SİBER SAVAŞ HUKUKU VE UYGULANMA SORUNSALI

Araş. Gör. Şeyda Türkay

GİRİŞ

Günümüzde, gelişen teknolojiye bağlı olarak ortaya çıkan küreselleşmenin etkisiyle, devletlerin geleneksel yapılarında ve birbirleriyle olan her türlü ilişkilerinde değişiklikler meydana gelmektedir. Bu değişimler barış zamanında ekonomi, kültürel iletişim, eğitim, ticaret gibi pek çok konuda olmakla beraber, devletlerin ya da aktörlerin, çatışma veya savaş durumlarında da meydana gelmektedir. 21. yüzyılda, gelişen teknoloji ve bilişim sistemleri, geleneksel savaş yöntemlerini de değiştirmiş, ortaya, siber dünyada gerçekleşen yeni savaş ya da saldırı kavramları çıkmıştır. Ağlar üzerinden bilgi edinme, saldırı, zarar verme, yok etme, kontrol etme gibi yöntemlerle hedeflere savaş açılmış ya da saldırıda bulunulmuştur. Teknolojinin oldukça yaygın, ulaşılması kolay ve ucuz olması sebepleriyle bu tip saldırılar sadece devletler tarafından değil, bizzat şahıslar tarafından yapılabilmekte; bu da bu suçların tespitini ve cezalandırılmasını zorlaştırmaktadır. Bu tip saldırıların, devlet desteği ile düşman bir aktör ya da devlete karşı işlenmesi durumu ise güncel olarak son derece ciddi ve hukuki bir zeminle çözülmesi gereken bir sorundur. Geleneksel savaşlarda olduğu gibi saldıranın aşikâr olmaması, çok farklı bölgelerden kaynaklanması, tespitinin ve kanıtlanmasının zor olması, bu suçların tanımını ve yaptırımının sağlanmasını zorlaştırmaktadır. 2007 yılında Estonya ve 2008 yılında Gürcistan'a karşı yapılan servis saldırılarının reddi (DoS), bu yeni savaş şeklinin operasyonel olduğunu ve ayrıca uluslararası hukukun siber savaş ile daha iyi bir anlayışın geliştirilmesi ihtiyacını kuvvetli bir şekilde göstermektedir. Mevcut uluslararası hukuk kurallarında geçen; saldırı, silah ve toprak gibi kavramlar siber saldırı ve savaşları açıklamaya yetmemektedir.

Coğrafyacıların stratejik gerçeklikleri, gelecekteki siber çatışmalar bağlamındaki kararların, soyut bir şekilde tam bir izolasyon ve uluslararası kamu hukukunun hükümlerinin yorumlanmayacağını ve uygulanmayacağını dikte etmekte, siberuzayı da içeren çözümlenmemiş Jus ad bellum ve Jus in bello konuları birçok önemli kaygıya yol açmaktadır.[1] Jus ad bellum kavramı genel olarak savaş yapma hakkıdır ve devletlerin güç kullanıp kullanamayacağı meselesini ortaya koyan kavramdır ve jus in bello'nun uygulanması çatışmanın başlamasına bağlıdır.[2] Jus ad bellum'un kaynağı çok daha yenidir ve B.M. Şartı'nın m. 2/4'ünde zikredilen kuvvet kullanma yasağına, söz konusu yasağın istisnası olan m.51'de ifade edilen meşru müdafaa hakkına ve B.M. Şartı'nın yedinci bölümüne dayanmaktadır.[3] Belirli eylemlerin silahlı saldırı mı veya güç kullanımı mı oluşturduğuna, nihai olarak karar veren mağdur devlet değil, asıl saldırgan devlet olacaktır; diğer bir deyişle, mağdur devletin hukuki yorumu, bu gibi eylemleri saygı duyulan hukuki sistemler ve askeri düzenle-

---

1 Sean Kanuck, **Sovereign Discourse on Cyber Conflict Under Intemational Law**, Texas Law Review Association, Symposium: Law at the Intersection of National Security, Privacy and Technology: II. Cybersecurity and Network Operations, Vol. 88:1571, 2010, s.1595.

2 Ayşe Nur Tütüncü, **İnsancıl Hukuka Giriş**, Beta Yay., İstanbul, 2006, s.12.

3 TÜTÜNCÜ, s.13.

meleri değerlendiren otoriteler, herhangi bir karşıt hukuk danışmanı yönlendirecektir.[4]

Çalışmamızda; siber savaş, siber uzay, siber terörizm tanımı yapılacak, siber savaş operasyonlarının öncesi ve uluslararası hukuk bağlamında gelişimine değinilecek, siber savaş operasyon silahlarından söz edilecek, saldırılarda sivil-asker ayrımının önemine ve egemenlik söylemine değinilerek, barışı korumak adına siber savaşa başvurulmasından ve siber savaş ile casusluk ilişkisinden söz edilecektir.

1. KAVRAMLAR

1.1. Siberuzay

"Siberuzay" ın uluslararası kabul görmüş bir tanımı olmamakla birlikte, çok sayıda tanımı mevcuttur. Etimolojik açıdan siber ve uzay kelimelerinin bir araya gelmesiyle oluşmakta, yalın olarak siber kelimesi sözlüklerde bulunmamaktadır.[5] Sibernetik; "güdümbilimi, kübernetik", teknolojik, biyolojik, sosyolojik ve ekonomik sistemlerde kumanda uç iletişim süreçlerini incelemeye dayanan bir amaca doğru yönlendirilmiş etki bilimi olarak tanımlandığı görülmektedir.[6] Çoğunlukla İnternet'i ifade etmek için kullanılan siberuzay; çok sayıda, hızla genişleyen, her biri farklı bir sayısal etkileşim ve iletişim yöntemi sağlayan siber uzayların birleşiminden meydana gelmektedir.[7] ABD Savunma Bakanlığı "siberuzay"ı "internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemci ve denetleyicileri de içeren, bilgi teknolojisi altyapılarının bağımsız ağlarından oluşan küresel etki alanı" olarak tanımlamaktadır. 2001 Kongre Araştırma Servisi, Kongre Raporu'na göre "siberuzay": "İnsanların, bilgisayarlar ve telekomünikasyon aracılığıyla fiziksel coğrafya dikkate alınmadan tümden birbirine bağlı olması" anlamına gelmektedir. Siberuzayın birden çok anlamının olması, devletler arasında uluslararası hukukun siber uzayda yönetilen savaşlara nasıl uygulanacağını gösterecek ortak bir antlaşmanın oluşturulmasının zorluğunu göstermektedir.[8] Thomas Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, kitabında daha sade bir dille şu şekilde tanımlamaktadır: "Siber uzay fiziksel bir yer değildir. Fiziksel boyut ya da uzay-zaman süreklilik ölçümlerine karşı koyar. Bilgisayar ağları, bilişim sistemleri ve telekomünikasyon altyapılarının işbirliği birleşiminin yarattığı çevrenin genel olarak *World Wide Web* olarak bilindiği bir kısaltmadır."[9]

Uluslararası Kamu Hukuku, farklı hukuk sistemlerinin kendine özgü unsurları da içeren bir amalgam temsil etmekte, Uluslararası Adalet Divanı Statüsü (UAD) ise uluslararası hukukun uygun kaynaklarını, verdiği kararlarla listelemekte, Uluslararası Hukuk Komisyonu Statüsü (UHK) de Uluslararası Teamül Hukukuna kaynak konusunda bir başka rehber olmaktadır.[10] Bu Statünün 19. madde "Bu bölüm, diğer maddelerin düzenlemeleri ışığında, haksız fiili işleyen devletin ya da herhangi bir başka devletin uluslararası sorum-

---

4 KANUCK, s.1596.

5 Toygar Akman, **Sibernetik: Dünü, Bugünü, Yarını**, Kaknüs Yay., İstanbul, 2003, s. 21.

6 **Türkçe Sözlük**, Türk Dil Kurumu, 9. Baskı, Ankara, 1998, s.1978.

7 Martin Dodge ve Rob Kitchin, **Mapping Cyberspace**, Routledge, London, 2001, s.1.

8 Steven A. Hildreth, **Cyberfare Warfare 11**, Congressional Research Service Report For Congress No. RL30735, 19 Haziran 2001, s.1, http://www.fas.org/irp/crs/RL30735.pdf, (e.t.28.01.2012).

9 Arie J. Schaap, **Cyber Warfare Operations: Development and Use Under International Law**, Air Force Law Review, Vol. 64, 2009, s. 125.

10 KANUCK, s.1584.

luluğunu oratdan kaldırmaz"[11] hükmü ilgili konu ile alakalı yasa metinleri, kararnameler, yargı kararları, andlaşmalar, diplomatik yazışmalar ve diğer belgeler sağlanmasına götürmektedir.[12] Bu belgelerden bazılarına ilerleyen konularda değinilmiştir. UAD ve UHK Statülerinin ikisi de Uluslararası Teamül Hukukunun devlet uygulamalarının meşru ve yol gösterici bir kaynak olduğunu açıkça belirtmektedir. Siberuzay bağlamında; tarihsel örneklerin yokluğundan, hukuki görüş veren hükümet yetkililerinin yeni uluslararası normlar oluşturmasından, ulusal güvenlik politikalarının deklare edilmesinden, askeri doktrinler formüle edilmesinden, angajman kurallarının kurulmasından ve devlet uygulamalarına aksi kanıt sağlanmasından hiçbir şey daha kritik olmamaktadır.[13] Siber çatışma yoluyla ulusal avantaj arayan devlet aktörleri, andlaşma mekanizmalarını reddederek çok taraflı zorlamalara karşı koyma fırsatına sahiptir; tersine çok taraflı çabalar, uluslararası hukuk toplumunca neyin kabul edileceğinin çerçevesini çizmek amacıyla bazı siber uzaydaki davranış normlarını kurmak için hizmet verebilir. Belki de gelecekte uluslararası siber silah kontrol aracı olacaktır, fakat çok yakın bir zamanda bu durum muhtemel görünmemekte, o zamana kadar, bu konu hakkında devlet uygulaması, uluslararası teamül hukukunun birincil kaynağı olmaya devam edecektir.[14]

1.2. Siber Savaş

Siberuzay gibi siber savaş kavramının da genel kabul görmüş bir anlamı bulunmamaktadır. Askeri sistemlerin ve orduların teknolojiye ve bilişim sistemlerine olan bağımlılığı giderek artmaktadır. Günümüzde birçok silah, hedef tespit, komuta kontrol ve haberleşme sistemleri bilgisayarlara ve yazılımlara bağlı olarak çalışmaktadır.[15]

ABD Savunma Bakanlığı "siber operasyonları" birincil amaç askeri hedefler ya da etkileri ya da siber kapasitenin istihdamı olarak tanımlamakta ve "bilgisayar ağı saldırıları" terimi olarak da kullandığı görülmektedir.[16] Savunma Bakanlığı bilgisayar ağı saldırılarını: "Bilgisayar ve bilgisayar ağlarındaki var olan bilginin, bilgisayar ağlarının kullanımı yoluyla bozulması, engellenmesi, geriletilmesi ya da yok edilmesi" şeklinde tanımlamaktadır.[17] Hava Kuvvetleri Politika Direktifi 10–7, "ağ savaşı operasyonları" (*network warfare operations*) terimini tanımlamak için bu tanımdan yaralanmaktadır. "Ağların aracılığı bağ-

---

[11] Report of the International Law Commission on the work of its fifty-third session, DOCUMENT A/56/10, (23 April–1 June and 2 July–10 August 2001), s.70, http://untreaty.un.org/ilc/reports/2001/2001report.htm, (e.t.14.02.2012).

[12] **Statute of the International Law Commission**, 1947, http://untreaty.un.org/ilc/texts/instruments/english/stat ute/statute_ e.pdf, (e.t.07.02.2012).

[13] KANUCK, s.1585.

[14] KANUCK, s.1585. Modern internet alanına bakıldığında, bilgisayarlarla; sivil ve askeri iletişim, güç sistemleri, arıtma sistemleri, sağlık kuruluşu altyapılarının çoğu kontrol edilmektedir. ABD'de ordu iki milyondan fazla bilgisayar kullanmakta ve on bin yerel ağ alanına ulaşmaktadır. Ayrıntılı bili için bkz. Jeffrey T.G. Kelsey, Hacking into International Humanitarian Law: The Principles of Disdinction and Neutrality in the Age of Cyber Warfare, Michigan Law Review, Vol. 106 No:7, 2008, s.1432.

[15] Ordu birimleri arasında her türlü bilgi alışverişi intranet adı verilen İnternet'ten bağımsız bilgisayar ağları aracılığıyla gerçekleştirilmektedir. Bu durum askeri sistemleri ve ülke savunmalarını siber saldırılara karşı hassas hale getirmektedir.

[16] Department of Defense Dictionary of Military and Associated Terms Joint Publication 1–02, s.86, http://www. dtic.mil/do ctrine/new_pubs/jp1_02.pdf, (e.t. 28.01.2012).

[17] Department of Defense, **Dictionary of Military and Associated Terms Joint Publication 1–02**, (JP 3–13), s. 67, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, (e.t. 28.01.2012).

lamında, ağ tabanlı kapasitenin yok edilmesi, kesilmesi, bozulması, zorla ele geçirilmesi" ifadesi bir başka tanım olarak karşımıza çıkmaktadır.[18]

2001 CRS Kongre Raporu'nda siber savaş; düşmanın aynı eylemi yapabilme yeteneğini inkâr ederek, siberuzaydaki bilgi ve bilgisayar ağlarına saldırının veya ağları savunmanın çok çeşitli unsurlarını ifade etmek için kullanılmaktadır.[19] Technolytics Enstitüsü Kıdemli Üyesi ve Strateji Yönetim Danışmanı Kevin Coleman "siber savaşı": "Ekonomik zarar verme ya da savunmayı bozma mekanizması olarak düşmanı, yasadışı işlemleri kullanan ya da iletişim ve altyapıların diğer parçalarını, bilgisayar ve ağlara saldırarak bozma çabasında olan bir saldırı" şeklinde tanımlamaktadır.[20] Bu çeşitli tanımlar yine siber savaşın ne anlama geldiğinin tanımlanmasındaki zorlukları göstermektedir.[21]

Doktrindeki farklı tanımlardan bir diğeri de şu şekildedir: "Politik ve askeri hedefleri desteklemek için barış, kriz ve savaş dönemlerinde hasımın sahip olduğu bilgi altyapısı, sistem ve süreçlerinin işlevselliğini engellemek, imha etmek, bozmak ve kendi çıkarlarımız için kullanmak amacıyla yapılan hareketlerle; düşmanın bu faaliyetimize karşı önlem almasını engelleyecek ve benzeri harekâtına karşı koyacak tedbirler ve süreçlerin tamamıdır".[22]

Günümüzde, dünyanın herhangi bir yerindeki teknik bilgiye sahip bir birey, yabancı hükümetlerin internet kaynaklarına karşı suç işlemeye karar verebilmektedir, fakat "Siber Savaş" gerçekten büyük bir tehdit midir? Mayıs 2009 sonlarında, ABD Başkanı Barack Obama'nın, kendi yönetiminde Amerika'nın siber güvenliği ve dijital varlıklarını korumaya yönelik yeni bir makam oluşturulmasına odaklandığı şeklindeki açıklaması, ulusal güvenlik kurumlarının bir dizi raporlamaları bu pozisyonda görevli devlet kişisine ulaştırılacağı ve Amerika Birleşik Devletleri'ni siber saldırılar, siber terörizm ve siber savaştan korunmasını sağlayacak şekilde geniş bir görevlendirme durumunun meydana gelmesi bu pozisyonun önemine vurgu yapmaktadır.[23] Bu devlet kademesinin gelişimi, ABD ve dünyada hükümetlerin dijital tehditlere karşı kendilerini korumak için almakta oldukları çeşitli adımlardan sadece bir tanesidir. Düşmanlar ve düşmanca hükümetlerin yanı sıra sadece kurumsal güvenlik aygıtlarını keşfetmekle ilgilenenleri de içeren devletin bünyesindeki tüm hükümet kuruluşları bu gibi çok çeşitli tehditler hakkında bilgiler bulmaya çalışmaktadır. Siber savaş tehdidi kesinlikle gerçek olmasına rağmen, herkesin aklındaki soru; medya, ordu ve bazı bilim adamları tarafından açıklandığı gibi

---

[18] **Air Force Policy Directive 10–7**, 6 Eylül 2006, s.20, http://www.survivalebooks.com/free%20manuals/2006 %20US %20Air%20Force%20INFORMATION%20 OPERATIONS% 2027p.pdf, (28.01.2012).

[19] Steven A. Hildreth, **Cyberfare Warfare 11**, Congressional Research Service Report For Congress No. RL30735, 19 Haziran 2001, s.1, http://www.fas.org/irp/crs/ RL30735.pdf, (e.t.28.01.2012).

[20] Kevin Coleman, **The Cyber Arms Race Has Begun**, 28 Ocak 2008, s.1–4, http://www.csoonline.com/article/ 216991/c oleman-the-cyber-arms-race-has-begun, (e.t. 28.01.2012).

[21] SCHAAP, s.126.

