://avalon.law.yale.edu/20th_century/leagcov.asp

[37] **Briand-Kellogg Paktı**. Antlaşmanın 2. maddesi ve tamamı için bkz.: http://avalon.law.yale.edu/20th_century/kbpact.asp

konusu maddeye göre, "Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Milletler'in amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar."[38]. Sözleşme, kuvvet kullanımının iki koşulda kabul edilebileceğini belirtmiş olup, bunlardan birincisi, uluslararası barış ve güvenliğin tehdit altında olduğuna karar verilmesi halinde, Güvenlik Konseyi kararı ile kollektif kuvvet kullanımına başvurulmasıdır. İkincisi ise, Konsey kararı olmadan, bir saldırıya karşı meşru müdafa hakkının kullanılmasıdır. Kollektif güvenlik, her ne kadar bugüne kadar hukuki ve siyasi bağlamda çeşitli tartışmalara konu olan soyut bir başlık olagelmiş ise de, BM Sözleşmesi'nde belirgin sınırları olan normatif bir çerçevede ele alınıp düzenlenmiştir[39]. Sözleşme'nin VII. Bölümü'ndeki 39.-41. maddeler, ekonomik önlemler de dahil olmak üzere, devletlere karşı uygulanacak yaptırım-

---

38 **BM Sözleşmesi Madde 2(4).** İlgili madde ve Sözleşme'nin tamamı için bkz.: https://www.un.org/en/documents/charter/chapter1.shtml. BM Sözleşmesi'nin Türkçe metni için bkz.: http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/bm1.html

39 Kollektif güvenliğin ekonomik yaptırımlar ve insan haklarıyla ilgisi hakkında bir inceleme için bkz.: Eugenia **López-Jacoiste**, **The UN Collective Security System and its Relationship with Economic Sanctions and Human Rights**, **Max Planck Yearbook of United Nations Law** (Armin von **Bogdandy**, Rüdiger **Wolfrum,** eds.) Vol.14 (2010), pp.273-335. 2.Madde hakkında ayrıntılı bir çalışma için bkz.: Stefan **Talmon, A Universal System of Collective Security Based on the Charter of the United Nations: A Commentary on Article 2(6) UN Charter**, Bonn Research Papers on Public International Law Paper, No.1, Institute of Public International Law, University of Bonn (20 November 2011). Kollektif güvenlikte ABD'nin rolü hakkında bir değerlendirme için bkz.: Kenneth **Anderson**, "United Nations Collective Security and the United States Security Guarantee in an Age of Rising Multipolarity: The Security Council as the Talking Shop of the Nations", **Chicago Journal of International Law**, Vol.10, No.1 (2009). Kollektif güvenlik ve insan hakları ilişkisi hakkında bir araştırma için bkz.: **Hierarchy in International Law: The Place of Human Rights**, (Erika de **Wet**, Jure **Vidmar**, eds.), Antonios **Tzanakopoulos**, "Collective Security and Human Rights", Oxford University Press, Oxford, 2012, pp.42-70.

ları; 42.-48. maddeler askeri müdahaleyi; 49.-51. maddeler ise meşru müdafa hakkını düzenlemiştir[40].

Güvenlik Konseyi kararı olmadan gerçekleştirilebilecek bir askeri müdahale kapsamında başvurulacak kuvvet kullanımı, yukarıda belirtildiği üzere, sadece 51. maddede belirtilen meşru müdafa hakkı çerçevesinde izin verilebilir bir fiildir. Söz konusu madde meşru müdafa hakkını "Bu Antlaşma'nın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez" şeklinde tanımladıktan sonra, inisiyatifi tekrar Konsey'e bırakmak üzere şu hükmü getirmiştir: "Üyelerin bu meşru savunma hakkını kullanırken aldıkları önlemler hemen Güvenlik Konseyi'ne bildirilir ve Konsey'in işbu Antlaşma gereğince uluslararası barış ve güvenliğin korunması ya da yeniden kurulması için gerekli göreceği biçimde her an hareket etme yetki ve görevini hiçbir biçimde etkilemez."[41].

Siber saldırının bir kuvvet kullanma olarak tanımlanıp tanımlanamayacağını cevaplayabilmek için öncelikle BM Sözleşmesi'ndeki 2(4). maddenin nasıl yorumlanacağını incelemek yerinde olacaktır. Viyana Andlaşmalar Hukuku Sözleşmesi (VAHS) bu sorunun cevaplanması için başvurulabilecek uygun bir kaynaktır. Sözleşme'nin 31. maddesine göre "Bir antlaşma, hükümlerine antlaşmanın bütünü içinde ve konu ve amacının ışığında verilecek alışılagelmiş anlama uygun şekilde iyi niyetle yorumlanır."[42].

---

40 BM Sözleşmesi VII. Bölümü hakkında ayrıntılı bir açıklama ve sınıflandırma grafiği için bkz.: Seven Bernhard **Garesi**, Johannes **Varwick**, **The United Nations, An Introduction**, Palgrave MacMillan, New York, 2005, p.81.

41 **BM Sözleşmesi**, VII. Bölüm. https://www.un.org/en/documents/charter/chapter7.shtml. Sözleşme ve ilgili bölümün Türkçesi için bkz.: http://www.uhdigm. adalet.gov.tr/sozlesmeler/coktaraflisoz/bm1.html

42 **Viyana Andlaşmalar Hukuku Sözleşmesi**, Madde 31. http://www.admiraltylawguide.com/conven/lawoftreaties1969.html Sözleşmenin ve ilgili maddenin Türkçesi için bkz.: http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/bm1.html

Maddenin bu ifadesi geniş şekilde yorumlanırsa, 'kuvvet', fiziksel saldırıları ve ekonomik, diplomatik ve propagandaya yönelik eylemler gibi zorlayıcı önlemlerin tümünü ihtiva eden geleneksel kavramlardan oluşmaktadır[43]. Ancak VAHS, aynı madde içinde, bir antlaşmanın 'amaç' ve 'niyet'ine göre de yorumlanabileceğini belirtmektedir. BM'nin kuruluş amacı ve BM Sözleşmesi'nin imzalanmasındaki niyet 'gelecek nesilleri savaştan korumak için uluslararası barış ve güvenliği sağlamak' olarak açıklandığından, burada kuvvet sadece dar anlamda askeri önlemleri ihtiva eden bir olgu olarak kabul edilmiştir[44].

Siber silahlar, yukarıdaki kavramsal çerçevede açıklanmaya çalışıldığı gibi, çok amaçlı enstrümanlar olup bir saldırıyı destekleyici yardımcı araç olarak kullanılabildikleri gibi, asli saldırı silahı olarak da kullanılabilirler[45]. Siber silahlar, internet trafiğini geçici olarak karışıklığa sürüklemek amacıyla veya bir elektrik güç ünitesine komut göndererek -Stuxnet saldırısında olduğu şekilde- söz konusu ünitenin imha olması gibi fiziksel tahrip yaratmak maksadıyla devreye sokulabilir[46]. Böylesine geniş spektrumda işlev gören silahların kullanılacağı bir siber saldırının kuvvet kullanma

---

43 Michael **Gervais** "Cyber Attacks and the Laws of War", **Berkeley Journal of International Law,** Vol.30, Issue 2 (2012), p. 536.

44 a.g.e., p.537. Yazar burada, 2(4). madddenin kuvvet kullanımını dar anlamda tanımladığını göstermek için BM Sözleşme'sinin *travaux préparatoires*'ını (hazırlık çalışmaları) örnek göstermiştir. Sözleşme'nin hazırlık safhasında Brezilya kuvvet kullanımına ekonomik müeyyide gibi tedbirlerin de dahil edilmesini istemiştir. Ancak bu öneri kurucu üyeler tarafından reddedilmiştir. Bu durum, Gervais'in belirttiği gibi, Sözleşme'nin kuvvet kullanma fiili olarak sadece askeri önlemleri kabul ettiğinin ispatı olarak değerlendirilebilir. Öte yandan, 'iletim yöntemi' yaklaşımında aslında 'yöntem'den çok siber silahın yaratacağı 'etki'ye önem atfedilmiştir. Yazarın bu yaklaşımı 'iletim yöntemi' başlığıyla tanımlaması çok da yerinde görünmemektedir. BM'nin kuruluş amacı ve niyeti hakkındaki başlangıç hükmü için bkz.: https://www.un.org/en/documents/charter/preamble.shtml. Aynı hükmün Türkçe metni için bkz.: BM Sözleşmesi, Giriş Notu, S.4. http://www.uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/bm1.html

45 a.g.e., p.537.

46 a.g.e., p.537.

anlamına gelip gelmediğine karar verebilmek oldukça güçtür. Bu kararı verebilmek için kullanılan en yetkin ölçütler Schmitt ölçütleridir ki, bunlar aşağıda ele alınacaktır. Ancak bu ölçütlere gelmeden önce literatürde rastlanan diğer yaklaşımlara değinmekte fayda vardır. Bu yaklaşımlardan biri, saldırının iletim yöntemini (delivery method) incelemeye yöneliktir. Saldırıda kullanılan siber silahtaki yazılımın türünü dikkate alan bu görüşe göre, dünya çapında çok sayıda bilgisayar sisteminde etki gösterebilen bir virüs ciddi zararlara neden olabilecekken, daha az etkili bir program göreceli olarak daha düşük hasara yol açabilecek, saldırının bir kuvvet kullanma olup olmadığı buna göre saptanacaktır[47]. Kuvvet kullanma olgusunu inceleyen ikinci yaklaşım, siber silahları 'kusursuz sorumluluk' (strict liability) standardı altında ele alınmasına dayalıdır. Siber saldırının 'anlık tahrip' (instantaneous destructive) anlamına geleceğini öne süren bu görüş, bu tip bir tahribin tartışmasız biçimde meşru müdafaya cevaz vereceğini iddia etmekte, böyle bir karşılığa neden olacak bir siber saldırının da mutlak surette bir kuvvet kullanımı sayılması gerekeceğini öne sürmektedir[48]. Üçüncü yaklaşım ise siber silahları, saldırı sonucunda yaratacakları etkiyi dikkate alarak, geleneksel fiziksel silahlara eşit bir araç olarak kabul etmektedir. Bu görüşe göre de, saldırının sonucu, fiziksel bir silahın neden olabileceği sonuca eşit ise, siber silah farklı bir şekilde değerlendirilmemeli, doğrudan bir kuvvet kullanımı olarak kabul edilmelidir[49].

Siber saldırının kuvvet kullanımı olarak yorumlanıp yorumlanmayacağına karar verebilmek için saldırı sonucunda 'meydana gelen etkileri' incelemek, esasta konuyla ilgili başka hukukçular tarafından da kabul gören

---

47 a.g.e., s.538.

48 Walter Gary **Sharp**, **Sr.**, **Cyberspace and The Use of Force,** Ageis Research Corp, Falls Church (1999), p.129-131.

49 Ian **Brownlie**, **International Law and The Use of Force by States,** Oxford University Press, Oxford, 1963, p.362. Brownlie'nin kuvvet kullanma yaklaşımı, siber savaş olgusunun teknolojik açıdan söz konusu olmadığı bir döneme denk gelmektedir. Bu nedenle, sözü edilen yaklaşımı savunanlar, o dönemde kimyasal ve biyolojik silahların fiziksel tahrip yaratmamalarına rağmen bir kuvvet kullanımı olarak sınıflandırılmalarını örnek göstererek, aynı yaklaşımın siber silahlar için de geçerli olabileceğini ileri sürmektedirler.

bir yöntemdir. Lin, bir siber saldırının ancak hedef üzerinde 'belirli bir etki' (a specified effect) yaratması durumunda, 51. madde kapasımda bir meşru müdafaya cevaz verecek bir kuvvet kullanımı olarak kabul edilebileceğini öne sürmektedir[50]. Ancak bir siber saldırı, casusluk amacıyla, ekonomik yaptırımlar çerçevesinde veya seçim sonuçlarını etkilemek için örtülü operasyon düzenleme gibi siyasi bir amaçla gerçekleşmişse, bir kuvvet kullanma olarak yorumlanmayacaktır[51]. Lin'in bu yaklaşımı aslında askeri terminolojideki 'etki-odaklı harekat' (effect-based operation) kavramının bir ifadesidir. Etki-odaklı harekatın işlevsel değeri ve uygulanabilirliği, özellikle ABD ulusal güvenlik çevrelerinde her zaman tartışmalı bir kavram olagelmiştir. Bir siber saldırının yarattığı etki o saldırının bir kuvvet kullanma olarak kabul edilip edilmeyeceğini belirlemede asli ölçüt olacaksa, öncelikle etki-odaklı harekatın incelenmesinde yarar vardır.