[22] Çalışma Grubu 4, **E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları**, Türkiye Bilişim Derneği, s.5

[23] The White House, **Remarks By The President On Securing Our Nation's Cyber Infrastructure**, Office of the Press Secretary, 29 Mayıs 2009, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our -nations-cyberinf rastructure, (e.t.29.01.2012).

büyük bir tehdit olup olmadığıdır. Ayrıca, böyle bir tehdit ile nasıl başa çıkılacağı hala ucu açık bir sorudur.[24]

Siber savaş kavramı üzerine; tarihten, önemli iki isimden ilki olan Clausewitz, Savaş Üzerine adlı kitabında savaşı: "Savaş, düşmanımızı istediğimizi yaptırmaya mecbur etmek için kullanılan güçtür"[25] şeklinde tanımlamıştır. Sun Tzu; en iyi savaş yolunun düşmanın dövüşmeden ele geçirildiği yol olduğunu belirtmiş, böylece siber savaşı bu iki askeri teoriyle bağdaştırdığımızda; siber savaş yoluyla amaçlanan güç yarışında galip olmak veya mağlup olana ya da hedefe kendi istediğini yaptırmanın yolunun geleneksel silahlı savaş yöntemleri yerine siber saldırılar yoluyla gerçekleştirilmesi durumuna yol gösterici oldukları görülmektedir.[26] Hemen hemen tüm gelişmiş ve bazı gelişmekte olan ülkelerde, insanların neredeyse tüm günlük ihtiyaçları bilgisayarlara ve siber varlıklara dayanmakta; gaz, elektrik, sağlık, ulaşım hizmetleri, banka imkânları hep siber varlıklar aracılığıyla, ağlar üzerinden çalışmaktadır. Bu teknolojik gelişmeler hayatı kolaylaştırdığı gibi, bu imkânları da tehlikeye açık hale getirmektedir.[27]

Günümüz dünyasında, devletler ve özel kuruluşlar tarafından sunulan hizmetlerin siber saldırılarla veya devlet ya da kurumlara açılabilecek siber savaş faaliyetleriyle tahrip edilmemesi gerekmektedir; çünkü siyasi aktör olarak kabul edilen hükümetler; insanların kontrol ve yönetimini; etkili hukuk gücünü kullanarak, güvenli ve demokratik bir ortam sağlayarak gerçekleştirmesi hükümetlerin varoluş sebebini oluşturmakta ve bu söylem devam ettirilmediğinde kendilerinin meşruiyet sebepleri de ortadan kaldıracak bir durum ortaya çıkarma tehlikesi ile karşı karşıya bırakmaktadır.[28]

1.3. Siber Savaş Faaliyetlerine Genel Bakış

En temel tanımı ile siber savaş özünde; dijital, teknolojik yollarla yürütülen bir savaş yöntemi anlamına gelmekle birlikte; savaşın kendisi olduğu gibi, siber savaş da altyapıyı devre dışı bırakma, istihbarat toplama ve propaganda dağıtımı kavramlarını içermektedir.[29] Amerika Birleşik Devletleri *hackerların* hükümet bilgisayarlarındaki gizli bilgilere ulaşmaya teşebbüs ettiği ya da bazı siber casusluk durumlarında başarılı olduğunu resmi olarak doğruladığı birkaç durumdan biri 1999 yılında, FBI tarafından, bir yıldan fazla bir süre boyunca Savunma Bakanlığı bilgisayarlarındaki bilgilere Rus *hackerlar* tarafından gizlice girildiğinden ettikleri şüpheyi "*Moonlight Maze*" (Ayışığı Labirenti) adlı soruş-

---

[24] Wojciech Gryc, **Cyber Warfare, Peace Magazine**, 2009, s.14.

[25] Carl von Clausewitz, **On War**, (editör ve çeviren: Michael Howard and Peter Paret), Princeton University Press, New Jersey, 1989, s.583 ve Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends", Strategic Analysis, 34:1, 2010, http://dx.doi.org/10.1080/09700160903354450, s.64.

[26] Sun Tzu'nun tanımına uygun olarak; siber savaşta, geleneksel savaş yöntemlerine kıyasla, fiziksel şiddet yöntemleri ve tahribat uygulanmamakta ya da saldırıların şiddetine bağlı olarak bunların dolaylı bir sonucu olarak fiziksel bir tahribat gerçekleşmemekte, asıl olarak hedef devletin sahip olduğu mahrem güce siber yolla ulaşılmak ve bu kaynaklar ele geçirilmek suretiyle hedef zor durumda bırakılarak yenilgiye mecbur bırakmaktır. Daha fazla bilgi için bkz. Sun Tzu, The Art of War, çeviren: Samuel B. Griffith, Oxford University Press, Oxford, 1963, s.77.

[27] SHARMA, s.65.

[28] SHARMA, s.66.

[29] GRYC, s.14.

turma ile doğrulamıştır.[30] 2003 sonları ve 2004 yılında meydana gelen Çinli *hackerların* suçlandığı kod adı "*Titan Rain*" (Titan Yağmuru) başka bir saldırı da ele alındığında, iki olayda ortak olan iki öğenin mevcudiyeti öncelikle, her iki *hackerın* da ABD hükümet bilgisayarlarından önemli bilgileri elde etmeyi başardığı şeklinde karşımıza çıkmaktadır.[31] İkinci olarak ise, her iki *hackerın* ya da *hacker* grubunun bulunmaya çalışılmadığı, yargılanmadığı hatta Rus veya Çinli olup olmadıklarının doğrulanamadığı şeklindedir.[32] Gerçek düşmanı bilmek, siber savaşın en büyük zorluklarından biridir ve dünyanın uzak bölgelerinden karmaşık yönlendirme sistemleri ve zarar verme amaçlı kullanılabilecek bilgisayarları kullanarak *hackerlar* çoğu zaman iz bırakmamakta ya da başkası gibi davranmaktadır.[33]

Pretty Good Privacy (PGP) ya da TOR gibi yazılım ürünleri ile ortalama ev kullanıcıları bile tarama şablonlarını anonimleştirebildiğinden ve kolluk kuvvetlerinin onları izleyebilmelerini oldukça zorlaştırabildiğinden, "*Google*" adlı arama motoru dahi kullanıcılarına gizliliği arttırılmış hizmet sunmaya başlamıştır. Bu tür bir anonimlik büyük bir karışıklığa yol açabilmektedir.[34] Kosova savaşı sırasında, Belgrad'taki Çin Büyükelçiliği yanlışlıkla NATO savaş uçakları tarafından bombalandığında birçok *hackerın* Amerikan web sitelerini hedef aldığı görülmüş, olayın başlangıcında Çin kökenli *hackerların* faaliyeti olduğu düşünülmüş, daha sonra saldırıların çoğunun basit bir şekilde Çin'deki bilgisayarlarca kontrol edilen Amerika Birleşik Devletleri'nin kendisi olduğu anlaşılmıştır.[35] Siber casusluk, infiltrasyon ve yoğun şekilde istihbarat toplama vakalarının en büyük projelerinden biri, 2009 yılının Mart ayında Toronto Üniversitesi'ndeki araştırmacılar tarafından "*GhostNet*" adlı proje ile 103 ülkede yüksek değerli siyasi bilgisayarlara virüs bulaştırarak, elçilik ve diğer devlet dairelerindeki bilgisayarlardan oluşan hedeflere *hackerlar* sahte komünikasyon göndermenin yanında e-posta, takvim kayıtları ve diğer özel datalara ulaşımını engellemiştir.[36] Yukarıda listelenen çoğu saldırının hükümet dışı kuruluşlar tarafından organize edilmesi, istihbarat ve hassas bilgilerin (örneğin çalıntı kredi kartı numaraları ya da çok gizli hükümet bilgileri) toplanması ve ikinci elden satışının aynı zamanda kazançlı bir iş olmasından dolayı bu tür saldırıla-

---

[30] Bob Drogin, **Russians seem to be Hacking ınto Pentagon Sensitive information taken-but nothing top secret**, Los Angeles Times, 7 Ekim Perşembe 1999, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/1999/10/0 7/MN58558.DTL, (e.t. 28.01.2012).

[31] M. E. Kabay, **Industrial Espionage, Part 8: China and Titan Rain, Network World**, 10 Kasım 2005, http: //www.networkworld.com/newsletters/ 2005/1107sec2.html?page=2), (e.t.28.01.2012).

[32] James A. Lewis, **Computer Espionage, Titan Rain and China,** Center for Strategic and International Studies - Technology and Public Policy Program, Aralık 2005, s.1–2, http://csis.org/files/media/csis/pubs/051214_china _titan_rain. pdf, (e.t. 28.01.2012).

[33] GRYC, s.14.

[34] Elinor Mills, **Google wants ability to 'combine' your user data**, CNET News, 25 Ocak 2012, http://www.z dnetasia.com /google-wants-ability-to-combine-your-user-data-62303592.htm, (e.t. 28.01.2012).

[35] Dorothy E. Denning, **Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy**, 1999, http://www.iwar.org.uk/cyberterror/resources/denning.htm, (e.t. 28.01.2012).

[36] Ron Deibert, Rafal Rohuzinski, **Tracking GhostNET: Investigating a Cyber Espionage Network**, Information Warfare Monitor, JR02–2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigat ing-a-Cyber-Espionage-Network, (e.t.28.01.2012).

rın giderek artan oranda gerçekleşmeye devam edeceğini kanıtlar niteliktedir. En çok endişe verici olan durum ise, bilgisayar ve web site hesaplarına ulaşmanın öğrenilmesinin oldukça kolay olmasıdır; örneğin, "çerezleri çalmak" (*stealing cookies*) veya bir arama motoruna "SQL Injection Saldırısı" göndermek bir web kullanıcısının web sitelere giriş bilgilerinin çalınması ya da onlara zarar verilmesi bu web formları kullanılarak mümkün olabilmektedir.[37]

1.4. Ciddi Bir Tehdit mi?

Siber riskleri azaltmak, ticari ve şahsi bir konu olduğu kadar küresel ve ülkesel bir güvenlik sorunudur.[38] Devlet destekli bilişim saldırılarına dair kanıtlar bulunmaktadır. Bilişim savaşı tehlikesi sadece siber saldırılarla değil, bazı durumlarda, jeopolitik, ekonomik ve askeri egemen güç olma mücadelesinde devletlerin stratejik bilgi alma amaçlarına da hizmet etmektedir.[39]Avrupa Konseyi, bilgisayar virüslerinin verdiği zararın tamiri amacıyla $12 milyar harcandığını beyan etmektedir.[40] İngiliz Endüstri Konfederasyonu üyeleri arasında yapılan bir anket sonucuna göre; 2000 yılında gerçekleşen en ciddi sibersuç saldırganlarının %44.8'i *hackerlardan*, %13.4'ü eski çalışanlardan, %12.8'i örgütlü suç gruplarından, %11.5'i mevcut çalışanlardan, %7.9'u müşterilerden, %5.8'i rekabetçilerden, %2.6'sı siyasal ve protesto gruplarından ve sadece %1.4'ü teröristlerden oluşmaktadır.[41]

---

[37] GRYC, s.14. Gerçekten de, SQL enjeksiyon saldırıları, Türk destekçiler tarafından İsrail Hükümeti'ni protesto etmek amaçlı Birleşmiş Milletlerin web sitesini tahrip etmek amacıyla kullanıldığı görülmekte ve bu tür benzer saldırıların ABD'deki devlet ve web sitelere sızmak ve zarar vermek amaçlı benzer saldırıların düzenlenmiş olduğuna dair kanıtları da kendi içinde barındırmaktadır. Bkz. Elinor Mills, Report: Turkish hackers breached U.S. Army servers, 29 Mayıs 2009, http://news.cnet.com/ 8301-1009_3-10252375-83.html, (e.t.28.01.2012).

[38] Richard Power ve Dario Forte, **"Ten years in the wilderness—a retrospective Part 2: Cyber Security = Na tional Security"**, Computer Fraud&Security: War&Peace in Cyberspace, Şubat 2006, s.16.

[39] Ekonomik İşbirliği ve Gelişim için kurulan bir örgütün raporunda; Çin'in bilgi ve iletişim teknolojileri alanındaki ihracatı, bir yıl öncesine göre %46'dan fazla artış göstererek 2004 yılında $180 milyara ulaştığı, ABD'nin ise %12 artış oranı ile $149 milyara ulaştığı yer almaktadır. Ayrıntılı bilgi için bkz. POWER and FORTE, s.18. FBI, siber suçluların En Zengin 500 Şirketin hemen hemen hepsine saldırıda bulunduğunu açıklamaktadır. Ayrıca bkz. Reducing On-line Credit Card Fraud, Web Developers Journal, http://www.webdevelopersjournal.com/arti cles/card_fra ud.html ve http://www.fbi.gov/publications/leb/2002/ju ne2002/june02leb.htm, (e.t.10.02.2012). Bu sebepledir ki, sibersuçlar ve siber terörizm FBI'ın üç numaralı önceliği durumundadır. Dan Verton, Lack of Incident Reporting Slows Cybercrime Fight, 31 Ekim 2002, http://computerworld.co m/securityto pics/security/cybercrime/ story/0, 10801, 75532, 00.html, (e.t.10.02.2012).

[40] Jon Swartz, **Crooks slither into Net's shady nooks and crannies; Crime explodes as legions of strong-arm thugs, sneaky thieves log on,** USA Today, 21 Ekim 2004, www.usatoday.com/printedition/money/200410 21/cybercrimecover.art. htm, (e.t.10.02.2012). Kredi kartları en ciddi örneği oluşturmaktadır; FBI'a göre, 1999-2003 yılları arasında bilgisayar güvenlik sistemleri üzerinden çalınan kredi kartı numarası sayısı 30 milyon olmakla birlikte, ortaya çıkardığı zarar $15 milyar olarak hesaplanmaktadır.[40] Bkz. KSHETRI, s.542. 2003 yılında ABD tüketicilerinin ve işletmelerinin dijital suçlar sebebiyle ortaya çıkan zararın $14 milyar olduğu açıklanmaktadır. Bkz. Swartz. Kredi kartları en ciddi örneği oluşturmaktadır; FBI'a göre, 1999–2003 yılları arasında bilgisayar güvenlik sistemleri üzerinden çalınan kredi kartı numarası sayısı 30 milyon olmakla birlikte, ortaya çıkardığı zarar $15 milyar olarak hesaplanmaktadır. Bkz. KSHETRI, s.542.

[41] KSHETRI, s.543.

Siber casusluk ve istihbarat toplama vakalarının oldukça yüksek orana sahip olduğu söylenmekle birlikte, asıl soruyu, gayretli bir grup *hackerın*; elektrik şebekesi, fiziksel altyapı, trafik ya da hastane sistemlerini çökertip çökertemeyeceği oluşturmakla birlikte, fiziksel altyapılara karşı düzenlenen siber saldırılar, siber savaşçıların cephaneliğinden, silah depolarından yoksundur.[42] IBM'in Internet Güvenlik Sistemi araştırmacıları, 2007 yılında -bir haftalık süre içinde- nükleer güç santrali kontrolünü kırıp ulaşmayı başararak, reaktör yazılımının tüm kontrolünü ele geçirerek, günümüzde bir nükleer felakete neden olmanın imkânsızlığının dışında, bu tür reaktörlerin kapatılmasının da oldukça kötü felaketlere sebebiyet verebileceğini ispatlamaktadır.[43] En yakın gerçek elektrik şebekesinin çökertilmesi ve hastane sistemlerinin bloke edilmesi durumu 2007 yılında Estonya'da elektronik bankacılık servislerinin devre dışı bırakılması ve hükümetsel ve haber medya web sitelerinin çökertilmesi ile gerçekleştiği görülmektedir.[44] Rus milliyetçilerinin suçlandığı, Gürcü web sitelerine karşı 2008 yılında Güney Osetya Savaşı sırasında benzer olayların yaşanması bir diğer örnek olarak karşımıza çıkmaktadır.[45]

Siber savaşlar uluslararası alan dışında ülkelerin içinde de bir tehdit unsuru haline gelebilir mi? Ya da hükümetlerin siber güçleri kendi insanları üzerinde kullanmasının sonuçları ne olabilir? Bu bizzat zorlama amaçlı güç kullanımı şeklinde olabileceği gibi, demokratik kurumların şeffaflığının zedelenmesi ile de şu şekilde olabilir; örneğin bugün pek çok ülkede seçimler siber altyapılar aracılığıyla yürütülmekte ve uygulamada çok ciddi hatalar yapıldığı kanıtlanmaktadır.[46] Temsili demokrasilerin en önemli unsurlarından biri olan bireyin oy kullanma hakkı siber güçlerin eline geçebilir mi? Teknolojinin hayatımızın her alanına girmesi bu gibi sorunları arttıracak gibi görünmektedir.

Web sitelerini çökertmek ya da zarar vermek kolay olmasa da bir devlette istikrarsızlığa neden olması veya sivil kayıplar meydana getirmesi muhtemel görünmemekte, siber savaşta en büyük sorunu, genellikle zamana karşı bir yarış olması oluşturmakta, ancak politik hedeflere karşı savaş açmak yerine, finansal bilgi çalmak ya da bilgisayarlar aracılığıyla istenmeyen e-postalar göndermek sık sık alt grupların tercih ettiği yöntemi de oluşturmaktadır.[47] Siber tehditlere karşı verilen güncel cevaplara yöneltilen eleştirilerden biri devlet kurumlarının genellikle yetki alanından emin olmaması, potansiyel cevapların meşruluğu ya da kendilerini ne çeşit araçlar kullanarak koruyacakları şeklinde olmakla birlikte, bu durum görünüşte basit sorunları daha da kötüleştirmektedir: elektronik oy makinelerinin son derece güvenilmez olduğuna dair kanıtların olması, ilgili Zen'lerin kullanımıyla birçok hükümet websitelerine virüs bu-

---

[42] GRYC, s.15.

[43] Andy Greenberg, **America's Hackable Backbone**, 08.22.07, http://www.forbes.com/2007/08/22/scada-hacker s-infrastruc ture-tech-security-cx_ag_0822hack.html, (e.t. 28.01.2012) ve **A Strategic Approach to Protecting SCADA and Process Control Systems**, IBM Global Services, Temmuz 2007, s.1–13, http://www935.ibm.com/services/us/iss/pdf/scada_ whitepaper.pdf, (e.t.28.01.2012).

[44] Ian Traynor, **Russia accused of unleashing cyberwar to disable Estonia**, The Guardian, http://www.guardian.co.uk/worl d/2007/may/17/topstories3.russia, (e.t. 28.01.2012) ve Joshua Davis, Hackers take Down the Most Wired Country in Europe, Wired Magazine: Issue 15.09, http://www.wired.com/politics/security/magazine/1509 /ff_estonia?currentPage=all, (e.t.28.01.2012) ve http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_att acks_2007_latest.pdf, (e.t. 28.01.2012).

[45] GRYC, s.15.

[46] POWER ve FORTE, s.19.

[47] GRYC, s.15.

laştırmak örnek olarak verilebilir ve böyle bir teknoloji ile zarar verici eylemler yapılabilir fakat sağlayacağı olumlu yanlar da görmezden gelinmeden, uygun bir hükümet politikası ve işbirliği ile ikincisi çok daha başarılı olabilir.[48]

2. SİBER SAVAŞ OPERASYONLARININ GELİŞİMİ

Bazı devletler, siber savaşı yeni bir askeri doktrinin parçası olarak kullanmaya başlamıştır.

2.1. ABD'deki Gelişim

Siber savaş operasyonlarının planlaması, yarım yüzyılı aşkın süre önce atom bombasının icadına rastlayan ve ardından bir bomba yerine nasıl nükleer savaş başlatılır fikri ile ortaya çıkmıştır.[49] Bir siber savaş stratejisi geliştirmenin ilk adımı 2002 yılında ABD Başkanın, siber savaşın silah olarak kullanılması angajman kuralları ulusal politika çağrısında bulunmak üzere Ulusal Güvenlik Başkanlık Direktifi 16'yı imzalaması ile atılmıştır.[50] Bu direktif "Hükümet, düşmanlara karşı siber saldırılar hazırlamak için yol gösterici ABD politikaları hazırlar" talimatını içermektedir.[51] 2003 Şubat'ında, Beyaz Saray, hükümete "Siber saldırılara ABD ulusal güvenlik topluluğunca karşılık verme koordinasyonunun geliştirilmesi" çağrısı olarak, siber güvenliği Ulusal Güvenliğin alt kümesi olarak sunan Güvenli Siberuzay Ulusal Strateji 'sini yayımlamıştır.[52] Aynı zamanda 2003 yılında Savunma Bakanlığı Bilişim Operasyonları Yol Haritasında Savunma Sekreteri'nin "Yol haritası, askeri kapasitenin hızla gelişen bilişim teknolojilerinin sağladığı yeni fırsatları kullanarak yeni ortaya çıkan tehditlere ayak uydurması yönünde değiştirilmesi, bakanlığın taahhüdünün başka bir örneğidir" şeklinde açıklaması mevcuttur.[53] Bu yayım, ağların giderek daha da operasyonların ağırlık merkezine oturduğunu ve Bakanlığın ağ ile savaşa hazır olması gerektiğine işaret etmektedir.[54]

Savunma Bakanlığı'nın O-3600.1 Direktifi, politikasının bilişim operasyonlarının: "bilişim teknolojilerinin avantajlarından yararlanarak tam spektrum hakimiyetini desteklemek için kullanılan, düşmanın karar döngülerini etkileyen network teknolojilerindeki stratejik ABD üstünlüğünün devamının sağlanması" olduğunu belirtmektedir.[55] Ortak Yayını 3–13, bilişim operasyonlarını planlama, hazırlama, yürütülmesi ve ortak operasyonlarda belirlenen destek için doktrin sağlayan bu yayımda: "bilgisayar network operasyonlarını askeri ve sivil örgütler tarafından, ağa bağlı bilgisayarların kullanımının arttırılması ve IT

---

[48] GRYC, s.15.

[49] Graham Bradley, **Washingtonpost.com:Bush Orders Guidelines for Cyber-Warfare**, Washington Post, 7 Şubat 2003, p. A01, http://www.washingtonpost.com/ac2/ wpdyn/A381102003Feb6?language=printer, (e.t.28.01.2012).

[50] Tony Bradley, **Pandora's Box**, Antionline Newsletter #7, Nisan/Mayıs 2003, s.15–16, http://www.Antionline.com/newsle tter/aonewsletter7.pdf, (e.t.28.01.2012).

[51] John Lasker, **U.S. Military's Elite Hacker Crew**, WIRED, 18 Nisan 2005, http:// www.wired.com/politics/se curity/news/ 2005/04/67223, (e.t. 28.01.2012).

[52] Paul Berg, **Air Force Cyber Command: What It Will Do and Why We Need It**, Air & Space Power Journal, 20 Şubat 2007, http://www.airpower.au.af.mil/ apjinternational/ apj-s/2007/1tri07/bergeng.html, (e.t.28.0 1.2012).

[53] U.S. Department Of Defence, **Information Operations Roadmap 1**, 30 Ekim 2003, s.1–72, http://www.gwu. edu/~nsarc hiv/NSAEBB/NSAEBB177/info_ops_roadmap. pdf, (e.t.28.01.2012).

[54] SCHAAP, s.127.

[55] U.S. Department of Defense, Directive IR. 3600.1, **Information Operations**, 14 Ağustos 2006, http://www.Fa s.org/irp/do ddir/dod/info_ops.pdf, (e.t.29.01.2012).

altyapı sistemlerinin desteklenmesi" neden kaynaklanarak "askeri operasyonları desteklemek için geliştirilen en yeni yeteneklerden biri" şeklinde belirtilmektedir.[56]

2.2. Çin'deki Gelişmeler

Çin, günümüzde önemli siber silahlara ve bilişim altyapısına sahiptir ve sahip olduğu siber savaş doktrini 2050'de küresel "elektronik hakimiyet" sağlama amacı taşıyan hedefi, düşmanın bilişim altyapısını kesintiye uğratabilmesini içermekte; 1999 yılında günlük bir gazete olan PLA'da Çin Halk Cumhuriyeti Halk Kurtuluş Ordusu (PLA) resmi medya söyleminde: "İnternet savaşı; kara, deniz ve hava kuvvetleri ile aynı değerdedir ve kendi askeri branşına sahip olmayı gerektirir" şeklinde belirtilmekte ve ayrıca askeri ve istihbarat kaynaklarına göre, Çin'in siber kuvvetleri ABD ve diğer devletlere siber saldırılar gerçekleştirmek üzere detaylı planlar geliştirmektedir.[57]

2.3. Rusya'daki Gelişmeler

Rusya'nın silahlı kuvvetleri, oldukça dikkat çeken saldırgan siber silahlarla, bilişim teknolojileri sektörü ve akademik uzmanların işbirliği ile sağlam bir siber savaş doktrini geliştirmektedir.[58] Rusya'nın siber savaş doktrini, eklendiğinde ve diğer savaş kuvvetleriyle birlikte çalıştığında bu kuvvetin savaş potansiyelini önemli ölçüde arttıran, bir silahı ya da taktiği tanımlayan askeri bir terim bir kuvvet çarpanı olarak hareket için tasarlandığı belirtilmekte ve diğer saldırgan siber stratejiler gibi, Rusya'nın stratejisi de geleneksel askeri operasyonlar başlamadan önce düşmanın kritik altyapısının yanı sıra bilişim altyapısına zarar verme kabiliyetini içerirken ve finansal piyasalar, askeri ve sivil iletişim kapasite stratejilerini de kapsamaktadır.[59]

2.4. Kuzey Kore'deki Gelişmeler

1998'de Kuzey Kore ordusu, sadece siber savaşa odaklanan ve kurulduğu günden bu yana istikrarlı bir şekilde boyutunu ve kapasitesini arttıran 121 birim oluşturmuş, bir dizi siber silah oluşturmak ve yaymak için teknik kapasiteye sahip ve 2007 Kasım ayında ilk yazılım bombasını test ederek BM Güvenlik Konseyi kararı ile Kuzey Kore'ye anabilgisayar ve laptop bilgisayarlar satışlarının yasaklanmasına neden olmuştur; fakat, BM'nin yanıtı Kuzey Kore ordusunu siber silahlar geliştirme programının devamlılığından caydırmaya yeterli olmamıştır.[60]

---

[56] **Joint Doctrine for Information Operations**, Joint Pub. 3–13, 9 Ekim 1998, s.1–136, http://www.c4i.org/jp3_ 13.pdf (e.t.29.01.2012). Ayrıca bu operasyonlarda görevlendirilmek üzere bir program oluşturulmuş, programın 6 aylık kısmından mezun olanların bilgisayarı bir silah sistemi gibi çalıştırması mümkün olacak şekilde, yaklaşık olarak yılda 100 öğrencinin Ağ Savaşı Lisans Eğitim kursunda daha ileri düzeyde eğitim almaları amaçlanmıştır. (Bu planlamanın belirtildiği kaynak, 2008 yılında oluşturulmuştur.) Bkz. SCHAAP, s.132.

[57] SCHAAP, s.132.

[58] Charles Billo ve Welton Chang, **An Analysis of the Means and Motivations of Selected Nations States**, Institute For Security Technology Studies At Dartmouth College, Kasım 2004, s.1–5, http://www.ists.dartmouth. edu/docs/execsum.pdf, (e.t.29.01.2012).

[59] Kevin Coleman, **Russia's Cyber Forces**, Defencetech.org., 27 Mayıs 2008, http://defensetech.org/2008/05/27/ russias-cyber-forces/, (e.t.29.01.2012).

[60] Kevin Coleman, **Inside DPRK's Unit 121**, Defencetech.org., 24 Aralık 2007, http://defensetech.org/2007/12/ 24/inside-dprks-unit-121/, (e.t. 29.01.2012).

2.5. Türkiye'deki Gelişmeler

Türkiye Ocak 2011'de ilk siber terör tatbikatını ve ikinci saldırı tatbikatını öncelikle çeşitli kurumlar arasında siber karşılığın koordine edilmesi için dizayn ederek 39 ulusal ve özel Türk kurumu kapsayarak gerçekleştirmiştir.[61] Türkiye Haziran 2011'de, Türkiye'deki internet kullanıcılarının devlet tarafından desteklenen internet filtrelerinin kullanımı için gerekli olan internet filtre yasaları oluşumunu açıklamış, akabinde Anonim adlı *hacker* grup, bu yeni yasalara tepki olarak hükümetin internet web sitelerine saldırmış ve Türk polisi Anonim grubundan 32 kişiyi göz altına almıştır.[62] Mart 2011'de, Türkiye Genel Kurmay Başkanlığı'nda Siber Komutanlık olarak hizmet edecek 3 temel komutanlık kurulmuştur. Genelkurmay, örgütsel konulara bağlı önemli gecikmelerden sonra büyük ölçüde ABD Siber Komutanlığı'nı model almaktadır. Mevcut kurulan takım, siber güvenlik eğitim uzmanı 8 bilgisayar mühendisinden oluşmaktadır.[63]

3. SİBER SAVAŞ OPERASYON SİLAHLARININ İLKİ: STUXNET, SCADA SİSTEMLERİ VE DENETLEYİCİLER

Her devlet, düşman bir devletin bilgisayar ağlarını çökertmek için özel *hackerlardan* oluşan ayrıcalıklı gruplar yetiştirerek, süper güç olmaya gerek kalmadan, yeterince tehdit oluşturabilmek için gereken bilgisayar ve yazılım silahlarına sahiptir[64]; bu yüzden endüstrisi en gelişmiş ülkelerin, teknolojik

---

[61] **Turkey conducts cyber terror drill**, Hurriyet Daily News, 27 Ocak 2011, http://www.hurriyetdailynews.com /n.P?n=turke y-conducts-cyber-terror-drill-2011-01-27, (e.t. 03.01.2012).

[62] Giles Tremlett, **Turkish arrests intensify global war between hacker activists and police**, The Guardian, 13 Haziran 2011, http://www.guardian.co.uk/ technology/ 2011/jun/13/ turkish-arrests-global-war-hackers-police, (e.t.03.01.2012).

[63] Umit Enginsoy ve Burak Ege Bekdil, **Turkey Raises Emphasis On Cyberspace Defense**, Defense News, 15 Ağustos 2011, http://www.defensenews.com/ story. php?i=7388376&c=FEA&s=SPE, (e.t. 03.01.2012).

[64] SİBER SAVAŞ OPERASYON SİLAHLARI: 1990'ların ortalarında, RAND Şirketinin yaptığı bir çalışmaya göre, siber savaşların yürütülmesi için siber silahların geliştirilmesi maliyetinin oldukça düşük olduğunu ve hemen hemen her devletin ulaşabileceği bir maliyetin yeterli olduğunu tespit edilmektedir. Günümüzde 140 devletin aktif operasyonel siber silah geliştirme programlarının olduğu tahmin edilmektedir. Bkz. SCHAAP, s.134. Siber silahlar, nerede ve nasıl kullanılacakları düşünülmeden ya da tartışılmadan, gizlice üretilmeye devam etmektedir. Bu gizlilikten ötürü, kapasitelerinin ne olduğuna dair kesin bilgi yoktur, bu da devletleri; kendilerini en kötüye hazırlamaları bakımından mecbur kılmaktadır. Ayrıca bkz. Cyberwar The Threat From The Internet, The Economist, 3–9 Temmuz 2010, s.11.

1. Hizmet Reddi Saldırısı (*Denial of Service)* (DoS) Attack): DoS saldırısı "Ağa yapılan saldırı, aşırı miktarda isteğin istilası ile düzenli işleyen trafiğin yavaşlaması veya tamamen kesilmesidir ve bu hizmeti kullanarak, bu hizmetin yasal kullanıcılarını engellemek için açık bir girişim olarak nitelendirilmektedir. Bkz. SCHAAP, s.134. Hedef alınan bilgisayarların kapasitesini aşacak şekilde eylemde bulunarak, sunucunun bilgisayarlardan gelen isteklerin reddinin sağlanması hedeftir. Ayrıntılı bilgi için bkz. Eric J. Sinrod ve William P. Reilly, Cyber-Crimes: A Practical Approach To The Application Of Federal Computer Crime Laws, Santa Clara University School of Law, Volume 16, Num.2, Mayıs 2000, s.12–16, http://www.sinrodlaw.com/CyberCrime.pdf, (e.t.29.01.2012). Bu tür bir saldırının avantajı, daha büyük ve ileri teknolojik bilgisayar veya ağa karşı sınırlı kaynaklarla gerçekleştirilmesidir; örneğin, bir saldırgan eski bir PC ve yavaş bir modem ile çok daha hızlı ve ileri teknolojiye sahip bilgisayar veya ağı etkisizleştirebilir. Ayrıca bkz. CERT Coordination Center, http://www.cert.org/ tech_tips/denial_of_service.html, (e.t.29.01.2012). Dağınık Hizmet Reddi Saldırısı

(Distributed Denial of Service (DDoS)) bireysel sisteme bağlı kitlece bilgisayar ve sistemlerine virüs saldırılarının yapılmasıdır ve bir DDoS saldırısı gerçekleştirilirken, bir saldırgan binlerce virüslü bilgisayardan faydalanır—zombiler ya da robotlar olarak bilinen—tek bir sisteme aynı anda saldırı gerçekleştirmektedir. Bkz. SCHAAP, s.134. DDoS saldırıları durdurmak zordur çünkü data/veri akış sistemi birden çok bilgisayar ve birden çok mekandan kaynaklanmaktadır. Ayrıntılı bilgi için bkz. Kevin Coleman, Department of Cyber Defense, An organization who's time has come!, Technolytics, Kasım 2007, s.2, http://www.technolytics.com/Dept of_Cyber_Defense.pdf, (e.t.10.02.2012). Hizmeti Düzenli Engelleme (*Permanent Denial-of-Service*) (PDoS) saldırısı sisteme öyle kötü zarar verir ki donanımın değiştirilmesi ya da yeniden yüklenmesini gerektirmektedir. Bir hizmet veya websitenin kullanımına sabotaj olarak kullanılan ya da kötü amaçlı yazılım gönderimini gizleyen DDoS saldırının aksine, PDoS tamamen donanım sabotajıdır. Bkz. Kelly Jackson Higgins, Permanent Denial-of-Service Attack Sabotages Hardware, Dark Reading, 19 Mayıs 2008, http://archive. cert.uni-stuttgart.de/isn/2008/05/msg00102.html, (e.t.29.01.2012).

2. Zararlı Programlar: Zararlı programlar (nadiren kötü amaçlı yazılım olarak da adlandırılır), normal bilgisayar fonksiyonlarını bozarak ya da uzaktan bir saldırgana arka kapı açarak bilgisayarın kontrolünü sağlayarak saldırmaktır. Bkz. Clay Wilson, Cong. Res. Serice Rep. For Congress No. RL32114, Computer Attack And Cyber Terrorism: Vulnerabilities And Policy Issues For Congress 15, 17 Ekim 2003, http://www.fas.org/irp/crs/RL32114.pdf, (e.t.29.01.2012). Kötü amaçlı yazılım bazen dosyaları sildiği gibi diğer yandan kullanılamaz hale getirir ve verilebilecek genel örnekler arasında virüsler, solucanlar (*Worms*) ve Truva atı (*Trojan Horse*) bulunmaktadır. Ayrıntılı bilgi için bkz. Techterms.com, The Tech Terms Computer Dictionary, Malware, http://www.techterms.com/definition/malw are, (e.t.29.01.2012). Bir virüs kendini bir dosya veya programla birleştirerek bir bilgisayardan diğerine yayılmaktadır. Daha fazla bilgi için bkz. Vangie Beal, Webopedia, The Difference Between a Virus, Worm and Trojan Horse, 06.29.2010, Son güncelleme: 03.29.2011, http://www. webopedia.com/DidYouKnow/Internet/2004/virus.asp, (e.t.29.01.2012). Kendi kendini üretme kodunun yanı sıra virüs normalde yararlı bir yük içermekte ve siber saldırganlar yararlı yükleri, verilerin bozulma ya da yok olması gibi zararlı yan etkileri programlayabilmektedir. Bkz. Introduction to Computer Viruses, S0PH0S.COM, 26 Mayıs 1998, http://www.sophos.com/en-us/press-offi ce/press-releases/1998/05/ va_virusesintro.aspx, (e.t.29.01.2012). Hemen hemen her virüs çalıştırılabilir bir dosyaya bağlıdır ve bir virüs bilgisayarda var olabilir ancak bu zararlı program açılmaz veya çalıştırılmaz ise bilgisayara zarar veremez. Bkz. Beal. Solucan da virüs gibi bilgisayardan bilgisayara yayılır fakat virüsün tersine herhangi bir kişinin yardımı olmadan bu yayılmayı gerçekleştirebilir (Bir sistemdeki dosyanın avantajı ya da bilgi taşıma özelliği, bir solucanın kendi başına yayılmasına izin vermektedir) ve solucanın en tehlikeli özelliği bir sistem üzerindeki kopyalanmasıdır; böylece her bir bilgisayara tek bir solucan göndermek yerine, kendisi yüzlerce binlerce kopyasını bilgisayarlara gönderebilir. Bkz. Beal. Truva atı "İçinde kötü niyetli ya da zararlı bir kod barındıran fakat zararsız bir programmış gibi görünen, bu yolla kontrolü ele geçirip kendisinde var olan seçilmiş türdeki zararı gerçekleştirebilir". Ayrıntılı bilgi için bkz. SearchSecurity.com, Trojan Horse, http://searchsecurity.techtarget.com/ definition/ Trojan-horse, (e.t.29.01.2 012). Bu türde bir Truva atı alanlar bunu açmakta tuzağa düşmektedir çünkü yasal bir kaynaktan gelen dosya ya da yasal bir yazılımmış gibi görünmekte ve Truva atı sistemdeki dosyaları silerek (virüsler ve solucanların aksine, Truva atları çoğalarak diğer dosyalara bulaşmamakta ve kendini kopyalayamamaktadır) ve bilgileri ortadan kaldırarak büyük çapta zarar vermektedir. Bkz. Beal.

3. Yazılım Bombası: Yazılım bombası, belirli bir olayın meydana gelmesi ya da önceden belirlenmiş bir zamanda meydana gelmesi için tasarlanmış zararlı bir koddur ve bir kez tetiklendiğinde, bilgisayarı bozar, verileri siler ya da sahte işlemler üreterek bir DoS saldırısını harekete geçirmektedir. Ayrıntılı bilgi için bkz. Kevin Coleman, Russia's Cyber Forces, DEFENSETECH.org., 27 Mayıs, 2008, http://defensetech.org/2008/ 05/27/russia scyber-forces/, (e.t.29.01.2012).