Etki-odaklı harekat, bazı çevrelerde 'hedeflenen amaca hizmet eden bir yöntem' olarak kabul edilirken, bazıları tarafından 'bilinen bir olguyu dikkat çekici bir isimle yeniden tanımlama girişimi' olarak görülmüştür[52]. Kavramı askeri literatüre kazandıran isim, 1991 Körfez Savaşı'nda ABD Hava Kuvvetleri Birleşik Hava Gücü Komutanı olan Tuğgeneral David A. Deptula'dır. Deptula, bir saldırıda zaferi belirleyecek olan unsurun, 'düşman için verimli görülen güvenilir sistemleri etkin şekilde kontrol altında tutmak' olduğunu iddia etmiştir[53]. Bu bağlamda, sözgelimi hava kuvvetlerinin etkin kullanımı, 1991 Körfez Savaşı'nda Irak'ın silahlı kuvvetlerini felç eden ve savaşma isteğini kıran asıl etken olarak yorumlanmaktadır. Bu tip bir kuvvet kullanımında esas olan, karşı tarafın yıpratılması veya tümüyle imha edilmesi için düşman unsurlarının bir hedef listesi dahilinde gelişigüzel vurulması değil,

---

50 Herbert S. **Lin**, "Offensive Cyber Operations and the Use of Force", **Journal of National Security Law & Policy,** Vol.4. No.63 (2010), p.73.

51 a.g.e., p.73.

52 Etki-odaklı operasyon hakkında iki görüşü de inceleyen tarafsız bir değerlendirme için bkz.: Gary H. **Cheek**, **Effects-Based Operations: The End of Dominant Maneuver?** Carlisle Barracks, U.S. Army War College, (April 2002).

53 David A. **Deptula**, **Effects-Based Operations: Change in the Nature of Warfare,** Aerospace Education Foundation, Arlington (2001), p.18.

kuvvet kullanımıyla düşman unsurlar üzerinde 'belirli etkiler'e ulaşılmasıdır. Buna göre, etki-odaklı harekat, barış, kriz ve savaş durumlarında, dost, düşman veya tarafsız unsurların davranışlarına şekil vermeye yönelik eşgüdüm içinde icra edilen harekettir[54]. Ancak etki-odaklı harekat, yıpratma, yoketme, zorlama ve taktik manevra gibi diğer savaş konseptlerinin yerini almak için tasarlanmış bir yöntem de değildir[55]. Deptula'nın genel kabul gören bu tanımı ışığında incelendiğinde siber saldırının etki-odaklı bir harekat olarak değerlendirilebileceği muhakkaktır. Gerçekten, Stuxnet örneklemi göstermiştir ki, bir devlet (ABD) siber saldırıyı barış durumunda başka bir devletin (İran) politikasını etkilemek veya değiştirmek için kullanmıştır.

Siber saldırı sonucunda meydana gelebilecek olan fiziki zararın, geleneksel silahlarla yapılan saldırı sonucunda meydana gelecek zarar eşiğine ulaşma olasılığı azımsanamayacak derecede yüksektir[56]. Stuxnet saldırısından sonra Natanz'da insan veya mal kaybına neden olan fiziksel bir etki gözlemlenmemişse de, bu saldırı, yaratabileceği etkileri açısından bu yargıyı doğrulamaktadır. Saldırı sonrasında tesisin soğutma sisteminde meydana gelebilecek bir arızanın nükleer serpintiye neden olmayacağını garanti etmek mümkün değildir. Sebep olabileceği etkiler göz önüne alındığında, siber saldırının fiziksel bir zarara neden olmasının 2(4). madde uyarınca bir saldırı fiili olarak yorumlanabileceği açıktır. Bu yorumun ışığında, bir siber saldırının 42. madde ile düzenlenen bir kollektif müdahaleye veya 51. madde ile

---

54 Edward A. **Smith**, **Effects-Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War**, Office of the Assistant Secretary of Defense, Command & Control Research Program, CCRP, Washington, DC (2006), p.14. Etki-odaklı operasonun önemi ve tarihsel gelişimi hakkında ayrıntılı bir inceleme için bkz.: Lee W. **Wagenhals**, Alexander H. **Levis**, Maris "Buster" **McCrabb**, **Effects-Based Operations; A Historical Perspective for a Way Ahead**, George Mason University, System Architectures Laboratory, C3I Center, Fairfax, (2003).

55 Edward C. **Mann III**, Gaiy **Endersby**, Thomas R. **Searle**, **Thinking Effects: Effects-Based Methodology for Joint Operations**, Air University, College of Aerospace Doctrine, Research and Education Paper, No.15 (October 2002) p.2.

56 Jonathan A. **Ophardt**, "Cyber Warfare and the Crime Of Aggression: The Need For Individual Accountability on Tomorrow's Battlefield", **Duke Law & Technology Review** Vol.9, No.3 (2010), p.15.

güvence altına alınan bir meşru müdafaya cevaz vereceğini varsaymak yanlış olmayacaktır.

i. Meşru Müdafa Hakkı ve Unsurları

Bir siber saldırının meşru müdafa hakkı yaratıp yaratmayacağı, aynı bu saldırının kuvvet kullanımı olarak yorumlanıp yorumlanamayacağı gibi tartışmalı bir konudur[57]. Soruyu cevaplamak için meşru müdafa hakkının ne şekilde doğabileceğini incelemekte fayda vardır. UAD eski yargıcı Robert Jennings ve Britanya Dışişleri Bakanlığı eski hukuk danışmanı Arthur Watts, yirminci yüzyılın başında yaşamış Alman uluslararası hukukçu Lassa Oppenheim'ın yeniden düzenledikleri eserinde, literatürde meşru müdafa hakkının hangi şartlarda oluşabileceğiyle ilgili en geniş genel kabul gören tanımlardan birini sunmuşlardır. Buna göre, bir devlet meşru müdafa hakkını ancak aşağıdaki şartlardan bir veya birden fazlasının gerçekleşmesi durumunda uygulayabilecek ve bir başka devlete karşı kuvvet kullanma fiili ancak bu durumlarda yasal olarak kabul edilebilecektir: a) bir devlete karşı silahlı saldırı düzenlenmesi veya doğrudan bir tehdit yöneltilmesi, b) saldırıya karşı savunma hareketine geçmek için acil bir gerekliliğin olması, c) pratik bir alternatifin bulunmaması ve bu saldırıyı önleyebilecek meşru gücü olan diğer devlet veya otoritelerin bu alternatifleri kullanamamaları, d) meşru müdafa kapsamında girişilecek hareketin saldırıyı engellemek için gerekli olanı yapmakla sınırlı tutulması[58].

---

57 Siber saldırının meşru müdafa hakkı bağlamında ele alındığı bir çalışma için bkz.: Titiriga **Remus,** "Cyber Attacks and International Law of Armed Conflicts; A "Jus Ad Bellum" Perspective", **Journal of International Commercial Law and Technology**, Vol.8, No.3 (July, 2013), pp.179-189. Uluslararası hukuk çevrelerinde siber saldırının tanımı ve meşru müdafaya cevaz verdiği konusunda bir uzlaşmaya varılması gerektiğini savunan bir görüş için bkz.: Matthew **Hoisington**, "Cyberwarfare and The Use of Force Giving Rise to The Right of Self-Defense", **Boston College International & Comparative Law Review**, Vol. 32 (2009), pp.439-454.