4. Sahte IP Adres Kullanımı (*IP Spoofing*): IP adres sahteciliği (*IP address forgery*) ya da taşıyıcı dosya hırsızlığı (*host file hijack*) olarak da bilinen Sahte IP Adres Kullanımı, korsanların gerçek kimliklerini gizleyerek kendisini güvenli bir sunucu (sistem) olarak göstererek bir websitenin gerçeğinden ayırt edilemeyecek sahte website düzenlemeyi, tarayıcı korsanlığı (hırsızlığı) (*hijack browsers*) ya da bir ağa erişim sağlamayı içeren bir korsanlık tekniğidir. Sahte IP Adres kullanımı tarayıcı korsanlığında kullanıldığı zaman, bir ziyaretçi yasal bir sitenin, internetteki resmi adres sistemine yazarak (tekdüzen kaynak konum belirleyicisi/*uniform resource locator*) (URL) korsan tarafından oluşturulan sahte web sayfasına alınır ve eğer kullanıcı korsanlığa maruz kalmış sitenin dinamik içeriği ile etkileşime geçerse, korsan önemli bilgilere veya bilgisayar ya da ağ kaynaklarına erişebilir hale gelmektedir. SearchSecurity.com, Definitions, IP Spoofing, http://searchsecurity.techtarget.com/definition/IP-spoofing, (e. t.29.01.2012).

5. Dijital Manipülasyon: Dijital yoldan manipülasyon, genellikle yeni bir anlam yansıtan sahte bir görüntünün üretilmesiyle, bilgisayar program araçlarının ve yazılımının kullanımı ile bir görüntünün değiştirilmesidir. Bu teknik hali hazırda var olan fotoğraf ya da video gibi görüntüleri içermektedir. Ayrıntılı bilgi için. M/Cyclopedia of New Media, Digital Manipulation, http://www.fourandsix.com/photo-tampering-history/, (e.t.29.01.2012). Fotoğraf değişikliği yoluyla istihbarat ve güvenlik topluluklarının amaçlarından birini yanlış bilgilendirme ya da aldatma oluşturmaktadır. Ayrıca bkz. Photo Alteration, http://www.espionageinfo.com/Pa-Po/Photo-Alteration.html, (e.t.10.02.2012). Dijital fotoğraf işleme yazılımı, teknik hileleri arttırmakta ve insanlar yazılımı kullanmada daha becerikli hale gelmektedir; böylece manipüle edilen görüntülerin tespiti giderek zorlaşmakta ve dijital fotografik manipülasyon gittikçe daha aldatıcı olmaktadır ki fotoğrafta yer alan kişi veya nesnelerin fotoğrafın çekildiği sırada gerçekten orada olup olmadıklarının tespiti bazen imkânsız hale gelmektedir. Photo Tampering throughout History, http://www.fourandsix.com/photo-tampering-history/, (e.t.29.01.2012). 2006 yılında İsrail ve Lübnanlı Hizbullah grubu arasındaki çatışma sürerken medyanın bir fotoğrafta manipülasyon yaptığı ortaya çıkarılmıştır. Bkz. Yaakov Lappin, Reuters Admits to More Image Manipulation, YNETNEWS.COM, 7 Ağustos 2006, http:// www.ynetn ews.com/articles/0, 7340, L-3287774, 00.html, (e.t.29.01. 2012). Bir devletin, diğer devletlerin internetinde yer alan görüntülerin değiştirilerek kolaylıkla fotoğraf manipülasyonuna maruz kalması makuldür. Video çekilirken dahi manipülasyon yapmak mümkündür. Bkz. SCHAAP, s.138. Video kareleri arasında ikinci bir fraksiyon, ön planda hareket eden herhangi bir kişi ya da nesne düzenlenebilir, çıkarılabilir ve görüntüde yer almayan nesneler görüntüye eklenerek gerçekmiş gibi gösteren bu akışkanlık modern videoyu oluşturan piksellerin değiştirilebilir özelliğinden kaynaklanmaktadır; örneğin Yorumlayıcıların savaş uçakları veya taburlarca tank görüntüleri yansıtmasıyla, uydu görüntü verilerine birtakım pikseller eklemesi artık mümkündür. Ayrıntılı bilgi için bkz. Ivan Amato, Lying With Pixels, Seeing is No Longer believing. Tech. Rev., Temmuz 2000, http://www.tech nologyrevie w.com/Infotech/12115/?a=f, (e.t.29.01.2012). Princeton Video Görüntüleme (PVI), bu durumu banliyöye ait park yerindeki demo kaset kaydında kullanmıştır. Bkz. http://www.digitalbroadcasting.com/storefronts/pvimage.html, (e.t.29.01.2012). Video manüpilatörleri önceden kaydedilmiş bir konuşmacının söylediği söz ve yaptığı hareketleri hiç söylememiş ve yapmamış gibi gösterebilir. Gerçek zaman kombinasyonu, mevcut ve gelişmekte olan post-prodüksiyon teknikleri ile sanal bir ekleme, inanılmaz sayıda manipülasyon fırsatlarına kapı açmaktadır. Örneğin, CNN canlı yayınına isteyen biri bir dünya liderini ekleyebilir ve bu kişiye istediği her şeyi söyletebilir. Bkz. SCHAAP, s.137. Devletler kendi amaçlarına uygun bulduğu tamamen uydurma canlı web yayınları yapabilir. Pentagon planlamacıları, 1990 yılında Irak'ın Kuveyt'i işgalinden sonra dijital geçişi tartışmaya başlamıştır. Ayrıntılı bilgi için bkz. William M. Arkin, When Seeing and Hearing Isn't Believing, Wash. Post.Com, 1 Şubat 1999, http://www. washingtonp ost.com/wp-srv/national/dotmil/arkin020199.htm, (e.t.29.01. 2012).

altyapıları ve ağlara bağımlılıkları sebebiyle, saldırıya en açık ülkeler olduğu savunulmaktadır.[65]

2010 yılında ilk siber savaş silahı olan Stuxnet bulunarak siber güvenlik tarihinde bir ilke imza atılmıştır.[66] Stuxnet[67]; seçtiği hedef, entellektüellik seviyesi ve gelecekteki kötü amaçlı yazılımlara etkileri açılarından oldukça önemlidir ve genel kanının aksine, Stuxnet endüstriyel casusluğa dair değildir: bilgi çalmamakla, değiştirmemekle ya da silmemekle birlikte Stuxnet'in amacı; fiziki ve askeri hedefler belirleyerek onlara zarar vermektir.[68]

SCADA sistemi; insan operatörlere, endüstriyel süreci izleme, süreçteki değerleri belleğe alma ve analiz etme imkânı sunan bir Windows uygulamasıdır ve SCADA uygulamasının Stuxnet saldırısında küçük bir rolü olduğu doğru olmakla birlikte; Stuxnet'in asıl saldırısı SCADA yazılımına değil, endüstriyel denetleyicilere karşı yapılmasıdır; ayrıca saldırı uzaktan kumanda edilmemekte, tamamen bağımsız ve internet bağlantısı gerektirmemektedir.[69]

Pompalar, vanalar, sürücüler (motorlar), termometreler ve takometreler gibi araçlar, direkt olarak veya endüstriyel bir şebeke bağlantısı aracılığıyla bir denetleyiciye elektrikle bağlıdır; böylece bir bilgisayar programı sadece bilgi üzerine çalışırken, denetleyici bir program fiziksel yapı üzerine çalışmakta ve böylece bir denetleyicinin hileleri, bilginin gizliliği, bütünlüğü ve kullanılabilirliğine dair olmaktan çok, fiziksel üretim sürecinin performansı ve verimliliği ile ilgili olmakta; ayrıca en kötü durumda denetleyici hileleri fiziksel zararla sonuçlanabilmektedir.[70]

Saldırganlar Stuxnet'i yayma amacıyla geleneksel solucan teknolojisini kullanmak yerine, USB bellekler ve yerel ağlar ile yerel dağıtım yöntemini seçmektedir. Stuxnet, bulduğu her kişisel Windows bilgisayarına bulaşabilirken, denetleyiciler konusunda şu yönden daha farklıdır; sadece belli bir üretici firmanın (Siemens) denetleyicilerini hedef alan Stuxnet, onları bulma yolunda (Ethernet, Profibus veya Siemens MPI denilen özel bir iletişim bağlantısı ile virüslü bir Windows kutusu iliştirerek), hedef üzerinde olduğundan emin olmak için karmaşık bir parmak izi sürecinden geçmektedir.[71] Stuxnet, saldırı sırasında önceden kaydedilmiş bilgiyi meşru bir koda işlemektedir.[72]

Stuxnet'in yararlandığı açıklar, Microsoft'un savunduğu yöntemlerle engellenebilecek gibi görünmemektedir; çünkü bu açıkların, yazılım ya da üretim bilgisi kusurundan değil; ürünün kendi meşru özelliklerinden kaynaklandığı görülmektedir.[73] Stuxnet'in kullandığı başlıca açık, mevcut denetleyicilerin

---

[65] Estonya'ya yapılan DDoS saldırıları gerçek bir siber savaş olmayabilir fakat artık birçok devlet, devlet destekli siber saldırıları ciddiye almaktadır. Örneğin ABD; Amerikan Askeri Ağlarını koruması amacıyla, Fort Meade, Maryland'de, Mayıs 2010'da Cyber Command (Cybercom) adlı bir örgüt kurmuştur. Birleşik Krallık ise, Government Communications Headquarters (GCHQ), Cheltenham'da siber güvenlik operasyonları merkezi kurmuştur. Daha fazla bilgi için bkz. Thomas M. Chen, "Stuxnet, The Real Start of Cyber Warfare?", IEEE Network, Kasım/Aralık 2010, s.1–3.

[66] Ralph Langer, **Stuxnet: Dissecting a Cyberwarfare Weapon**, Focus, Mayıs/Haziran 2011, s.49.

[67] Ralph Langner'a göre Stuxnet ilk gerçek "siber silah"tır çünkü fiziksel ve askeri zarar verme hedefi taşımakta dır.

[68] CHEN, s.2.

[69] LANGNER, s.49.

[70] LANGNER, s.49.

[71] LANGNER, s.49.

[72] LANGNER, s.50.

[73] LANGNER, s.51.

dijital kod imzalama yöntemine izin vermemesinden ileri gelmektedir ve denetleyici kodun nerden geldiğine bakmadan meşru bir kabul etme durumu mevcuttur fakat dijital imza yönteminde, denetleyici, yüklenen kodun meşru bir mühendislik istasyonundan alındığından emin olabilmektedir.[74]

Yukarıda belirtilen yöntem veya yöntemler yoluyla siber saldırıya teşebbüs etmeye sebep olabilecek etkenler de oldukça çeşitlidir. Bazı kişi ya da gruplar, hatta devletler, ideolojik sebeplerle siber savaş ya da saldırı yoluna gitmekte, devlet ideolojisi benimseme yolu ile siber saldırılarda bulunulabileceği gibi, bu devlet ideolojilerine karşı olarak da bu faaliyetler yapılabilmektedir. İdeoloji temelli bu faaliyetlere yerinde bir örnek; İslam ideolojisini benimsediklerini savunarak Batı dünyasına karşı mücadele eden grupların gerçekleştirdiği siber saldırılar verilebileceği gibi; 1998 yılında, ABD, Birleşik Krallık, Hollanda ve Yeni Zelanda'dan, kendilerini Milworm olarak adlandıran altı *hackerın*, Hindistan'ın Bhabha Atom Araştırma Merkezi (BARC) websitesini hackleyerek "Eğer nükleer bir savaş başlarsa, ilk çığlık atacak olan siz olacaksınız" şeklindeki bıraktıkları mesaj da verilebilir.[75] Saldırının uygulanacağı hedefin sembo-

---

[74] LANGNER, s.51.

[75] D. E. Denning, Hacktivism: An Emerging Threat to Diplomacy, American Foreign Service Association, 25.06.2007, www.a fsa.org/fsj/sept00/Denning.cfm, (e.t.10.02.2012); Motivasyon: Maddi sonuçlara ulaşma arzusu motivasyon ile sağlayacağı gibi; gurur, prestij, tatmin gibi manevi sebeplerle de insanlar motive olmaktadır ve bu motivasyonlar da siber suçların işlenmesine sebep olmaktadır. Bkz. J. Hirshleifer, The bioeconomic causes of war, Managerial and Decision Economics 19 (7/8), 1998, s.457–4 66, http://time.dufe.edu.cn/spti/artic le/hirshleifer/hirshleifer170.pdf, (e.t.29.01.2012). Temel olarak iki kategoride incelenebilen motivasyon tipleri mevcuttur: İlki; içsel kaynaklı motivasyonlar, ikincisi ise; dışsal kaynaklı motivasyonlardır. İçsel motivasyonun temeli, insanın yeterlilik ve kendi kaderini kendisi belirleme ihtiyaçlarına dayanmaktadır. Ayrıntılı bilgi için: E.L Deci ve R.M. Ryan, Intrinsic Motivation and Self-determination in Human Behavior, Plenum Press, New York, 1985, s.35, http://www.google.com.tr/books?hl=tr&lr=&id=p96Wm nER4QC&oi=fnd&pg=PA1&dq=Deci+E.T, +Ryan, +R.M+1985+Intrinsic+Motivation+and+Selfdetermination+i n+Human+Behavior&ots=3cGT x2vc23&sig=eG5t cI60CDo0grCtdw9xai0Qw38&redir_esc=y#v=onepage&q &f=false, (e.t.29.01.2012). Kendi içinde; eğlence temelli içsel motivasyon ve zorunluluk-toplum temelli içsel motivasyon olarak ikiye ayrılmaktadır. Ayrıca: S. Lindenberg, Intrinsic Motivation in a New Light, Kyklos 54 (2/3), 2001, s.317–342, http://www.ppsw.ru g. nl/~lindenb/ documents/articles/2001_Lindenberg-Intrinsic_motivation_in_a_new_light.pdf, (e.t.29.01.2012). Eğlence temelli içsel motivasyon; bir faaliyette yer almanın kişiye eğlence ve kendi varlığının tadını çıkarma duygusu vermesi anlamına gelmektedir ve bu sebepler dışında herhangi bir maddi çıkar vs. söz konusu değildir çünkü birey bu tip bir motivasyonla siber saldırı faaliyetlerinde bulunabilir. Bkz. E.L Deci ve R.M. Ryan, Intrinsic Motivation and Self-determination in Human Behavior, Plenum Press, New York, 1985, s.35, http://www.google.com.tr/books?hl=tr&lr=&id=p96WmnER4QC&oi=fnd&pg=PA1&dq =Deci+E.T, +Ryan, +R. M+1985+Intrinsic+Motivation+ and+Selfdetermination+in+H uman+Behavior&ots=3cGT x2vc23&sig=eG5tcI6 0CDo0grCtdw9xai0Qw38&redir_esc=y#v=onepage&q&f =false, (e.t.29.01.2012). Zorunluluk-Toplum temelli içsel motivasyonda ise; siber saldırı faaliyetlerini gerçekleştiren birey ya da gruplar kendilerini bir topluluğa, bölgeye veya devlete ait hissetmeleri sonucu, böyle bir faaliyette bulunmaları gerektiği kanısına vararak motive olabilmektedirler. Ayrıntılı bilgi için bkz. K.R. Lakhani, R.G. Wolf, In: J. Feller, B. Fitzgerald, S. Hissam, K. R. Lakhani (Editörler), Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects, MIT Press, 2005, http://ocwmit.edu/courses/sloan-school-of-management/15-352-managing-innovation-emerging-trends-spring-2005/readings/lakhaniwolf.pdf, (e.t.29.01.2012). Dışsal motivasyonda, saldırganın asıl amacı yüklü miktarda kazanç elde edebilmektir, bu yüzden genellikle büyük şirketlere, bankalara saldırırlar ve saldırıyı kaldırmak için fidye talep ederler

lik olarak öneminin yüksek olması, yani saldırı durumunda faaliyetin ses getirebilir olması ve tehlikeliliğinin de yüksek olması o hedefi daha cazip kılmaktadır; buna en iyi örnek; 9/11'de İkiz Kuleler, Pentagon ve Beyaz Saray'a gerçekleştirilen saldırılardır.[76] Dolayısıyla sembolik önem arz eden mekân, kurum ya da kişilerin bu saldırılara maruz kalma ihtimali, diğer türdeşlerine göre daha yüksek olduğu görülmektedir.[77]

4. SİBER SAVAŞ OPERASYONLARININ CASUSLUK İLE İLİŞKİSİ

Casusluk, bilgi toplayan devletin mağdur devlete zarar verme ya da başka bir devlete fırsat vermek adına mağdur devletin ulusal savunması hakkında bilgi edinme, sunma, aktarma, ilişki kurma veya alma eylemidir.[78] ABD Savunma Bakanlığı, "Bilgisayar Ağı Sömürüsü" terimini "hedef veya düşmanın otomatik bilişim sistemleri veya ağlarından veri toplamak üzere, bilgisayar ağları kullanımı üzerinden gerçekleştirilen operasyonlar veya istihbarat toplama kapasitesi" şeklinde tanımlamaktadır.[79] 1907 4. Lahey Sözleşmesi'ne Ek 24. Madde'de silahlı çatışma sırasında özellikle "savaş hileleri ve işbirliği bilgileri elde etmek için düşman ve ülkesi hakkında gerekli bilgilere cevaz verilebilir" koşuluyla casusluğun meşru olduğu yer almaktadır.[80] Yüzyıllar buyunca casusluk devletler tarafından uygulana geldiği gibi, bugüne kadar hiçbir uluslararası konvansiyonda barış zamanı casusluğun meşru olduğu yer almamakta ve ayrıca uluslararası hukuk, casusluğu temelde yanlış bir eylem olarak kabul etmemektedir.[81] Potomac Enstitüsü Araştırma Görevlisi Thomas Wingfield, casusluk hakkını devletin temel öz-savunma hakkının bir parçası olduğu sonucuna vararak, 1961 Diplomatik İlişkiler Hakkında Viyana Sözleşmesi'nin barış zamanında ulusların casusluk faaliyetinde bulunmalarını dış ilişkiler ve dış politikanın özündeki gizli bilgi edinme eylemlerin bütünü köklü hakları olarak tanındığının yer aldığını vurgulamaktadır.[82] Genelde casusluk, uluslararası hukuk kapsamında yasal ve iç hukuklarda yasa dışı olarak kabul edilmektedir.[83]

Moonlight Maze ve *Titan Rain* eylemleri siber casusluk faaliyetlerine en bilinen iki örnek olarak gösterilmekte ve aynı zamanda bu iki olay bilgisayar çağında casusluğun nasıl değiştiğini göstermektedir; ayrıca özünde hala casusluktur ve uluslararası hukuk bağlamında yasal veya yasadışı faaliyetleri

---

fakat bazı şirketler buna yanaşmasa da, pek çoğu bu fidyeleri ödemek durumunda kalmaktadırlar. Bkz. KSHETRI, s.554.

[76] J.F. Coates, **What's next? Foreseeable terrorist acts**, The Futurist 36 (5), 2002, s.23–26.