58 Robert **Jennings**, Arthur **Watts** (eds.), **Oppenheim's International Law**, Ninth Edition, Oxford University Press, Oxford, 1991, p. 412.

Burada görüldüğü gibi, meşru müdafa hakkının en önemli unsurlarından ikisi 'gereklilik' (necessity) ve 'orantılılık'tır (proportionality)[59]. Gereklilik, çatışmanın çözümü için barışçıl araçların mevcut olup olmadığı, saldırının doğası, tarafların maksatları ve uluslararası topluluğun işlevsel müdahale olasılığı bulunup bulunmadığı gibi unsurları ihtiva eden bir olgudur[60]. Orantılılık ise, saldırı veya tehdide karşılık vermek için kulanılacak olan gücün ölçeğini, kapsamını ve süresini kısıtlamaktadır[61]. Uluslararası hukukçu Yoram Dinstein, 'yakınlık' (immediacy) unsurunun da bu iki ölçütün yanında üçüncü ölçüt olarak kabul edilmesi gerektiğini belirtir. Bu ölçüte göre, bir müdafa fiilinin meşru kabul edilebilmesi için, orantılı ve gerekli olmasının yanısıra, 'zamanında', yani saldırıya 'yakın' bir zamanda yapılması da şarttır. Saldırı ve meşru müdafa arasında makul bir süreden daha fazla zaman olması, kuvvet kullanma gerekçesini zayıflatan bir etken olarak kabul edilebilecektir[62].

11 Eylül terör saldırılarının ardından meşru müdafa hakkı çerçevesinde kuvvet kullanımı geniş tartışmalara neden olmuştur. ABD'nin Cumhuriyetçi Parti yönetimindeki politika yapıcı mercileri ve bunlara yakın akademik çevreler, devlet fiziki bir saldırıya maruz kalmasa da, açık ve yakın bir tehlike (clear and present danger) ile yüzyüze olması durumunda meşru müdafa hakkının doğacağını iddia etmişlerdir. Bu çerçevede, doğrudan saldırıya uğramayan ancak varlığı yadsınamayacak bir saldırı tehdidi ile karşı karşıya kalan bir devletin bu tehidede karşı kuvvet kullanmasının meşru olacağı öne sürülmüştür. Bush doktrini olarak da bilinen bu strateji, ön-alıcı saldırı (pre-emptive attack) ve önleyici saldırı (preventive attack) olmak üzere iki müstakil başlık altında esasen 11 Eylül saldırısından çok

---

59 Graham H. **Todd**, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare With an Asymmetric Definition", Vol.64, Cyber Law Edition, **The Air Force Law Review,** (2009), p. 98.

60 **Operational Law Handbook,** International & Operational Law Depertmant, The Judge Advocate General's Legal Center, U.S. Army, Charlotsville, 2007, p.4.

61 a.g.e., s.4.

62 Yoram **Dinstein**, **War, Aggression and Self-Defence,** Cambridge University Press, 4th ed., Cambridge, 2005, pp.235-242.

daha önce kavramsallaştırılmıştır. 1956 ve 1967'deki Arap-İsrail savaşlarını inceleyen İsrailli siyaset bilimci Efraim Inbar, bir saldırının potansiyel bir düşman tehdidinin yok edilmesi amacıyla gerçekleşmesi durumunda 'önleyici' olarak kabul edilmesi gerektiğini; ani bir düşman saldırısı beklentisi üzerine gerçekleşmesi halinde ise 'ön-alıcı' olarak tanımlanması gerektiğini belirtmiştir[63]. Önleyici saldırı kavramı ABD resmi devlet belgelerinde yer almamış, ancak ön-alıcı saldırı resmi olarak 2002'de Ulusal Güvenlik Stratejisi (National Security Strategy) belgesinde açıklanmıştır. Buna göre, ABD teröristlere karşı meşru müdafaa hakkını kullanmak için gerekirse tek başına hareket etmekten çekinmeyecek ve kendi halkını ve ülkesini korumak için tehdit gördüğü unsurlar harekete geçmeden onlara karşı ön-alıcı saldırı düzenleyebilecektir[64].

Meşru müdafa hakkı kapsamında gerçekleştirilecek bir siber saldırının, yukarıdaki farklı ölçüt ve değerlendirmeler dikkate alındığında, ancak belirli durumlarda uluslararası hukuka uygun bir eylem olarak kabul edileceği görülmektedir. Jennings ve Watts'ın ölçütleri bu tip bir saldırıyı planlayacak ve icra edecek olan devletler için oldukça kısıtlayıcı bir çerçeve getirmektedir. Bu şartların sağlanması durumunda bile, bir siber saldırının meşru sayılması büyük oranda gerekli ve orantılı olma şartlarına bağlı olacaktır. Önleyici ve ön-alıcı saldırılar ise, kesin sınırları belli olmadığından ve siyasi amaçlar doğrultusunda hukuki bir düzenlemeye oturtulmadan uygulanabileceklerinden, meşruiyetleri tartışmaya açık uygulamalardır. Ön-alıcı saldırı

---

63 Efraim **Inbar**, "The "No Choice War" Debate in Israel", **Journal of Strategic Studies**, March (1989) p.35.

64 **The National Security Strategy of The United States of America**, (September 2002), p.6-15. Belge için bkz.: http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/ Önleyici ve ön-alıcı saldırı kavramları arasındaki fark ve konunun uluslararası hukuk açısından taşıdığı önem hakkındaki rapor için bkz.: Karl P. **Mueller**, Jasen J. **Castillo**, Forrest E. **Morgan**, Negeen **Pegahi**, Brian **Rosen**, **Striking First: Preemptive and Preventive Attack in U.S. National Security Policy**, 2006, RAND Corporation, p.1-15; p.121-182; p.189-211. Her iki kavramın meşru müdafaa hakkı açısından değerlendirilmesi için bkz.: Fatma **Taşdemir**, **Uluslararası Terörizme Karşı Devletlerin Kuvvete Başvurma Yetkisi**, USAK, Ankara, 2006, s.238-247.