[77] Hedefin kapsamı bakımından geniş olması, örneğin; büyük bir şirkete yapılan saldırı onun yayılmış olduğu pe k çok ağa da yansıyacağından ve saldırganlara yeni hedefler doğuracağından, onu diğer hedeflere göre daha çeki ci yapmaktadır.

[78] Joint Chiefs Of Staff, Joint Publication 1-02, Department Of Dhf. Directive Of Military &Assoc'D Terms, 12 Nisan 2001, s.190, http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02 (01).pdf, (e.t.29.01.2012).

[79] Joint Chiefs Of Staff, Joint Publication 1–02, Department Of Dhf. Directive Of Military &Assoc'D Terms, 12 Nisan 2001, s.113, http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02 (01).pdf, (e.t.29.01.2012).

[80] ICRC, **International Humanitarian Law - Treaties & Documents**, http://www.icrc.org/ihl.nsf/WebART/19 5200034?O penDocument, (e.t.29.01.2012).

[81] Roger D. Scott, **Territorially Intrusive Intelligence Collection and International Law**, 46 A.F. L. Rev. 21 7, 1999, s.218.

[82] Thomas C. WIingfield, **The Law Of Information Conflict: National Security Law In Cyberspace 17**, Aeg is Research Corp., 2000, s.350

[83] Jennifer J. Rho, **Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Ali en Tort Statute**, 7 Cffl. J. INT'L L.695, 2006–2007, s.701.

belirlemeye çalışırken siber savaş operasyonlarına bakıldığından daha farklı olarak değerlendirilmelidir.[84] *Moonlight Maze* olayında Rus *hackerlar* bir yıl boyunca Savunma bakanlığı bilgisayarlarına nüfuz ederek büyük miktarda kritik verileri çalmışlar, Pentagon ve FBI yetkililerine göre, *Moonlight Maze* Savunma Bakanlığı'nın yanı sıra Enerji bakanlığı, NASA, askeri müteahhitler ve ordu ile bağlantılı sivil üniversiteleri de hedef alan, Rusya devletinin desteklediği ABD teknolojisini elde etme istihbarat kampanyası olarak tanımlamış ve bu olayda Savunma Bakanlığı ağlarında herhangi bir zarar ya da imha raporlamamıştır.[85] NASA Genel Müfettişi Roberta Gross: "Zararın ne olduğunu anlatmak zor… Sistemi kapatmadılar. Dosyalardaki listeleri alıp, kişilerin yönetiminde nelerin olduğunu görmek istediler" açıklamasında bulunmuştur.[86]

Titan Rain, Çin merkezli olduğuna inanılan 2003 yılında ABD bilgisayar sistemlerine bir dizi koordineli saldırılara verilen addır. Devlet destekli casusluk, kurumsal casusluk ya da rastgele *hacker* saldırılar olup olmadığının hassas doğası belirsizdir.[87] ABD, bu saldırıları Çin'in Guangdong eyaletine kadar takip etmiş ve SANS Enstitüsü Müdürü Alan Palier'a göre, kullanılan tekniklerin ordu dışından başka bir kaynaktan gelmesi muhtemel görünmemekte ve *hackerların*, uzman havacılığın ve gece planlama yazılımını da kapsayan Füze Havacılık Ordu Komutanlığı'nın merkezi olan Redstone Arsenal'deki askeri sırları çaldığı düşünülmektedir.[88]

5. SİBERUZAYDA SİBER SALDIRI FAALİYETLERİ

5 Aralık 2005 tarihinde ABD Hava Kuvvetleri Misyonu 'nu şu şekilde değiştirmiştir: "Amerika Birleşik Devletleri Hava Kuvvetleri Misyonu; Havada, uzayda ve siberuzayda uçmak, savaşmak ve kazanmaktır" ve siberuzayın bu tanıma ilave edilmesi yeni bir durumdur: Savaş alanı 1990'larda başlayıp günümüzde de devam eden harpte bir devrim meydana gelmektedir.[89] Ancak, siberuzaydaki askeri operasyon deneyimleri değişkendir. En son ve yaygın olarak bildirilen Estonya (2007) ve Gürcistan'da (2008) hem özel hem kamu kurumlarında meydana gelen olaylarda, siber saldırıların inkârı ile sonuçlanmıştır.[90] Bu örnekler, siber operasyonların fiili tehdit seviyesinin neden değişken olduğunu göstermektedir. Bazı tehditlerin sonucu ekonomik zarardan öteye

---

[84] SCHAAP, s. 141.

[85] C. Christopher Joyner ve Catherine Lotdonte, **Information Warfare as International Coercion: Elements of a Legal Framework**, 12 EUR. J. INT'L L. 825–841, 2001, s.840, http://www.ejil.Org/pdfs/12/5/1552.pdf (e.t.29.01.2012).

[86] JOYNER, s.841.

[87] SCHAAP, s.141.

[88] **Hacker Attacks in US Linked to Chinese Military: Researchers**, 12 Aralık 2005, http://seclists.org/isn/200 5/Dec/0059.html, (e.t.29.01.2012).

[89] Tammy M. Knierim, Lou Anne DeMattei ve Sebastian M. Convertino, **Flying and Fighting in Cyberspace**, Maxwell Paper No.40Air War College, Temmuz 2007, s.15, http://aupress.au.af.mil/digital/pdf/paper/mp_0040_ convertino_demattei_ knierim_ flying_fighting_cyberspace.pdf, (e.t.30.01.2012).

[90] "DDoS"; kaynağa gönderilmesi mümkün birçok komünikasyon teklifi gönderilerek bilgisayar kaynağının kullanılamaz hale getirilmesi için yapılan teşebbüslerdir. Böylece sistemin aşırı yüklenmesiyle, sisteme düzenli olarak gönderilen iletişim istekleri kullanılamaz hale gelmektedir). Estonya da görülen olay Tallin'de Sovyet döneminden kalma bir savaş tehcir olayı anıtı ile ilgiliyken, Gürcistan'daki olay 2008 yılındaki Rusya-Gürcistan savaşı sırasında gerçekleşmiş, aynı zamanda her iki olayda da hiç bir fiziksel zarar ve yaralanma meydana gelmemekle beraber, ticari faaliyetlerdeki kısmi kesinti medeni ve politik hakların tecavüzü ile birleşerek çok büyük miktarda parasal zarar ortaya çıkmıştır.

geçmezken, diğerleri yeni bir tür kitle imha silahı olarak ya da "Elektronik Pearl Harbor" korkusu ile sonuçlanabileceği kaygısını taşımakta, her durumda devletler bu konuya silahlı kuvvetlerde özel siber üniteler kurarak yüksek derecede önem verdiklerini göstermektedir.[91] Konu ile ilgili olarak NATO tarafından Devletlerin silahlı kuvvetlerinin katılımıyla 2008 yılında Tallin temelli siber savunma politikasının belirlenmesi için Siber Savunma Mükemmellik Merkezi kurulmuştur.[92]

Bir devletin faaliyetine referans olabilecek açık bir metin olmamasına rağmen, silahlı kuvvetlerin siber operasyonları mevcut olmayan eşik düzeyi meşruluğu çeşitli yönetimler tarafından ölçülmektedir. Siber operasyonların meşruluğu, bu tip devlet eylemine açık metinsel bir referans bulunmamasına rağmen, çeşitli sistemlerin ölçtüğü silahlı kuvvetler alt sınır olarak kabul edilmemelidir. Örneğin, Uluslararası Telekomünikasyon Birliği (ITU) Tüzüğü m.38, uluslararası telekomünikasyonun kesintisiz sürdürülebilmesinin üye devletlerce sağlanmasını zorunda bırakmaktadır.[93] Sibergüvenlik kültürünün tanıtımı için başvurulan bilgi sistemleri ve ağlarının korunması ile ilgili bir dizi araç mevcuttur. OECD Bilgi Sistemleri ve Ağ Güvenlik Yönergeleri ya da 23 Aralık 2003 BM Genel Kurul Kararı 58/199[94], "Küresel Sibergüvenlik Kültürü ve Kritik Bilgi Altyapılarının Korunması" örnek gösterilebilir.[95] Siberuzaydaki devlet eylemleri böylece geleneksel egemenlik kuralları ve toprak bütünlüğü ile sınırlanmaktadır. Bundan dolayı, eğer yasaklanmış müdahale olarak nitelendiriliyorsa silahlı kuvvetler düzeyinde değillerse hukuk dışı olarak nitelendirilmelidir.[96] Estonya olayında, Estonya hükümeti, diğer devletlerle yurt dışı kaynaklı DDoS-saldırılarını durdurmak amacıyla dış ağ bağlantısını kesmiştir. Bu eylem, bir devletin bir diğer devletin iç işlerine karşı istemeyerek yapılmış da olsa, bir devlete atfedilebilir olduğu müddetçe bir tehdit olarak görülmektedir.[97] Uluslararası çevre hukuku bağlamında, komşu devletlerin birbirlerine önemli zarar vermesinin yasaklanması oldukça sağlam temeller üzerinde yapılandırılmıştır. Benzer bir yasağın varlığı internet altyapısının entegrasyon ve güvenliği bağlamında bazı yazarlarca uygun bulunmakla birlikte, genel olarak oluşturulamadığı görülmektedir.[98]

---

[91] On Bush's Watch, **U.S. Suffered Its "Electronic Pearl Harbor**, 3.18.2010, Güncelleme: 5.25.2011, http://w ww.huffingt onpost.com/2009/11/10/on-bushs-watch-us-suffere_n_352204.html, (e.t.30.01.2012).

[92] Johann-Christoph WOLTAG, Cyber Warfare, Max Planck Encyclopedia of Public International Law, Rüdiger Wolfrum (editör), Oxford University Press, 2010, s.1.

[93] http://www.itu.int/net/about/basic-texts/constitution/chaptervi.aspx, (e.t.31.01.2012).

[94] Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, United Nations General Assembly, A/RES/58/199, Fifty-eighth session, 30 January 2004, s.1-3, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf, (e.t.12.02.2012).

[95] A.A. Streltsov, **International information security: description and legal aspects**, icts and international security, s.7, http://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2642.pdf, (e.t.10.02.2012).

[96] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf?OpenElement, (e.t.31.01.20 12).

[97] WOLTAG, s.4.

[98] WOLTAG, s.3.

5.1. Siber Savaşın Tanımı ve Ayrımı

Siber savaş, öncelikle bilgisayar sistemi kullanan askeri faaliyetlerin ağlar aracılığıyla saldırı amacını kapsamakla birlikte, muhaliflerin ana amacı, tipik olarak bu sistemlerin kullanımının genellikle inkâr etmek ya da işlevleri kendi yönetim ve kontrolü altına almak için onlara erişmek ve hedef ağ yoluyla ulaşılabilen tüm bilgisayar sistemlerini kapsamaktadır.[99] Bu cihazlar, mobil telefonlardan düzenli kullanılan kişisel bilgisayarlara ya da askeri birliklerin kontrol sistemlerine dek uzanan, denetleyici kontrol ve verilere ulaşma sistemleri (SCADA) gibi karmaşık altyapı sistemleri yönetiminde kullanılmaktadır. Siber savaş kavramı, silahlı çatışma devam ederken bu gibi eylemlerle sınırlı iken, yine de askeri siber operasyonlar barış zamanı ve kısa süreli silahlı çatışmalar sırasında farkında olunmalıdır.[100] Genellikle siber savaş, bilgisayar ağı saldırılarıyla (CNA) eşit tutulmaktadır, fakat CNA'da dahi zarar vermek için kinetik enerji kullanmamakta ve bunların canlı varlıklar üzerindeki etkileri biyolojik ve kimyasal silahlar ile karıştırılmaktadır. Siber operasyonların icrası göreceli olarak düşük maliyetli olmakla birlikte, bunların kullanımı da özellikle terörist örgütler ve küçük veya gelişmemiş silahlı kuvvetlere sahip devletler için cazip olmakla birlikte, siber operasyonlar çok çeşitli yollardan kullanılabilmektedir.[101] Bu yüzden mevcut olan çeşitli seçenekler arasından açıkça ayıt edilmeleri çok önemlidir. İzinsiz bir şekilde, BM Şartı m.2/4 "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" bağlamında silahlı kuvvetlerce devralınmasına rağmen yine de askeri bilgisayar ağı operasyonları mevcuttur, bu bağlamda çalınan bilgilerin niteliği, örneğin güvenlik amacıyla hayati olarak sınıflandırılan veriler, silahlı çatışma operasyonları olarak nitelendirilmesi tartışma konusu oluşturmaktadır.[102] Böyle bir bakış açısı, geleneksel casusluk işlemi ile sert bir çelişki oluşturmasına rağmen, sonuçta bu durum uluslararası hukukta yasaklanmıştır. Dahası, herhangi bir devlet desteği olmaksızın bilgisayar sistemleri kullanımı ile bireylerin gerçekleştirdiği eylemler, açıkça bireysel siber suç birimleri olarak ayrılmalıdır. Bu durum ülkelerin kendi ceza kanunlarınca ve uluslararası alanda Avrupa Konseyi üyesi olmayan ülkeler için de örnek bir mevzuat olan Avrupa Konseyi Siber Suç Konvansiyonu müeyyidelendirilmektedir.[103] Terör örgütleri, artan oranda düşük maliyet nedeniyle siber saldırılar için altyapı oluşturarak internet yardımıyla operasyonları için gerekli koordinasyon ve hazırlıkları gerçekleştirmektedirler.[104]

---

[99] Johann-Christoph WOLTAG, Cyber Warfare, Max Planck Encyclopedia of Public International Law, Rüdige r Wolfrum (editör), Oxford University Press, 2010, s.1.

[100] Eric Byres, **The Myths and facts behind Cyber Security Risks for Industrial Control Systems**, British Columbia Institute Of Technology A Polytechnic Institution, http://www.nealsystems.com/downloads/Myths%2 0and%20Facts%20for %20Control%20System%20Cyber-security.pdf, (e.t.30.01.2012).

[101] Joint Publication 3–13, **Information Operations**, 13 Şubat 2006, http://www. dtic.mil/doctrine/new_pubs/jp3 _13.pdf, (e.t.30.01.2012).

[102] **Charter of the United Nations**, http://www.un.org/en/documents/charter/ chapter1.shtml, (e.t.12 0.01.2012).

[103] 23 Kasım 2001'de imzalanıp, 1 Temmuz 2004'te yürürlüğe girdi ETS No 185, **Convention on Cybercrime**, Council of Europe, http://conventions.coe.int/ Treaty/ en/Treaties/html/185.htm, (e.t.30.01.2 012).

[104] WOLTAG, s.2.

Saldırganlık eylemleri; tehdit ya da güç kullanımı ve silahlı saldırı terimlerince kolayca referans bulabilmesine rağmen, bu terimler BM Şartında tanımlanmamakta, "bağlayıcı olmayan hukuk", diğer bağlayıcı olmayan kaynaklar bu terimleri açıklığa kavuşturmaya çalışmış olsa da, ulusal güvenlik stratejilerini ve politik beyan deklarasyonları sorununu kesin ve açık olarak belirtirken, egemen devletler aktif olarak bu hükümleri hukuki yorumlarla etkilemeyi araştırmaktadır.[105] BM uluslararası bilişim güvenliği konusunda hükümet uzmanlarından oluşan heyetin Rus üyesinin belirttiği gibi: Bilişim silahlarının pratikte kullanılacağına dair hiç şüphe olmamakla birlikte bazı silahlı kuvvetler şimdiden ICT'leri kullanacak özel birimler hazırlamaktadır.[106] Cenevre Sözleşmeleri ve diğer anlaşma araçlarının silahlı çatışmaların yürütülmesi amacıyla genel ilkelerin kodifiye edilmesi için çaba gösterilmesine rağmen (gereklilik, orantılılık, ayrım, ayrımcılık ve insancıllık dâhil), yeni teknolojilerin geliştirilmesi her zaman savaş araç ve yöntemleri üzerinde sınırlamalar getirilmesi için zorluklar ortaya çıkarmaktadır.[107] Uluslararası toplum içinde iki önemli tartışmanın ilki, Uluslararası İnsancıl Hukukun mevcut kurallarının ve normlarının siber çatışmalara uygulanabilir ölçüde genişletilmesi ve ikinci olarak bilgi silahları ile ilgili lex specialis silahsızlanma önlemlerine ihtiyaç olup olmadığının belirlenmesidir.[108] 2001 yılında AB adına konuşan İsveç Delegesi, BM Genel Sekreterliği'ne bir gönderme yapmıştır: "AB, Genel Kurul kapsamında, Birinci Komitenin ana forumunun bilgi güvenliği konusunun tartışılması fikrinde değildir. Bu soru, ağırlıklı olarak silahsızlanma ve uluslararası güvenlik dışındaki diğer konuları kapsadığından beri, AB, en azından bu konunun bazı yönlerini tartışmak üzere, diğer komitelerin daha iyi olduğuna inanmaktadır".[109] Ardından 2004 yılında, Amerika Birleşik Devletleri ve İngiltere resmen askeri ICT'lerin kullanımını sınırlayan bir uluslararası antlaşmaya karşı olduğunu belirtmiş, her iki devlet de Uluslararası İnsancıl Hukuk hükümlerinin, bu tür teknolojilerin kullanımını düzenlemesinin yeterli olduğunu deklare etmiştir.[110] Diğer yandan Rusya ve Çin'i de içeren, SCO (*Shanghai Cooperation Organisation*) Antlaşması'na taraf olan devletler, yaygınlaşan savunma kapasitesi, ulusal güvenlik ve kamu güvenliğini tehlikeye sokan bilişim silahlarının kullanılmasını azaltan uluslararası hukukun gelişimi ile ilgili toplu önlemler

---

[105] KANUCK, s.1586.

[106] A.A. Streltsov, **International Information Security: Description and Legal Aspects**, DISARMAMENT F., 2007 (Issue 3), s.11, http://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2642.pdf, (e.t.08.02.2012).

[107] **Convention on Prohibitions or Restrictions on tbe Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects**, 10 Ekim 1980, S, TREATY Doc. No. 103–25 (1994). 1342 U.N.T.S. 137, http://www.icrc.org/eng/resources/documents/publication/p0811.htm, (e.t.08.02.2012).

[108] Sean Watts, Combatant Status and Computer Network Attack (3 Ağustos 2009), Virginia Journal of International Law, Vol. 50, No. 2, s. 392–393, 2010, http://ssrn.com/abstract=1460680, (e.t.08.02.2012).

[109] The Secretary-General, **Developments in the Field of Information and Telecommunications in the Context of International Security**, delivered to the General Assembly, U, N, Doc. A/62/98, 2 Temmuz 2007, http://www.disarmament.un.org/library.../a-62-98.pdf, (e.t.08.02.2012).

[110] The Secretary-General, **Developments in the Field of Information and Telecommunications in the Context of International Security**, delivered to the General Assembly, U.N. Doc, A/59/116, 23 Haziran 2004, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/407/04/PDF/N0440704.pdf?OpenElement, (e.t.08.02.2012).

almış ve SCO üyesi olmayan Brezilya 2009 yılında çok benzer bir pozisyonu BM Genel Sekreterliği'nde ileri sürmüştür: "Birleşmiş Milletler ayrıca şu hususlara özel önem vererek, siber savaşlarda devletler arası çatışma durumlarında bilgi ve telekomünikasyonun kullanılması tartışmalarında devletlerarası çatışma durumları ile ilgili tartışmalarda öncü bir rol oynamalıdır: Bilgi silahların kullanımı için bir davranış kanununun oluşturulması."[111] Devletlerin ağ uygulaması gözlemlerinden askeri ICT kullanımı ile ilgili bir lex specialis ihtiyacına ilişkin derin anlaşmazlık bulunmakta, sadece genel olarak şu anda hiçbir görüşün kabul edilmemesinden ziyade, BM Güvenlik Konseyi daimi üyelerinden ABD, İngiltere ve Fransa yeni bağlayıcı kurallara karşılar iken, Rusya ve Çin bu grubun görünürde aleyhindedir.[112] Bu resmi açıklamaların bazıları eski olmakla birlikte ulusal pozisyonları değişmektedir; örneğin, Başkan Obama'nın 29 Mayıs 2009'daki konuşması ve Beyaz Sarayın Siber Uzay Politika İncelemesi (*White House Cyberspace Policy Review*), ABD'nin, henüz herhangi bir resmi bağlayıcı enstrümanları müzakere etmeye hazır olmasa da uluslararası bir güvenlik meselesi olarak siber çatışmaları tartışmak için yeni bir istek duyduğuna işaret etmektedir.[113] Devlet uygulamaları çift-yönlü, egemen devletler; bireysel veya toplu olarak jus in bello ve jus ad bellum kuralları özyineleme süreciyle yorum oluşturarak, kendi ulusal stratejilerini, tespit politikalarını, askeri doktrinlerini ve angajman kurallarını üretirler ve uluslararası teamül hukuku, BM Şartı, Cenevre Sözleşmeleri ve diğer Uluslararası İnsancıl Hukuk hükümleriyle gelecekteki uygulamaları etkileyen faaliyetleri yürütmelidirler.[114]

Mevcut yasal duruma baktığımızda, devletlerin askeri siber operasyonları çerçevesindeki problemler, uluslararası hukuk tarafından açıkça ele alınmamıştır. Şimdiye kadar CNA'ların yasaklanması veya düzenlenmesi için uluslararası alanda yapılan tek girişim, Rusya Federasyonu'nun BM Genel Kurulu'nda kabulü için 1998 yılında önerilen Karar Tasarısı olmuştur fakat kabul edilmemiştir.[115] Devletin siber operasyonlardaki göreceli yeniliğinden dolayı, devletin bu konudaki devlet uygulamaları bu bağlamda gözlenmemektedir. Bir yandan bu konunun güncelliği, diğer yandan bir düzenlemenin olmayışı, metot olarak geleneksel kuralların uygulanması ve siber savaşın varlığı bu alanı ele alan her yaklaşım için yol gösterici olması gerekmektedir.[116]

6. SİBER TERÖRİZM VE KÜRESELLEŞME

Stratejik ve Uluslararası Çalışmalar Merkezi tarafından 1998 yılında, "Sibersuç, Siber Terörizm, Siber Savaş, Ektronik Bir Yenilginin Önlenmesi" başlığıyla yayınlanan raporda, siber terörizm kavramı: "Ulusaltı gruplar, gizli ajanlar ya da bireyler tarafından; bilgi ve bilgisayar sistemlerine, bilgisayar

---

111 The Secretary-General, **Developments in the Field of Information and Telecommunications in the Context of International Security**, delivered to the General Assembly, U, N, Doc. A/62/98, 2 Temmuz 2007, http://www.disarmament.un.org/library.../a-62-98.pdf, (e.t.08.02.2012).

112 The Secretary-General, **Developments in the Field of Information and Telecommunications in the Context of International Security**, delivered to the General Assembly, U, N, Doc. A/62/98, 2 Temmuz 2007, http://www.disarmament.un.org/library.../a-62-98.pdf, (e.t.08.02.2012).

113 White House. **Cyberspace Policy Review**, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace _Policy_ Re view_final.pdf, (e.t.08.02.2012).

114 KANUCK, s.1588.

115 http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf, (e.t.31.01.2012).

116 WOLTAG, s.2.

programlarına ve verilerine karşı önceden planlanan, siyasi olarak motive edilen ve muharip olmayan hedeflere karşı şiddetle sonuçlanan saldırılar" olarak tanımlanmaktadır.[117]

Siber terörizm, konsept olarak bilgisayar ve diğer yüksek teknoloji türlerinin silah olarak kullanılmasıyla 1990'ların ortalarından itibaren bilgi savaşları altında tartışılmaya başlamış, iki ülkede (ABD ve Çin) bilgi savaşı kapasitelerinde gelişmeler görülmüş fakat ABD'de 09.11.2001'de meydana gelen olaylar ve ardından gelen tepki, terörizm korkusunu arttırmış, sonuç olarak siber terörizm yeni bir düzleme taşınmıştır.[118] Yeni bir terör tehdidine karşı güçlü ve anlaşılır bir tepki oluşmuş ve ileri teknoloji saldırıları başlatma kavramı dendiğinde, siber terörizm nedir?[119] Özellikle batı dünyasındaki hükümetler genel olarak, Uluslararası Güvenlik ve İşbirliği Merkezi tanımına benzer bir "siber terörizm" anlamını kabul etmekte, buna göre Uluslararası Siber Suç ve Terörizm Sözleşmesi Önerisi başlıklı bir belgede "Meşru bir otorite tarafından tanınmamış kısıtlı kullanım veya tehdit siber sistemlere karşı şiddet, bozulma ya da müdahalede bulunma anlamına gelir; meğerki bu tür bir kullanım kişi ya da kişileri yaralama ya da ölümle sonuçlansın, toplumsal kargaşaya neden olsun, azımsanamayacak ekonomik zarar versin ya da fiziksel özelliklere zarar versin" şeklinde tanımlanmaktadır.[120] Bazı durumlarda, bu terimin, saldırının teröre sebep olup olmamasına bakılmaksızın bir ulus devletin çıkarlarına teröristler veya hükümet dışı kuruluşlarca saldırı olduğu durumlar anlamına gelmektedir.[121]

Siber terörizmi klasik anlamda terör eylemlerinin bilgisayar ve bilgisayar sistemleri kullanılarak icra edilmesi olarak tanımlamak mümkündür.[122] Dorothy Denning'in makalelerinde siber terörizmi: "Siber uzay ve terörizmin birleşimidir. Siber terörizm, siyasi ve sosyal mercilere ve kişilere gözdağı vermek, baskı oluşturmak maksadıyla resmi birimlerin bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır. Daha da ötesi, bir saldırının siber terörizm olarak tanımlanması için bireye ya da mala karşı şiddet içermesi gerekmekte, en azından "korku yaratacak kadar hasara" yol açmalıdır" şeklinde tanımlamıştır.[123] Siber terör ölümcül olan ya da fiziki hasara yol açan, şiddetli ekonomik kayba neden olan saldırılar olarak örneklenmektedir. Kritik altyapı odaklarına yapılan ciddi saldırılar yarattığı etkiye göre siber terörizm olarak tanımlanmaktadır. Önemli olmayan servislere verilen rahatsızlıklar siber terörizm olarak tanımlanmamaktadır."[124]

---

[117] Lech J. Janczewski ve Andrew M. Colarik, Managerial Guide for Handling Cyber-Terrorism and Information Warfare, Idea Group Publishing, The U.S.A, 2005, s.43.

[118] Andrew JONES, **Cyber Terrorism: Fact or Fiction**, Computer Fraud and Security, 2005, s.1.

[119] JONES, s.4.

[120] **A Proposal for an International Convention on Cyber Crime and Terrorism**, Ağustos 2000, http://www. iwar.org.uk /law/resources/cybercrime/stanford/cisac-draft.htm, (e.t.02.02.2012).

[121] JONES, s.4.

[122] Gizem Özkışlalı, **Küreselleşme, İnternet ve Terörizmin Değişen Yüzü; Siber Terörizm**, Yüksek Lisans Tezi, Ankara, 2008, s.70.

[123] Dorothy E. Denning, **Is Cyber Terror Next?**, Social Science Research Council, http://essays.ssrc.org/sept11/ essays/denn ing.htm, (e.t.02.02.2012).

[124] Türk Asya Stratejik Araştırmalar Merkezi, **Siber Terörizm Raporu**, Stratejik Rapor No: 2 Aralık 2004.

İleri teknoloji kullanımı ile terörizm, bu sorunu gidermek üzere yürürlüğe girmiş mevzuat olan Anti-terörizm, 2001 Suç ve Güvenlik Yasası, 2005 Terörizmi önleme Yasası ve ABD Yurtseverlik Kanunu, terör korkusunu etkilemek yerine yüksek teknolojinin kullanımı yoluyla terörizmi yansıtacak gibi görünmektedir.[125] Şu anda mevzuatta ele alınmayan konu bilgisayar teknolojilerinin kullanımı yoluyla terörizmin mümkün olup olmadığıdır.[126] Şu anda "siber" yetenekler ile birçok insanı korkutmanın tek yolu, onlara donanım yoluyla saldırı tehdidi yöneltmektir.[127]

Son dönemde yapılan ABD Kongresi Kongre Kütüphanesi Araştırma Merkezi'nin ortaya koyduğu sonuca göre, ABD bilgisayar sistemine koordine edilmiş büyük veya küçük çaplı EMP silahları ile kurgu bir saldırı yapılmasının teknik ustalık gerektirmenin yanı sıra terör örgütlerinin ötesinde bir kapasite gerektirmektedir.[128] Londra'da ABD Kongresi tarafından gerçekleştirilen Avrupa Kongre Kütüphanesi konferansına katılan Bruce Schneier, çağrı cihaz ağlarına zarar verme ve e-mail durdurmanın terör eylemi olamayacağını belirterek internetin kullanımını ve diğer iletişim ağlarını çökertmenin korkudan çok kızgınlığa yol açacağını belirtmektedir.[129] Aynı konferansta karşıt görüş belirten Lord Harris Haringey, Britanya'nın "elektronik 9/11" riski altında durduğunu, çünkü Kritik ulusal Altyapı'nın (CNI) birçok çalışan şirketlerinin elektronik saldırılara karşı en yüksek seviyede güvenlik unsurunu sürdürmek zorunda olduklarını iddia etmektedir.[130] Kritik Ulusal Altyapı'ların (CNI) bireysel unsur-

---

[125] JONES, s.1.

[126] Olaylara rasyonel olarak bakıldığında şu soru sorulmalıdır: bir bilgisayar aracılığıyla terör olayına neden olmak mümkün müdür? Eğer cevap evet ise, o zaman nasıl mümkündür? Şu anda bilgisayar teknolojisine o kadar bağımlı olunup olunmadığına dair büyük bir şüphe mevcuttur. Nüfusun büyük bir bölümünü kapsayan güç kaynağını etkilemenin teröre neden olacağı düşünülebilir mi? Bilgisayar kullanımı yolu ile demiryolu sisteminin devre dışı bırakılmasıyla kazaya sebep olmak bir terörist eylem olarak anlaşılabilir mi? Bu sorunun cevabı potansiyel olarak evet şeklinde verilebilir fakat kesinlikle bu durum ölçeğe ve bu kişi veya grubun isteğine bağlı olarak değerlendirilmelidir. Bkz. JONES, s.4.

[127] JONES, s.4. Bir teröristin güç kaynağını çökerttiğini düşünürsek, bu hareketin etkileri ne olur? Eğer sadece 2003 yılındaki olaylara bakarsak, en az ikisi Londra'yı, biri İsviçre'yi ve İtalya'nın belli bölgelerini, bir diğeri ABD'nin doğu yakasında 50 milyon insanı elektriksiz bırakan dünya çapında bir dizi elektrik kesintilerine kısmen bilgisayarların neden olduğu görülmekle birlikte, etkilenen bu insanlar üzerinde terörün hiçbir izine rastlanılmamıştır. Ayrıntılı bilgi için bkz. The Guardian, 15 Ağustos 2003, http://www.guardian.co.uk/news/200 3/aug/15/informer, (e.t.02.02.2012). 50 milyon insanı etkileyen bir güç ünitesinin kapatılırsa ve bu kişiler bu olayı zaman zaman yaşanabilen bir durum olarak kabul ediyorlarsa, terör yapmak için gerekli olan nedir? Çeşitli teknolojilere artan oranda bağımlı hale geldiğimiz yadsınamaz bir gerçek olmakla birlikte, insanların büyük çoğunluğu bu aletlerin arızalı olmaları veya yoklukları durumunun teröre neden olma kapasitesi olarak algılanmamaktadır. Bkz. JONES, s.1. Aslında bir diğer gerçek şudur; sadece herhangi bir bağımlılığa sahip en gelişmiş uluslar hem ilk hem de en çok etkilenen olmaktadır; örneğin Afganistan'ı ele aldığımızda yüksek teknolojiye bağımlılık oldukça düşüktür. Bunun sonucu olarak siber teknolojinin kötüye kullanılması sonucunda Afganlar neredeyse hiç etkilenmemiş olacaktır. Bkz. JONES, s.4.

[128] Clay Wilson, **Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress**, CRS Report for Congress, Order Code RL32114, s.5, http://fpc.state.gov/documents/organization/45184.pdf, (e.t.02.02.2012).

[129] JONES, s.2.

[130] Graeme Wearden, **Cyberterrorists poised to attack', warns Labour peer**, 28 Nisan 2005, http://www.silic on.com/tech nology/security/2005/04/28/cyberterroristspoised-to-attack-warns-labour-peer-39129961/, (e.t.02.0 2.2012). 2004 Ağustos

ları potansiyel saldırılara karşı savunmasız olduğu konusunda hiçbir şüphe bulunmamaktadır.[131]

Kritik sistemlerin çökertilmesi durumunda, bu durumun sorumluluğunu kimin taşıyacağı belirsizdir. Açıktır ki elektronik saldırının kaynağını kesin olarak belirlemek özellikle kısa dönemde çok zordur.[132] Fiziksel bir saldırıda, kurşun ve bomba ile yürütülen büyük fiziksel yıkımların onarımı veya zarar gören altyapının yenilenmesi zaman almaktadır; fakat, bir siber saldırıda, fiziksel bir zararın oluşması muhtemel görünmemekle birlikte (nükleer santrallere yapılacak hackleme faaliyetleriyle kritik duruma yol açmak gibi örnekler hariç olmak üzere) kontrol sistemlerinin her şeyden önce dış dünya ile bağlantılı olmaması ve ikinci olarak her şeyi kapsayan güvenlik sistemlerinin bunları engellemesi umut edilmektedir.[133] Altyapısal fiziksel imha eksikliğinin anlamı, herhangi bir siber saldırının etkisini belirli bir süre devam ettirmek oldukça zor gibi görünmekle birlikte verilen zararın ilgili otoritelerce eski haline veya eski haline yakın bir şekle döndürülmesi realistik bir zaman aralığında mümkündür. Suçlular finansal bir fırsat görürse, sistemler için bir tehdit olacaktır, fakat bu insanları terörize etmek veya devleti karıştırmaktan çok, karla ilgili olacaktır.[134]

Son 20 yıldır yaygın komünikasyon sistemlerinin desteği ve telekomünikasyon ve bilgisayar teknolojileri tarafından ticari faaliyetlerdeki küreselleşmenin arttığı görülmekte, bu durumun en önemli etkisi ulusal sınırların birçok durumda mantıksız ve anlamsız olması gibi birçok önemli etkileri mevcuttur.[135] Terörizmin doğasında önemli bir değişiklik olduğu görülmektedir. Geçmişte terörist grupların nispeten yerel hedefleri, dağınık grupların birbirleriyle işbir-

---

ayında Kaspersky Laboratuarları'ndan Eugene Kaspersky, Rusya haber ajansı servisi RIA Novosti'nin İslami teröristler tarafından büyük ölçekte bir "elektronik cihat" saldırısının olabileceği uyarısında bulunmuş, saldırının ABD, İsrail ve Batı Avrupa ülkelerindeki politik ve finansal web sitelere karşı hedef aldığını savunmuş, bu saldırı tehdidi bu vesilelerin aracılığıyla başarısız olduğunu belirtmiştir. Daha fazla bilgi için bkz. John Leyden, 'Electronic Jihad' fails to materialise, 26 Ağustos 2004, http://www.theregister.co.uk/200 4/08/26/cyberfu d/, (e.t.02.02.2012).

[131] JONES, s.2.

[132] **Information Assurance – the Achilles' Heel of Joint Vision 2010?**, 2 Mart 1999, http://www.airpower.au. af.mil/airchr onicles/cc/ashley.html, (e.t.02.02.2012). Detaylı olarak hazırlanmış 1998 yılı Şubat ayında geçekleşen örnek bir olay olarak gösterilebilecek "Solar Sunrise" saldırısının aynı zamanda ABD Savunma bilgi Altyapısı bir sonraki saldırısı için bir hazırlık göstergesi olarak algılanmış, bu dönemde ABD Hava Kuvvetleri Körfez'deki potansiyel operasyonlar için seferber olarak mevcut kaynakların tümü kullanılarak, bu saldırıyı belirlemek 17 gün sürmüştür. Başlarda gönderilme noktaları olarak İsrail, Birleşik Arap Emirlikleri (BAE), Fransa, Tayvan ve Almanya düşünülmekteyken, aslında Kaliforniya'daki Cloverdale eyaletindeki 2 genç tarafından idare edildiği ortaya çıkarılmıştır. Bkz. JONES, s.2

[133] JONES, s.5.

[134] JONES, s.6. Radikal İslam örgütlerine göre bu yeni tip terörizm, "Siber-Cihat" olarak adlandırılmaktadır. Ayrıntılı bilgi için bkz. Shaul Shay, Netwars and Networks, Mark Last ve Abraham Kandel (editör), Fighting Terror in Cyberspace içinde (33), World Scientific Publishing, The U.S.A, 2005, s.33. Haziran 2002'deki, Washington Post gazetesi haberine göre; Afganistan mağaralarında bulunan bilgisayar disklerinde El-Kaide'nin A.B.D bilişim altyapısını hedef aldığı ortaya çıkmış, Suudi Arabistan, Endonezya ve Pakistan'daki anahtarları kullandıkları ve acil telefon sistemlerini, elektrik hatlarını, su kaynaklarını ve dağıtımını, nükleer enerji santrallerini ve gaz tesislerini inceledikleri belirtilmiş; ayrıca, enerji, su, taşıma ve iletişim klavuzları sağlayan yazılım programlarının yer aldığı sitelerde dolaştıkları belirlenmiştir. Bkz. POWER ve FORTE, s.17.