doktrini Afganistan askeri müdahalesinde uygulanmış ve büyük ölçüde siyasallaştırılmış saikler nedeniyle uygulamaya koyulduğu için uluslararası hukukçular tarafından ağır eleştirilere hedef olmuştur. Meşru müdafaya yönelik bir siber saldırının bu doktrinler çerçevesinde gerçekleştirilmesi hukuki sakıncalarla birlikte siyasi sorunları da beraberinde getirecektir. Görünen odur ki, siber saldırının meşru müdafa kapsamında bir kuvvet kullanma fiili olarak kabul edilmesi ancak çok istisnai şartlar altında söz konusu olabilecektir. Bu tip bir saldırının fiziksel araç ve yöntemler yerine virüs, Trojan atı veya solucan gibi programlar aracılığıyla gerçekleştirilmesi, fiili geleneksel silahlarla yapılan askeri bir saldırıdan farklı kılmayacaktır.

ii. Tallinn Kılavuzu ve Schmitt Ölçütleri

Modern toplumlardaki altyapının yüksek teknolojiyle bütünleşmiş olması, siber saldırıların etkilerini konvansiyonel silahların yarattığı etkiler kadar ciddi bir seviyeye çıkarabilmektedir[65]. Böylesine güçlü etkiler neden olabilecek siber saldırılar için uygulanacak hukuki düzenlemeler, 2009 yılında NATO Müşterek Siber Savunma Mükemmeliyet Merkezi'nde (NATO Cooperative Cyber Defence Centre of Excellence, CCD-COE) ele alınmıştır. Estonya'nın Tallinn kentinde toplanan CCD-COE'ye bağlı Uluslararası Uzmanlar Grubu (International Group of Experts), siber savaş hakkında geçerli olabilecek düzenlemeleri, silahlı çatışma hukuku uzmanı Michael Schmitt'in editörlüğünde hazırladıkları kılavuzda yayınlamışlardır. Tallinn Kılavuzu olarak bilinen belge, siber savaşın *jus in bello* ve *jus ad bellum* boyutlarıyla ilgili bir doküman olup, siber suçlarla veya siber terörizmle ilgili bir muhteviyata sahip değildir[66]. Bağlayıcı bir nitelik taşımayan ancak bugüne kadar konuyla ilgili olarak hazırlanmış en kapsamlı uluslararası hukuk dokümanlarından biri sayılabilecek Kılavuz, öncelikle

---

65 Muharrem **Gürkaynak**, Adem Ali **İren**, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, , C.16, S.2, (2011) s.265.

66 Myrna **Azzopardi**, "The Tallinn Manual On The International Law Applicable To Cyber Warfare: A Brief Introduction On Its Treatment Of Jus Ad Bellum Norms", **Malta Law Review**, Vol.3 (2013), p.175.

siber uzayı 'uluslararası bir alan' olarak görmüş ve her devletin sadece kendi egemenlik alanında bir hakka sahip olabileceğini belirtmiştir. Kılavuz'un 1 numaralı kuralına göre, her devlet kendi egemenlik alanı içindeki kendi siber altyapısı ve faaliyetleri üzerinde kontrol yetkisine sahiptir[67]. Siber uzayın fiziksel bir olgu olmayışı sınırlarını tarif etmeyi güçleştirmekte; ancak aynı oranda da zorunlu kılmaktadır. Bu nedenle Kılavuz'da söz konusu alan açıkça tarif edilmiş, bu alanın ülkenin siber altyapısının (bilişim donanımlarının) bulunduğu kara bölgesi, iç sular, karasuları, takımada suları ve ulusal hava sahası olduğu belirtilmiştir[68].

Tallinn Kılavuzu'nun 11 numaralı kuralı siber saldırıyı kuvvet kullanımı açısından değerlendirmiştir. Buna göre, bir siber saldırı, ölçeği ve etkileri açısından kuvvet kullanma olarak yorumlanabilecek siber-dışı bir başka saldırıyla mukayese edilebilir seviyede ise kuvvet kullanımı anlamına gelir[69]. Bir devletin siyasi bağımsızlığı veya bölgesel bütünlüğüne yönelik bir kuvvet kullanımını veya tehdidi içeren bir siber saldırı da hukuka aykırı olarak kabul edilecektir[70]. 11 numaralı kuraldan, Kılavuz'da siber saldırının 'sebep olabileceği sonuçlara göre' değerlendirilmesi gerektiği yönünde bir anlayışın benimsendiği anlaşılmaktadır. Bu da belgede, saldırıların etki-odaklı harekat kavramı çerçevesinde değerlendirildiğini ortaya koymaktadır. Belgeyi hazırlayan uzmanlar grubu, kuvvet kullanımının tanımında kullanılacak uygun bir eşiğin belirlenmesi için UAD'nın *Nicaragua v. United*

---

67 **Tallinn Manual On The International Law Applicable To Cyber Warfare,** The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence (2013), p.25. Kılavuzdaki 'egemenlik' kavramı tanımlanırken, 1928'de La Hey'deki Uluslararası Daimi Hakem Mahkemesi (Permanent Court of Arbitration) tarafından verilen *Palmas Adaları Davası*'ndaki karar esas alınmıştır. Karara göre, devletler arasındaki egemenliğin anlamı bağımsızlıktır. Dünyanın belli bir bölgesi için bir bağımsızlık olgusundan bahsedilirken anlaşılması gereken, o bölgede, bir devletin başka bir devletin dahli olmadan hareket etme hakkıdır. **Island of Palmas (Netherlands v. United States of America)**, 2 R.I.A.A. 829, 838, Permenant Court of Arbitration (1928).

68 a.g.e.,p.25.

69 a.g.e.,p.47.

70 a.g.e.,p.45.

States of America davasında belirlediği 'ölçek ve etki' ölçütlerini esas almışlardır. UAD, söz konusu davaya ilişkin kararında, silahlı bir çatışmanın varlığından söz edebilmek için çatışmanın ölçeği ve etkilerine bakılması gerektiğini belirtmiştir[71]. Tallinn Kılavuzu, konuya bu açıdan bakıldığında, sadece psikolojik harekat veya siyasi ve ekonomik güvenin sarsılmasına yönelik siber harekatların bir saldırı olarak yorumlanamayacağını savunmaktadır[72].

Kılavuzun hazırlanmasında görev alan Schmitt, siber saldırının bir 'silahlı kuvvet' (armed force) kullanımı olarak kabul edilmesi için belirli ön şartların gerçekleşmiş olmasını gerekli görmüştür[73]. Buna göre, bir siber saldırının kuvvet kullanma sayılabilmesi için altı temel ölçüt esas alınmalıdır[74]. Birinci ölçüt saldırının 'şiddet derecesi'dir (severity). İnsanın ihtiyaçlar hiyerarşisinde fiziksel dirlik en önemli unsur olduğu için bu değere yöneltilecek bir saldırının şiddeti bir ölçüt olarak önem taşımaktadır[75]. İkinci

---

71 **Nicaragua v. United States of America**, 1986 I.C.J. 14, (1986), para. 195.

72 **Tallinn Manual**, p.48.