[135] JONES, s.6.

liği yaptığı ve birbirlerini desteklediklerine dair açık kanıtlar mevcuttur ve bir ulus devlet ya da yerel bölgesel bazlı amaçları bulunmuştur.[136] Aktif olan terörist grupların büyük bir çoğunluğu, farklı niyetlere sahiptir. Köktendinci terörizmin artması çok önemli bir değişime neden olmakta ve batı dünyası önemli değişik değerlere sahip bireyler veya gruplarla başa çıkmaya çabalamaktadır.[137] Batı kültürü nasıl tamamen değişik değerlere inanan ve kendilerini inançları uğruna ölmeye gönüllü bu kişilerle nasıl başa çıkacaktır? Bu durum dikotomik bir ayrımı ortaya koymaktadır. 1900'lerin ortalarında Geçici İrlanda Cumhuriyet Ordusu (PIRA) gibi terörist grupların teknik kapasitesi ve Birleşik Krallık Kritik Ulusal Altyapı gibi bir anlayış ile siber saldırılar yürütebilecek iken öyle yapmayı tercih etmemişler, arzu ettikleri tanıtımı başarmışlar ve sonraki gün İngiltere'de hükümete baskı, mermi ve bomba kullanmak suretiyle şehir merkezlerinin zarar görmesi caddelerde bulunan vücut parçalarını gören halkın tepkisiyle gerçekleşmiştir fakat grafiksel gösterilerle hükümet üzerinde aynı seviyede bir baskı gerçekleştiremezler.[138] Terörist örgütlerin; mesajlarını açıklamak, propaganda yapmak, haberleşmek ve bilgi saklamak için siber teknolojileri kullanacağına dair hiç şüphe yoktur. Ayrıca, kombine bir operasyonun parçası olarak fiziksel bir saldırı gerçekleştirmek için siber saldırı kullanacaklardır, fakat bu seviyede bir etkinin genel nüfus üzerinde doğrudan fiziksel saldırı oluşturabilmesi için daha zamana ihtiyaç vardır. Siber saldırıda fiziki bir bölgeye saldırmaya ve silah ya da patlayıcılara sahip olmaya gerek olmadığından, bu işi yapan biri yakalandığında, delillerin toplanması ve korunması ayrıca hâkim ve jürinin teknik konulardaki sınırlı bilgisi nedeniyle mahkûm olma olasılığı çok düşüktür. Bu türün 1990'larda potansiyel teröristler tarafından kullanılması cazip olsa bile, bu teröristler bizim korkmamız gereken teröristler olduğunu göstermez, bu yol kendi ölümlerine yol açacak bir sebep haline gelmektedir.[139]

7. BARIŞI KORUMA SİBER SAVAŞI VE SİBER SAVAŞIN KURALLARI

Dünyanın bazı bölgelerinde siber savaşın yoğunluğu giderek daha da artmakta olduğundan Çin ve Tayvan silahlı kuvvetlerinde, siber savaşa adanan bağımsız birimler kurmuşlardır.[140] Son dönemde yaşanan olaylar siber savaşın, sınırların ötesindeki savaşçılar tarafından etkilerinin daha da kötüleştiğini göstermektedir.

Bilgi Savaşı ya da Info Savaş terimi, 1976 yılında Pentagon Değerlendirme Direktörü Andrew Marshall tarafından yönetilen bir grup stratejist tarafından ortaya konmuştur.[141] Bu kavram şimdiki askeri, teknolojik ve profesyonel bülten, konferans ve workshoplardan önce, 90'ların başında hem popüler

---

136 JONES, s.7.

137 JONES, s.6.

138 **Security for the Next Generation**, The National Security of the United Kingdom, Güncelleme:2009, Cabinet Office, Haziran 2009, s.41, http://www.official-documents.gov.uk/document/cm75/7590/7590.pdf, (e.t.02.02.2012).

139 JONES, s.7.

140 Thomas P. Cahill, Konstantin Rozinav ve Christopher Mule, **Cyber Warfare Peacekeeping**, Proceedings of the 2003 IEEE Workshop on Information Assurance United States Academy, ISBN 0-7803-7808-3/03, 2003, s.100.

141 Peter Schwartz, **Warrior in the Age of Intelligent Machines**, Wired Magazine, Nisan 1995, http://www.wir ed.com/wire d/archive/3.04/pentagon_pr.html, (e.t.02.02.2012).

hem de akademik anlamda gelişmeye başlamıştır.[142] Siber savaşı bilgi savaşından ayırmak çok daha karmaşık bir konudur. Ulusal Savunma Üniversitesi'nden Martin Libicki 1995 yılında Siber Savaşı şu şekilde tanımlamıştır: "Yedi şekildeki bilişim savaşı, siber savaştan biri – bilgi terörü, semantik saldırılar, simula-savaş ve Gibson savaşı içeren geniş bir kategori – açıkça en az derecede çözümlenebilir olandır çünkü şimdiye kadar en hayali olma durumundan dolayı, bir bütün olarak bilişim savaşının derecesi farklılık gösterir".[143] Global bilgi altyapısı bu türdeki savaşçıları mümkün kılacak şekilde evrimleşmektedir. Altyapı, bu tür saldırıları mümkün kılacak şekilde hiç evrimleşmeyebilir. Libicki ise, bu altyapı ve saldırıları "*hacker* savaş" ya da "sibersavaş" olarak tanımlamaktadır.[144]

Alford'a göre; "Siber Savaş (CyW) –Bir rakibi zorlamak üzere, rakibin sistemi içinde kontrol yazılımlara karşı yürütülen, milli iradeyi yerine getirmek üzere yapılan eylemdir. CyW şu şekilleri içermektedir: siber filtreleme, siber manipülasyon, siber saldırı, siber baskın. Siber savaş: "Uluslararası siber aktörler – kasten siber savaş yöneten bireyler (siber operatörler, siber birlikler, siber savaşçılar, siber güçler) tarafından yürütülmektedir. Kasti olmayan siber savaş saldırılar –siber aracılığıyla yapılanın anlamı, ulusal güvenliği etkileme amacı taşımayan saldırılardır (siber suç)."[145]

Çin, PLA birimlerinin oluşumu da dâhil olmak üzere, özelikle PLA birimlerince, 1993 yılından beri siber savaşlara odaklanmıştır.[146] Çin, Tayvan'a askeri çalışma amaçlı simule siber saldırılar yürütürken, cevap olarak Tayvan ise Group Tiger Information Warfare birimini oluşturmuş, böylece Çin ve Tayvan hakkında iki siber uzay arasında "Sanal Keşmir" yarattıkları ifade edilmektedir (Hindistan ve Pakistan arasındaki ihtilaflı Keşmir toprakları gibi).[147]

Parks ve Duggan DARPA sözleşmesi altında tecrübelerini Sandia Ulusal Laboratuvarları'nda tecrübe ederek, Sandia Ulusal Laboratuvarları Kırmızı Takım Enformasyon Tasarım Güvencesi (IDART) altında geleneksel savaşlara göre ilkeler belirlemişlerdir.[148] Siber savaşta:

1) Eylemlerin kinetik etkileri olmalıdır (Kinetik).

2) Siber dünyada gizlenmek üzere aktif adımlar atmak mümkün fakat kimsenin bakmamasına rağmen yapılan şey görünürdür (Gizleme ve Görünürlük).

3) Siber dünyada davranışı değiştiren yasalar mevcut olmamasının istisnası, değişim için fiziksel dünyada hareket gerektirmektedir (Değişkenlik).

---

[142] **Proceedings of European Conference on Information Warfare and Security 2002, 2003**, http://books.goo gle.com.tr/b ooks?hl=tr&id=EVsPIeM4w5AC&q=cyber#v=onepage&q=conferences&f=false, (e.t.02.02.2012).

[143] Martin Libicki, **What is Information Warfare**, Strategic Forum 28, Institute for National Strategic, Studies, Mayıs 1995, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394692, (e.t.02.02.2012).

[144] CAHILL, RAZINOV ve MULE, s.101.

[145] Lione1.D. Alford, **Cyber Warfare: A New Doctrine and Taxonomy**, CrossTalk: The Journal of Defense Software Engineering, Vol. 14 No. 4, Nisan 2001, http://www.ldalford.com/technical_writing.htm, (e.t.02.02.2012).

[146] Qiao Liang ve Wang Xiangsui, **Unrestricted Warfare**, Beijing: PLA Literature and Arts Publishing House, Şubat 1999, http://cryptome.org/cuw.htm, (e.t.02.02.2012).

[147] CAHILL, RAZINOV ve MULE, s.101.

[148] Raymond C. Parks ve David P. Duggan, **Principles of Cyber-warfare**, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5–6 Haziran 2001, s.122, http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf, (e.t.02.02.2012).

4) Siber dünyada; otoriter, erişimci ya da bir saldırganın sergilemek istediği eylemi sergileyen bir eylem yeteneğine sahip bir varlık mevcuttur. Saldırganın amacı bu sahte tavırla hareket eden kimlik ile eylemde bulunabilmektir (Sahte Tavır).

5) Silahlar çift kullanımlıdır (Çift Kullanımlı Silah).

6) Savunmacı ve saldırgan kullandıkları siber uzayın çok küçük bir bölümünü kontrol etmektedir (Bölme).

7) Siber uzayın bir bölümünü kontrol edebilen bir kişi, rakibi de kontrol eder (gasp).

8) Siber uzay tutarlı ya da güvenilir değildir (güvenilmezlik).

9) Hedeften fiziksel uzaklık önemli değildir (yakınlık).[149]

Alford, siber savaşı sadece iki kural ile tanımlar: "…Veri kabul eden herhangi bir yazılım kontrol sistemi teorik olarak gizlice sistemin filtrelenmesi sonucu saldırıya uğrayabilir. Bunun anlamı veri kabul eden her sistemin savunmasız olduğudur. Temelde siber sistemlere sızmanın iki yolu mevcuttur: fiziksel ve sinyal verileri... Her yazılım kontrol sistemine siber filtreleme amaçlı bir teşebbüs beklenmektedir."[150]

İlk olarak, saklanmak ve sahte tavır takınmak Devletin Ulusal Siber Savaşı'nda hazırlık için ve gizli eylemlerin başında gelen iki önemli adım iken, ikinci olarak, tüm siber uzayın ötesinde karşı tarafın tüm siber alanına ulaşana kadar, saldırganlar ve savunucular önemli ölçüde büyük bölünmelerle başa çıkmalıdır.[151] Üçüncü olarak, Alford'un ikinci tanımı geliştirilirse: "…Tüm yazılım kontrol sistemlerinin simultan siber filtrelemelerin hedefi olması beklenmektedir." Somali, Bosna ve Ruanda'daki başarısız tecrübeler ve özellikle Sierra Leone ve Batı Timor'daki BM personelinin öldürülmesi barışın sürdürülmesi kavramını değişikliklere uğramıştır. İngiltere, "Barışı Destekleme Operasyonları" (PSO) konseptini geliştirerek "Kuvvetli bir şekilde Barışı Sürdürme" kavramına dönüştürmüştür.[152]

Barışı Koruma Siber Savaşı Kurallarına bakıldığında; barışı sürdüren siber savaş kavramı ve barışı sürdüren kinetik savaşın ayrıldığı noktalar: Siberuzayda mümkün mertebede etkili ve serbest kullanımda, bir siber savaş sonunda tüm savaşçıların verilmesiyle sona ermektedir. Kinetik savaşta savaşçılar, "sahipsiz toprak" ve "Tampon Bölge" şeklinde ayrılmakta iken, Siber barışta, önceki savaşçılar siber uzayın genelinde bir başkasıyla hala etkileşimde olmalıdır.[153]

8. SALDIRIYA HAZIRLIK VEYA SAVUNMA AMAÇLI ZORUNLU ASKERLİK VE SAVAŞÇI STATÜSÜ

Siber saldırılar kaynağı, niyeti, alanı ve süresi açısından belirsiz olduğundan, ileriye yönelik zorunlu siber askerliğin olabilirliğini varsaymak makul görülmektedir. Bu durum, saldırıların doğasına dikkat çekmektedir: 2007 yılında Estonya'da yaşananlar temelinde ve benzer saldırılar; kinetik savaşın karakterindeki sürekli saldırıların tersine, siber saldırıların nispeten sınırlı bir

---

[149] CAHILL, RAZINOV ve MULE, s.101.

[150] Lione1.D. Alford, **Cyber Warfare: A New Doctrine and Taxonomy**, CrossTalk: The Journal of Defense Software Engineering, Vol. 14 No. 4 Nisan 2001, http://www.ldalford.com/technical_writing.htm, (e.t.02.02.2012).

[151] CAHILL, RAZINOV ve MULE, s.102.

[152] CAHILL, RAZINOV ve MULE, s.102.

[153] CAHILL, RAZINOV ve MULE, s.103.

süre için olacağı varsayımına götürmektedir.[154] Bu varsayımlar birçok faktör tarafından temellendirilmektedir; kinetik savaşçıların aksine siber savaşçılar fiziksel olarak hedef devletin bölgesinde bulunmak zorunda değil; kinetik saldırılar belirli bir hedefe ulaşmak için sıfır toplamlı bir mücadelenin parçası olduğundan uzun olma eğilimindedirler.[155] Siber saldırganlar faaliyetlerini uzaktan gerçekleştirir ve çok farklı hedeflere sahip olabilir.[156] Her ne kadar siber saldırı eyleminde bulunacak kişiler farklı hedeflere sahip olabilirse de, 1977 tarihli Ek 1 No.lu Protokol'ün 52. maddesindeki askeri hedef dışındaki tüm hedeflerin sivil sayılmakta olduğu hükmü hatıra gelmektedir.[157] Bir saldırı veya saldırılar serisi kendi başına amaç olabilir, örneğin saldırganların amacı sadece belli süre için hedeflenen sistemleri devre dışı bırakmak olabilir, bu şekilde saldırganlar, yeteneklerini ve/veya mağdur devletin bu tip saldırıları önleme yetersizliğini, bir devletin güvenliğini baltalayabildiğini göstermek istemekte, bu ve benzeri sebepler nedeniyle, gereken bir kuvvet olarak zorunlu uygun siber askerlik modeli, ihtiyaç duyulduğunda eğitimli ve aktifservis denilen "milli muhafız" ya da "rezerv" güçler oluşmasını gerekli kılmaktadır. Siber Savunma Ligi'nin (CDL) bu ihtiyaç duyulan modeli karşılayabileceği görülmektedir.[158]

Siber çatışmanın doğasında askeri rezervleri harekete geçirmek için uygun kriterlerin belirlenmesi bir sorundur ve zorunlu siber askerler, devlet destekli bir saldırı olduğuna dair açık bir kanıt yoksa harekete geçmemelidir fakat tecrübeler göstermektedir ki; saldırının gerçek destekçisi ve kaynağı saldırı bittikten uzun süre sonra da belirsiz kalmakta, bu nedenle ulusal muhafızlar veya milis kuvvetler iç yasaların uygulanması veya iç huzursuzlukları bastırmak için kullanılmalıdır.[159] Siber savunmaya bu yaklaşımın uygulanmasıyla, zorunlu rezerv askerlerin eğer kamu düzenini bozabilecek önemli bir kanıt mevcut ise harekete geçirilmesi önerilebilirken, rezervistler tek potansiyel kayıpların ekonomik olduğu durumlarda; örneğin büyük e-ticaret sitelerine saldırı gibi, saldırılara karşı savunma amaçlı harekete geçmemelidir. Yaşamı ve sağlığı tehlikeye atan durumlarda; örneğin enerji nakil hatları, su kaynakları, sağlık tesisleri gibi alanlara yapılan saldırılarda aktivite edilmelidir.[160]

Zorunlu askerliğe IT personelinin alınması, eğitim ve iş tecrübesi bilgileri yanında, çeşitli alanlara, yazılıma ve endüstri alanına aşinalık gibi çok daha detaylı bilgilerin bilinmesi gerekeceğinden, bu seçim sürecinde devletin payına, daha çok çaba ve planlama düşeceği anlamına gelmektedir.[161] Siber saldırıların doğası, IT (*Information Technology*) yapılarını etkileyecek belirli seviyede bir uzmanlık ve belirli sektörlerde de deneyim gerektirmektedir. Örneğin, Finansal kurumlar tarafından çalıştırılan IT uzmanları, elektrik şebekesi saldırılarına karşılık verecek bilgiye sahip değildir. Hızlı ve etkili bir savunma, sistem di-

---

[154] Susan W. Brenner ve Leo L. Clarke, **Conscription and Cyber Conflict: Legal Issues, 3rd International Conference on Cyber Conflict**, CCD COE Publications, Estonia, 2011, s.2.

[155] BRENNER ve CLARKE, s.2.

[156] BRENNER ve CLARKE, s.3.

[157] **Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977,** http://www.icrc.org/ihl.nsf/FULL/470?O penDocument, (e.t.14.02.2012). Ayrıntılı bilgi için bkz. TÜTÜNCÜ, s.82.

[158] BRENNER ve CLARKE, s.3.

[159] BRENNER ve CLARKE, s.3.

[160] BRENNER ve CLARKE, s.3.