73 Schmitt bu ölçütleri aslında 11 Eylül'den çok önce, siber saldırı teknolojilerinin henüz bugünkü kadar gelişmediği erken bir tarihte belirlemiştir. Bu nedenle, bu ölçütler güncel teknolojik gelişmeleri yansıtmaktan uzaktır. Ancak Schmitt'in amacı, teknolojik gelişmelere göre hukuki bir eşik (threshold) belirlemek değil, siber saldırının kuvvet kullanma fiili kapsamında değerlendirilmesinde kulanılacak olan, teknolojik gelişmelerden bağımsız daimi ölçütler oluşturmaktır. Bir siber saldırının uluslararası hukuk açısından değerlendirilmesi için başvurulacak bu ölçütlerin teknolojik gelişmelere göre sürekli değişemeyeceği, bunların kalıcı ilkeler olmaları gerektiği aşikardır. Bu nedenle, Schmitt'in ilkeleri güncel teknolojik referanslar taşımasa da, kalıcı normlar teşkil ettikleri için bu makalede temel ölçüt olarak ele alınmıştır.

74 Schmitt bu ölçütleri tanımlarken, fiziksel kuvvet kullanmayı ekonomik ve siyasi yaptırımlarla mukayese etme yoluna gitmiştir. Böylece, fiziksel kuvvet kullanma ile diğer zorlama tedbirlerinin sonuçları arasındaki farklılıklara dikkat çekmiş ve kuvvet kullanmanın hangi şartlar altında gerçekleşmiş olabileceğini tespit etmeye yarayacak ölçütlere ulaşmaya çalışmıştır. Yazar, araştırmasında fiziksel kuvvet kullanmayı 'silahlı zorlama' (armed coercion) olarak tanımlamayı tercih etmiştir.

75 Michael N. **Schmitt**, **Computer Network Attack and The Use of Force in International Law: Thoughts on A Normative Framework**, Research

ölçüt saldırı ve sonuçların ortaya çıkması arasında geçen süreyi ifade eden 'yakınlık'tır (immediacy). Yazar burada, bir silahlı zorlama fiilinin olumsuz sonuçlarının son derece kısa bir zaman diliminde ortaya çıkacağı gerçeğinden hareket etmiştir[76]. Siber silahla gerçekleştirilen bir saldırının sonuçları, kullanılan teknolojinin doğası gereği, saldırıyla aynı anda kendini göstermelidir. Üçüncü ölçüt 'doğrudanlık'tır (directness). Schmitt'e göre, silahlı zorlama fiilinin sonuçları, *actus reus*'a (suçun varlığını fiziken ispatlayan unsura) çok sıkı bir şekilde bağlıdır[77]. Çalışmada ele alınan dördüncü ölçüt 'yayılabilirlik'tir (invasiveness). Buradaki temel varsayım, hedef alınan ülkeye karşı gerçekleştirilecek silahlı zorlamayı oluşturan hareketin bilfiil o ülke üzerinde vuku bulması gerektiğidir. Dolayısıyla böyle bir hareket, başka bir ülkenin sınırlarına yayılmadan hedef alınan ülkenin haklarına karşı bir tecavüz anlamına gelebilecektir[78]. Schmitt'in belirlediği beşinci ölçüt 'ölçülebilirlik'tir (measurability). Silahlı bir zorlamanın sonuçlarını ölçebilmek, diğer zorlayıcı yöntemlerin sonuçları hakkında bilgi sahibi olmaya oranla çok daha kolaydır[79]. Sonuncu ölçüt ise 'muhtemel meşruiyet'tir (presumptive legitimacy). Kuvvet kullanma, meşru müdafa dışında yasaklanmış bir fiil olduğundan, şiddet içeren bir fiilin kanunsuz ilan edileceği açıktır. Bu nedenle, silahlı bir zorlamanın sonuçları kendiliğinden hukuka aykırı olarak yorumlanacaktır[80]. Schmitt'in ilk iki ölçütü incelendiğinde, aslında bunların yukarıda daha önce değinilen unsurları içerdiği görülmektedir. Ancak sonraki ölçütler göreceli olarak daha özgündürler. Silahlı zorlama olarak tanımlanan fiziksel kuvvet kullanmanın hangi şartlara bağlı olarak vuku bulmuş olabileceğine bu ölçütleri kullanarak karar vermek yerinde görülmektedir.

Publication 1 Information Series, Institute for Information Technology Applications, USAF Academy, Colorado (June 1999), p.18.

76 a.g.e., p.18.

77 a.g.e., p.18.

78 a.g.e., p.19.

79 a.g.e., p.19.

80 a.g.e., p.19.

SONUÇ

Siber silah ve siber saldırı olguları, bilgisayar bilimlerindeki ilerleme ile elde edilen teknolojik avantajların kaçınılmaz sonucunu ifade etmektedir. Bilişim sektöründeki gelişmeler sayesinde, bilgisayarlar ve bilgisayar ağları ülkelerin kritik altyapılarını teşkil eden en önemli unsurlardan biri haline gelmişlerdir. Zararlı bilgisayar yazılımları ve programları, barış, kriz veya savaş zamanlarında devletler tarafından saldırı veya savunma amaçlarıyla bu altyapı unsurlarına karşı kullanılabilecek bir silaha dönüşmüşlerdir. Bu avantajı en kapsamlı şekilde kullanan devlet sahip olduğu sermaye ve teknoloji birikimi nedeniyle kuşkusuz ABD'dir. Stuxnet saldırısıyla ABD, politikasını etkilemek istediği devletler üzerinde siber silahları kullanmakta tereddüt etmeyeceğini açıkça göstermiştir. Her ne kadar söz konusu saldırıda bir rolü olduğunu itiraf etmemişse de, saldırıyı ve virüsü inceleyen bilişim uzmanları tarafından failin ABD olduğuna kesin gözüyle bakılmaktadır.

Bu çalışmada, ABD'nin siber silahlarla ilgili resmi devlet politikasının saldırı değil savunma odaklı olduğu, ancak yönetim erki tarafından yayınlanan konuyla ilgili yönergede, siber silahlara saldırı amacıyla da başvurulabileceğinin açıklandığı görülmüştür. Bu gerçek, siber saldırı fiilinin uluslararası hukuk açısından incelenmesini zaruri kılmaktadır. Literatürde siber saldırının kuvvet kullanımı olarak kabul edilmesi gerektiğine yönelik bir fikir birliği oluştuğu görülmüştür. Ancak siber saldırının bir kuvvet kullanımı sayılabilmesi için belirli koşulların yerine gelmesi gerekmektedir. Siber saldırı sonucunda meydana gelen etki, saldırının bir kuvvet kullanımı olarak yorumlanması için temel ölçüt olarak kabul edilmektedir. Bir siber saldırının mağdur devlet üzerinde yarattığı etkinin, fiziksel bir kuvvet kullanımı sonucunda oluşabilecek etkiye eşit olması durumunda, söz konusu mağdur devlet saldırgan devlete karşı kuvvet kullanabilecektir. Bu kuvvet kullanımı, mağdur devlet tarafından, BM Sözleşmesi'nin 51. maddesi ile düzenlenmiş meşru müdafa hakkı çerçevesinde uygulanabileceği gibi, Sözleşme'nin VII. Bölümü'nde tanımlanan bir Güvenlik Konseyi kararıyla da uygulanabilecektir.

Siber silahlar ve siber saldırı, henüz tanımları, kapsamları ve sınırları kesin olarak belirlenmiş kavramlar değildir. Siber saldırı fiillerini düzen-

leyen, devletlerin siber alandaki haklarını ve sorumluluklarını kesin olarak belirleyen ve böyle bir saldırı karşısında uygulanabilecek yaptırımları ortaya koyan çok taraflı bir uluslararası antlaşma mevcut değildir. Tallinn Kılavuzu, siber saldırı alanında oluşturulmuş en kapsamlı düzenlemelerden biri olmakla beraber, herhangi bir bağlayıcılığının bulunmaması bu alanda daha çok çaba sarfedilmesini gerekli kılmaktadır. Siber saldırı, Stuxnet saldırısında görüldüğü gibi, ciddi sonuçlar doğurabilecek bir fiildir. Söz konusu saldırıda can kaybının yaşanmamış olması, gelecekte meydana gelebilecek saldırılarda bu tip kayıpların yaşanmayacağı şeklinde yorumlanmamalıdır. Siber saldırı ve siber silahların kuvvet kullanmaktan kaçınma ilkesi çerçevesinde, aynı konvansiyonel ve nükleer silahlar gibi, başvurulacak son yol (last resort) olarak kabul edilmesi ve sadece meşru müdafa amacıyla kullanılması ancak kapsamlı bir uluslararası antlaşma sayesinde mümkün olabilecektir. Konuyla ilgili hak, sorumluluk ve güvencelerin kesin bir dille ortaya koyulduğu hukuki düzenlemelerin hazırlanması için zaman kaybetmeden çalışmaya başlanmasında fayda olduğu muhakkaktır. Bu süreçte devlet kurumları, akademik çevreler, sivil toplum kuruluşları ve sorumlu bireylere düşen de, kamu güvenliği açısından konuyu ulusal ve uluslararası topluluk gündeminde tutmaya devam etmektir.

Kaynakça

Makaleler

Anderson, Kenneth, "United Nations Collective Security and the United States Security Guarantee in an Age of Rising Multipolarity: The Security Council as the Talking Shop of the Nations", **Chicago Journal of International Law**, Vol.10, No.1 (2009).

Chen,Thomas, M. **Stuxnet, The Real Start of Cyber Warfare?,** IEEE Network (November/December 2010).

Collins, Sean **McCombie**, Stephen, "Stuxnet: The Emergence of a New Cyber Weapon And Its Implications" **Journal of Policing, Intelligence and Counter Terrorism**, Vol.7, No.1 (April 2012).

Farwell, James, **Rohozinski**, P. Rafal, "Stuxnet and The Future of Cyber War", **Survival** Vol.53, No.1 (February-March 2011).

Gervais, Michael, "Cyber Attacks and the Laws of War", **Berkeley Journal of International Law,** Vol.30, Issue 2 (2012).

Gürkaynak, Muharrem, **İren**, Adem Ali, "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, C.16, S.2 (2011).

Hoisington, Matthew, "Cyberwarfare and The Use of Force Giving Rise to The Right of Self-Defense", **Boston College International & Comparative Law Review**, Vol. 32 (2009).

Inbar, Efraim "The "No Choice War" Debate in Israel", **Journal of Strategic Studies**, March (1989).

Jenkins, Ryan, "Is Stuxnet Physical? Does It matter?" **Journal of Military Ethics**, Vol.12, No.1 (2013).

Langner, Ralph "Stuxnet: Dissecting a Cyberwarfare Weapon", **Journal IEEE Security and Privacy**, Vol.9, Issue3 (May/June 2011).

Lin, Herbert S., "Cyber Conflict and İnternational Humanitarian Law", **International Review of the Red Cross,** Vol.94, No.886 (Summer 2012).

Lin, Herbert S., "Offensive Cyber Operations and the Use of Force", **Journal of National Security Law & Policy**, Vol.4, No.63 (2010).

Lin, Herbert S., "Offensive Cyber Operations and the Use of Force", **Journal of National Security Law & Policy,** Vol.4. No.63 (2010).

Lynn III., William J., "Defending a New Domain: The Pentagon's Cyberstrategy", **Foreign Affairs** Vol.89, No.5 (2010).

Mcgraw, Gary "Cyber War is Inevitable (Unless We Build Security In)" **The Journal of Strategic Studies**, Vol.36, No.1 (2013).

Ophardt, Jonathan A., "Cyber Warfare and the Crime Of Aggression: The Need For Individual Accountability on Tomorrow's Battlefield", **Duke Law & Technology Review** Vol.9, No.3 (2010).

Peterson, Dale "Offensive Cyber Weapons: Construction, Development, and Employment", **The Journal of Strategic Studies**, Vol.36, No.1, (2013).

Remus, Titiriga, "Cyber Attacks and International Law of Armed Conflicts; A "Jus Ad Bellum" Perspective", **Journal of International Commercial Law and Technology**, Vol.8, No.3 (July, 2013).

Todd, Graham H. "Armed Attack in Cyberspace: Deterring Asymmetric Warfare With an Asymmetric Definition", Vol.64, Cyber Law Edition, **The Air Force Law Review,** (2009).

Türkay Şeyda, "Siber Savaş Hukuku ve Uygulanma Sorunsalı", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,** C. LXXI, S. 1, s.1177-1228, (2013).

Kitaplar

Brownlie, Ian, **International Law and The Use of Force by States,** Oxford University Press, Oxford, 1963.

de Wet, Erika, **Vidmar**, Jure, eds., **Hierarchy in International Law: The Place of Human Rights**, Antonios **Tzanakopoulos**, "Collective Security and Human Rights", Oxford University Press, Oxford, 2012.

Dinstein, Yoram, **War, Aggression and Self-Defence,** Cambridge University Press, 4th ed., Cambridge, 2005.

Garesi, Seven Bernhard, **Varwick**, Johannes, **The United Nations, An Introduction**, Palgrave MacMillan, New York, 2005.

Jennings, Robert, **Watts,** Arthur, (eds.), **Oppenheim's International Law**, Ninth Edition, Oxford University Press, Oxford, 1991.

López-Jacoiste, Eugenia, **The UN Collective Security System and its Relationship with Economic Sanctions and Human Rights**, **Max Planck Yearbook of United Nations Law** (Armin von **Bogdandy**, Rüdiger **Wolfrum,** eds.).

Middlemas, Keith, **Barnes**, John, **Baldwin: A Biography**, Littlehampton Book Services Ltd., Worthing, 1969.

Operational Law Handbook, International & Operational Law Depertmant, The Judge Advocate General's Legal Center, U.S. Army, Charlotsville, 2007.

Owens, William A. **Dam**, Kenneth, **Lin**, W. Herbert, (ed.), **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities**, Committee on Offensive Information Warfare, National Research Council, The National Academies Press, Washington, DC (2009).

Taşdemir, Fatma, **Uluslararası Terörizme Karşı Devletlerin Kuvvete Başvurma Yetkisi**, USAK, Ankara, 2006.

Raporlar/Tezler

Albright, David, **Brannan**, Paul, **Walrond**, Christina, **Stuxnet Malware and Natanz: Update of ISIS Report** (December 22, 2010) Applications, USAF Academy, Colorado (June 1999).

Ashmore, William, C. **Impact of Alleged Russian Cyber Attacks,** School of Advanced Military Studies, Fort Leavenworth. (2009).

Cheek, Gary H., **Effects-Based Operations: The End of Dominant Maneuver?** Carlisle Barracks, U.S. Army War College, (April 2002).

Chen, Thomas M., **Stuxnet, The Real Start of Cyber Warfare?,** IEEE Network (November/December 2010).

Clapper, James R., **Statement for The Record Worldwide Threat Assessment Of The US Intelligence Community,** Senate Select Committee On Intelligence (2013).

Deptula, David A., **Effects-Based Operations: Change in the Nature of Warfare,** Aerospace Education Foundation, Arlington (2001).

Falliere, Nicolas, **Murchu**, Liam O., **Chien**, Eric, **W32.Stuxnet Dossier** Symantec Security Response, Symantec (February 2011).

Langner, Ralph, **To Kill a Centrifuge A Technical Analysis of What Stuxnet's Creators Tried to Achieve**, The Langner Group, (November 2013).

Mann III, Edward C., **Endersby**, Gaiy, **Searle**, Thomas R., **Thinking Effects: Effects-Based Methodology for Joint Operations**, Air University, College of Aerospace Doctrine, Research and Education Paper, No.15 (October 2002).

Mele, Stefano, **Cyber-Weapons: Legal and Strategic Aspects**, Italian Institute of Strategic Studies "Niccolò Machiavelli", Rome, (June 2013).

Mueller, Karl P., **Castillo,** Jasen J, **Morgan**, Forrest E., **Pegahi**, Negeen, **Rosen**, Brian, **Striking First: Preemptive and Preventive Attack in U.S. National Security Policy**, RAND Corporation (2006).

Schmitt, Michael N., **Computer Network Attack and The Use of Force in International Law: Thoughts on A Normative Framework**, Research Publication 1 Information Series, Institute for Information Technology.

Sharp, **Sr.**, Walter Gary, **Cyberspace and The Use of Force,** Ageis Research Corp, Falls Church (1999).

Sinopoli, Anthony, F. **Cyberwar and International Law: An English School Perspective,** Yüksek Lisans Tezi, Government and International Affairs, University of South Florida (2012).

Smith, Edward A., **Effects-Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War**, Office of the Assistant Secretary of Defense, Command & Control Research Program, CCRP, Washington, DC (2006).

Talmon, Stefan, **A Universal System of Collective Security Based on the Charter of the United Nations: A Commentary on Article 2(6) UN Charter**, Bonn Research Papers on Public International Law Paper, No.1, Institute of Public International Law, University of Bonn (20 November 2011).

United States General Accounting Office, **Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems**, (March 2004).

Wagenhals, Lee W., **Levis**, Alexander H., **McCrabb**, Maris "Buster", **Effects-Based Operations; A Historical Perspective for a Way Ahead**, George Mason University, System Architectures Laboratory, C3I Center, Fairfax, (2003).

Bildiriler/Çalışma Kağıtları

Iasiello, Emilio, **Cyber Attack: A Dull Tool to Shape Foreign Policy,** 5th International Conference on Cyber Conflict. (2013).

Kara, Mehmet, **Çelikkol**, Soner, **4. Ağ ve Bilgi Güvenliği Sempozyumu Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği**, Atılım Üniversitesi, 25-26 Kasım 2011.

Karnouskos, Stamatis, **Stuxnet Worm Impact on Industrial Cyber-Physical System Security**, IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society, (2011).

Sheng, Su, **Yingkun**,Wang, **Yuy**i, Long, **Yong**, Li, **Yu**, Jiang, **Cyber Attack Impact on Power System Blackout**, IET Conference on

Reliability of Transmission and Distribution Networks, (22-24 Nov.2011).

Uluslararası Antlaşmalar, Uluslararası Mahkeme Kararları ve Uluslararası Kılavuzlar

BM Sözleşmesi

Briand-Kellogg Paktı

Island of Palmas (Netherlands v. United States of America), 2 R.I.A.A. 829, 838, Permenant Court of Arbitration

Nicaragua v. United States of America, 1986 I.C.J. 14

Tallinn Manual On The International Law Applicable To Cyber Warfare

Viyana Andlaşmalar Hukuku Sözleşmesi

Devlet Belgeleri

Presidential Policy Directive/PPD-20, (2012)

Cyberspace Policy Review, (2009)

Strategy for Operating in Cyberspace, (2011)

The National Strategy to Secure Cyberspace, (February 2003)

Comprehensive National Cybersecurity Initiative, (January 2008)

Elektronik Kaynaklar

http://avalon.law.yale.edu/20th_century/kbpact.asp

http://avalon.law.yale.edu/20th_century/leagcov.asp

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.259.7495

http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6109934.

http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888

http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/

http://www.admiraltylawguide.com/conven/lawoftreaties1969.html

http://www.bbc.co.uk/news/world-middle-east-11414483

http://www.symantec.com/connect/blogs/stuxnet-breakthrough

http://www.tandfonline.com/doi/abs/10.1080/13567888.2011.575612#preview

http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/

http://www.wired.com/threatlevel/2011/07/stuxnet-timeline/

http://www.youtube.com/watch?v=_9Gt2Ek4inM.

https://www.un.org/en/documents/charter/chapter1.shtml

https://www.un.org/en/documents/charter/chapter7.shtml