[161] BRENNER ve CLARKE, s.4.

zaynı ve bunun sürdürülmesini sağlayan parçaları yapan kişiler yerine, asker olarak bu kişilere ihtiyaç duyulmaktadır.[162]

CDL, Savunma Ligi'nin parçası olduğundan, CDL üyeleri devletlerdeki milli muhafız ordusu veya rezerv kuvvetlerdeki gibi bir statüye sahip oldukları kabul edilmelidir. CDL üyeleri, diğer ülkelerde kurulmuş benzer birimler gibi, 3. Cenevre Konvansiyonu m.4'te belirtildiği üzere tahminen savaşçı olarak nitelendirilmektedir.[163] CDL türünde siber rezerv kuvvetleri, göreve çağrıldıklarında savaşçı olarak kabul edilecektir ve eğer olmaz ise savaşçı olmayan sivil statüsüne sahip olacaklardır. Yani, CDL türündeki siber rezerv kuvvet üyesi göreve çağrıldığında savaşçı statüsünde olacaktır.[164]

IT altyapı sahiplerinin siber savunma birlik üyelerinin saldırılara vereceği karşılıkta kullandıkları mal varlığının uluslararası hukuktaki statüleri temel bir konuyu oluşturmakta ve bu kategoride yer alan birey ve şirketlerin çoğu zorunlu askerlerin işvereni olmakta, böylece CDL şeklindeki aktif siber şirketler savaş hukukuna göre savaşçı statüsündedir.[165] Buradaki sorun bu işverenlerin statüsünün aynı olup olmayacağıdır. Cenevre Konvansiyonlarına Ek 1 No.lu Protokol'de, sivillerin muhasamatta doğrudan yer almaları durumunda, savaşan devletler arasında bireylerin muhasamatın yönetilmesinde açıkça eylemde bulunmalarının, savaşçı olmama durumlarını kaybettikleri yer almaktadır.[166] Sadece savaş araçları üretmek doğrudan katılım anlamına gelmemekte, fakat zorunlu askerin sadece savunma amaçlı olsa da işverenin IT varlığını silah olarak kullanılması, bir saldırıya karşı savunma, sadece silah üretimi olarak yorumlanmamalıdır.[167] Herhangi bir siber savaş çabasında muhasamata doğrudan katılma kavramında başka bir katılımcıyı ortaya çıkarır: Internet Servis Sağlayıcılar (Internet Service Providers/ISPs), siber saldırıların ve siber şirketlerin karşı saldırıları ticari ISP'lerce iletilir, fakat ISP'lerin siber düşmanlıklarda doğrudan yer alabilmesi konusu tartışmalıdır, bazıları ISP'lerin rolünün düşman hedeflerini bombalayan askeri uçakları kullananlarla eşdeğer görmektedir.[168]

9. ULUSLARARASI İNSANCIL HUKUK BAĞLAMINDA HACKLEME

Siber savaş, açık bir şekilde uluslararası hukukta yer almayan, gelişmekte olan bir savaş türü olması dolayısıyla, kimileri siber savaşın hukuki kısıtlamaya tutulması fikrindeyken, bu yeni çatışma şekline Uluslararası İnsancıl Hukukun nasıl uygulanacağı konusunda bir fikir birliğine varamamakta ve savaş suçu suçlamaları riskine rağmen, devletlerin siber savaşların yasaklanması adına güçlü teşvikleri bulunmaktadır.[169] Birçok siber savaş kaçınılmaz

---

[162] BRENNER ve CLARKE, s.4.

[163] **Geneva Convention Relative To The Treatment Of Prisoners Of War of 12 Ağustos 1949** (Geneva Convention III), http://protection.unsudanig.org/data/legal/Third%20Geneva%20Convention%20 (POW), %2019 49.pdf, (e.t.02.02.2012).

[164] BRENNER ve CLARKE, s.4.

[165] BRENNER ve CLARKE, s.7.

[166] **Protocol Additional to the Geneva Conventions of 12 Ağustos 1949, and Relating to the Protection of Victims of International Armed Conflicts** (Protocol I) Article 50, 8 Haziran 1977, 1125 U.N.T.S.3., http://treaties.un.org/doc/Publication/UNTS/Volume%201125/volume-1125-I-17512-English.pdf, (e.t.06.02.2012).

[167] Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Yves Sandoz (editör), 1987, s.619.

[168] BRENNER ve CLARKE, s.8.

[169] KELSEY, s.1427.

olarak tarafsızlık kanunlarını, bu ihlalleri konvansiyonel savaşlara göre siber çatışmaların olasılığını arttırarak ihlal edebilir.[170]

1999 yılında NATO'nun Yugoslavya'ya karşı yürüttüğü kampanya sırasında siber savaşı kullanmasının tedirginliği, bilgisayar ağı yoluyla yapılan saldırıların belirsizliğinin insancıl hukukla nasıl bağlantılı olduğu sorusunu kanıtlar niteliktedir.[171] Bilgisayar ağı yoluyla yapılan saldırılara var olan kuralları uygulamak üzere, çeşitli terimlerin yorumlarını kabul etmek gerekir. En önemlileri, "silahlı çatışma" ve "saldırı" kavramlarının sonuç tabanlı yorumlarıdır.[172]

Olası siber çatışmalar, Uluslararası İnsancıl Hukukun var olan kurallarına bağlı olarak tarafsızlığı, ihaneti, farklılığı ve insancıllığı içeren yasal ve stratejik zorlukları ortaya çıkarmakta, bu kavramlardan hiçbiri eksiksiz ve tam anlamıyla belirtilmiş veya çözülebilmiş olmasa da, bu kavramların tümü siber çatışmaların bazı yönlerinin hukuk alanında ne kadar sorunlu olabileceğini göstermektedir.[173] Eğer devletler etkili bir şekilde ICT ağlarının geçişini sağlayan data paketlerini ya da hava sahalarına nüfuz eden elektromanyetik dalgaları izleyemez veya kontrol edemez ise, siber çatışmalara uygulanmadan önce tarafsızlığın geleneksel düşüncesine dönülmüş olunacaktır.[174] Normalde, savaşçıların yansız bir devletin bölgesini kullanarak silah konuşlandırması ya da silahlı saldırı başlatması yasaktır."[175] Dahası, bir devlet yansızlığını tarafsız kalarak sadece sürdürmektedir. Eğer bunlar egemen topraklar olarak kabul edilirse, "savaşçıların yansız kuvvetin bölgesi üzerinden askerlerini ya da savaş malzeme ve mühimmat konvoylarını geçirmesi yasaklanmıştır. Ancak kısmi ya da tam bir müşterek olma durumunda, savaşçılara ait bir kuvvetin yansızlığı etkilenmez."[176] Bilgi silahlarının yabancı ICT ağlarını iletme analojisi açık iken, uygun hukuki bir norm açıklıktan oldukça uzaktır, çünkü yansızlığın geleneksel kavramsallığı izlenebilir eylemlere ve olayın geçtiği yerin hukuki statüsü üzerinde hemfikir olunmasına göre değişmektedir. Uluslararası İnsancıl Hukukun uzun soluklu başka bir ilkesi, ihanetin yasaklanmasıdır. "Silahlı çatışmalara uygulanan uluslararası hukuk koruması, güvene ihanet niyetiyle muhalifin güvenini kazanma amacında olan eylemler, anlaşma yapmaya yetkisi olduğuna ya da anlaşmaya zorunlu olduğuna onu inandırır." [177] Siberuzayın problemli doğasının özelliği, yasal savaşçı eylemleri (dost veya düşman olması fark

---

[170] KELSEY, s.1427.

[171] Bradley Graham, **For a description of hesitancy to use CNA during Operation "Allied Force", "Military Grappling with Rules for Cyber Warfare: Questions Prevented Use on Yugoslavia"**, Washington Post, 8 Kasım 1999, s. A1, http://www.washingtonpost.com/wp-srv/WPcap/1999-11/08/011r-110899-idx.html, (e.t. 05.0 1.2012).

[172] Michael N. Schmitt, **Wired warfare: Computer network attack and jus in bello**, RICR Juin IRRC Haziran 2002 Vol. 84 No. 846, s.397, http://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf, (e.t.08.08.2011).

[173] KANUCK, s.1592.

[174] KANUCK, s.1593.

[175] Convention Conceming the Rights and Duties of Neutral Powers in Naval War, madde 10, 18 Ekim 1907, http://www.icr c.org/ihl.nsf/FULL/240, (e.t.11.02.2012).

[176] Convention Conceming the Rights and Duties of Neutral Powers in Naval War, madde 10, 18 Ekim 1907, http://www.icr c.org/ihl.nsf/FULL/240, (e.t.11.02.2012).

[177] **Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts** (Protocol I), 8 Haziran 1977, madde 37–39, http://www.icrc.org/ihl. nsf/full/470?opendocu ment, (e.t.07.02.2012) ve **Convention (III) relative to the Treatment of Prisoners of War**. Geneva, 12 Ağustost 1949, madde 4 (A) (2), http://www.icrc.org/ihl.nsf/FULL/375, (e.t.07.02.2012).

etmez) ve sivillerin eylemlerinin neredeyse ayrılmasını imkânsız kılmakta, ayrıca bilişim silahlarındaki askeri amblemlerle eşdeğer olmaksızın, ayrım ilkesine ve ihanete karşı yasaklamaya bağlı kalmak son derece zor olmakla birlikte stratejik bir perspektiften, Uluslararası İnsancıl Hukukun ihaneti, hainliği ve cesareti içeren prensipleri, şiddetli çatışmalar süresince belirli insancıl eylemlerin mümkün kalmasını temin etmektedir.[178] Bunlar olmadan, kaynak ve yardım verilemez, teslim olma inandırıcı olmaz ve ateşkes anlamsız hale gelmekte, siber çatışmaları hava savaşı ile karşılaştıran askeri stratejistler, Uluslararası İnsancıl Hukukun tarihinde de bu prensiplerin uygulanması için çalıştığını bilmekte, ayrımın ve ayrımcılığın prensipleri ayrıca egemenlerin savaş tehlikelerinde sivil varlıkları korumak için önlem almasını da içermektedir.[179] Dahası, belirli noktalardaki sivillere karşı ya da askeri operasyonlardan bağışık alanlarda kullanılması yasaklanmıştır.[180] Modern ICT ağları bağlamında hukuki sorumluluk da neredeyse anlamsız olmakta, eğer Uluslararası İnsancıl Hukuk hükümet ve askeri kuruluşun kendilerine ait bilgi altyapılarını kurması ve kullanmasını gerektireceği şeklinde yorumlanmazsa, kilit askeri hedeflerin paha biçilemez sivillerle birlikte kullanımı kaçınılmaz olacaktır; sonuç olarak, askeri komutanların, gereklilik ve orantılılık ilkeleri bağlamında hangi seviyedeki ikincil (ek) zararın değerlendirmesi hâkime kalacaktır.[181]

9.1. Hukuk Kurallarının Önemi ve Uluslararası Andlaşmalar

Suçun önlenmesinde hukuk kurallarının öneminin ve suç teşkil eden davranışa karşı uygulanacak yaptırımın önceden belirlenmiş olmasının, suçun işlenmesindeki caydırıcılık açısından önemli olmakla birlikte, siber suçlara ilişkin evrensel hukuk kuralları henüz oluşmadığından bu alanda sorunlarla karşılaşılması oldukça muhtemeldir ve örgütlü siber suçlara bakıldığında, bu suçların genel olarak, bu suçları hukukunda barındırmayan ya da çok az değinen, caydırıcılık özelliği olmayan ya da çok hafif olan ülkelerde işlendiği görülmektedir.[182]

Siber suçlar işlendiği takdirde, bu faaliyetlerin çok güçlü yaptırımlarla karşılanacağının açıkça belirtildiği ülkelerde, suçun oranının düşmesi oldukça olasıdır, ancak devlet desteğiyle başka bir devlete karşı işlenen siber suçlar bu konuda sorun teşkil etmektedir ve belki de hukukun ilerlemesine engel olmaktadır; örneğin Doğu Avrupa ve Rusya zayıf sibersuç hukukları sebebiyle bilgisayar suçlarının işlenmesine ortam sağlamaktadırlar.[183]

Savaşta, siber silahların kullanımının sınırlandırılması uygulamaları üzerine genel bir konsensüs sağlanması ile birlikte, askeri stratejistler son on

---

[178] KANUCK, s.1594.

[179] **Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts** (Protocol I), 8 Haziran 1977, madde 58, http://www.icrc.org/ihl.nsf/ full/470?opendocument, (e.t.07.02.2012).

[180] **Convention (IV) relative to the Protection of Civilian Persons in Time of War**, Geneva, 12 August 1949, madde 28, http://www.icrc.org/ihl.nsf/full/380, (e.t.07.02.2012) ve **Protocol Additional to the Geneva Convent ions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts** (Protocol I), madde 51 (7), 8 Haziran 1977, http://www.icrc.org/ihl.nsf/full/ 470?opendocument, (e.t.11.02.2012).

[181] KANUCK, s.1595.

[182] P. Williams, **Organized crime and cybercrime: synergies, trends, and responses**, 13 Ağustos 2001, Office of International Information Programs, U.S. Department of State, http://usinfo.state.gov, (e.t.05.01.2012).

[183] KSHETRI, s.548.

yıldır siber savaşların potansiyel tehditlerinin ve fırsatlarının farkında olmasına rağmen uluslararası toplum bu yeni türdeki çatışmaya Uluslararası İnsancıl Hukukun nasıl uygulanabileceğine dair konsensüs henüz sağlanamamıştır.[184] Bazıları var olan Uluslararası İnsancıl Hukuk kurallarının siber savaşın yeni paradigması ile başa çıkamayacağını ve bunun kullanımını düzenleyecek yeni bir uluslararası konvansiyona ihtiyaç olduğunu belirtmektedir.[185] ABD hükümetinin de dâhil olduğu diğer çalışmacılar, yeni bir andlaşma oluşturma çabalarına karşı çıkmakta ve mevcut İnsancıl Hukuk çerçevesinin benzetme yoluyla siber savaşa uygulanabileceğini savunmaktadır.[186] Yeni bir andlaşma yapılmasına karşı olan argümanlar, oldukça etkilidir. George K. Walker: "…teknolojinin değişkenliği ve üssel büyümesi, siber savaş durumlarında şimdiye kadar uygulamanın göreceli eksikliği ve dünya çapında elektronik arena da nispeten az sayıdaki iddia ve karşı iddialar bağlamında siber savaş üzerinde herhangi bir uluslararası antlaşma muhtemelen mürekkebi kurumadan donanım ve uygulamış açısından eskimiş olurdu" açıklamasında bulunmuştur.[187] Uluslararası İnsancıl Hukuk, karşılaştırma (benzeşim) yolu ile siber savaşa uygulanabilir fakat Uluslararası İnsancıl Hukukun bu durumu karşılaması için gelişmesi ve bazı durumlarda geleneksel savaşlardan ziyade siber savaşları teşvik etmesi gerekmektedir.[188]

9.2. Uluslararası İnsancıl Hukuk Açısından Ayırt Etme İlkesinin Anlamı

1977 Cenevre Konvansiyonlarına Ek 1 No.lu Protokol ayırt etme ve sivil-savaşçı ayrımı (*principle of distinction*) ilkesini göstermektedir: "Silahlı çatışma hukukunda yer alan sivil kişi ve nesneleri korumayı amaçlayan teknik bir terimdir. Bu prensip bağlamında, bir yandan silahlı çatışmanın tarafları siviller ve sivil nesneler diğer yandan savaşçılar ve askeri hedefler arasında her zaman ayrım gözetmelidir ".[189] 1 No.lu Ek Protokol bağlamında siviller ve sivil nesneler hedef olamaz.[190] Devletler "dolayısı ile siviller ve askeri hedeflerin ayrımında yetersiz olan silahlar kullanmamalıdır".[191] Askeri operasyonların gerçekleştirilmesinde savaşanların, sivil halkı, sivilleri ve sivil hedefleri hedef dışı tutmak

---

[184] KELSEY, s.1430.

[185] Jeffrey K. Walker, **The Demise of the Nation-State, The Dawn of New Paradigm Warfare, and a Future for the Profession of Arms**, 51 A.F. L. REV. 323, 2001, s.337–38, http://www.afjag.af.mil/shared/media/docum ent/AFD-081204-028.pdf, (e.t.06.03.2012).

[186] Bradley Graham, **Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia**, The Washington Post, 8 Kasım 1999, sec. A, s.1.

[187] George K. Walker, Information Warfare and Neutrality, Vanderbilt Journal of Transnational Law, 2000, http: //findarticles.com/p/articles/mi_hb3577/ is_5_33/ ai_n28809531/, (e.t.06.02.2012).

[188] KELSEY, s.1431.

[189] Heike Spieker, **Civilian Immunity**, in Crımes of War 84, 84 (Roy Gutman & David Rieff eds. 1999), s.84, http://www.crimesofwar.org/a-z-guide/civilian-immunity/, (e.t.14.02.2012).

[190] **Protocol Additional to the Geneva Conventions of 12 August 1949**, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), madde 51 (2), 51 (1), 8 Haziran 1977, http://www.icrc.org/ihl.nsf /WebList?ReadForm&id=470&t= art, (e.t.14.02.2012).

[191] **Legality of the Threat or Use of Nuclear Weapons**, Advisory Opinion, 1996 I.C.J. 226, 257, July 8, http://ww w.icj-cij.org/docket/index.php?p1=3&p2=4& k=e1&p3=4&case=95, (e.t.14.02.2012).

için sürekli özen gösterme görevi vardır.[192] Saldırılar sadece askeri hedeflerle sınırlı olacaktır. Hedefler söz konusu olduğunda, askeri hedefler doğaları, konumları, amaçları ya da kullanımları gereği askeri eylemlere etkin bir katkıda bulunan ve tamamen ya da kısmen yıkılması, ele geçirilmesi ya da tarafsızlaştırılması durumunda, zamanın şartlarında, kesin bir askeri avantaj sağlayan hedeflerle sınırlıdır.[193] Savaş sırasında doğal çevre, uzun vadeli, geniş alana yayılmış, ciddi zararlara karşı korunacak [194] ve barajlar, su kanalları ve nükleer elektrik üretim tesisleri gibi tehlike arz eden unsurlar içeren yapılar, söz konusu saldırının sivil halk arasında ciddi kayıplara neden olacağı durumlarda, askeri hedefler olsa dahi, saldırıya hedef olmayacaktır. [195]

9.2.1. I No.lu Ek Protokol Madde 58 (a) ve (b) Kapsamında Birbirine Bağlılık, Hedef Belirleme ve Uygulanabilirlik

ABD hükümetinin iletişim araçlarının %98'i, sivil sahipli ya da sivillerce işletilen ağlardan oluşmakta ve bu ağlar, gizli ve gizli olmayan mesajlar ile askeri operasyonları yönetmek amacıyla verilen askeri emir ve direktifleri içeren iletişimleri de kapsamakta, ayrıca Pentagon ve diğer karargâhlardaki stratejik karar vermekle yükümlü kişileri bilgilendirmek amacıyla, savaş alanından gelen güncel istihbarat ve bilgi raporlarını da içermektedir.[196]

Bu iletişim ağları askeri hedef oluşturmakta ve silahlı bir çatışma zamanında düşman tarafından hedef olarak kullanılma olasılığı bulunmakta bu durumla ilgili askeri hedeflerin tanımı I No.lu Ek Protokol'ün 52. maddesinde yer almaktadır.[197] Bu maddenin başlığı sivil hedeflerin genel korunmasıdır ve sivil nesnelerin hedef olamayacağı belirtilmektedir. Ayrıca bu madde sivil nesneler ve askeri nesneler arası zıtlıkları vurgulamaktadır. Maddenin ikinci paragrafında sivil nesneler, askeri hedef olmayan tüm nesneler olarak tanımlanmaktadır.

Bu maddenin başlığı, "Sivil Hedeflerin Genel Korunması" şeklindedir ve sivil nesnelerin hedef haline gelemeyeceği belirtilmekte, sivil nesneler ile askeri hedeflerin ayrımı yapılmaktadır.[198]

Bir hükümetin askeri ya da istihbarat organı; bilgisayarlar, touters, ağlar, kablolar ve diğer siber varlıklar askeri iletişimi sağlamaları sebebiyle hedef olmakta fakat bu nesneler, aynı işlevi hükümet yerine sivil bir şirket için yerine

---

[192] **Protocol Additional to the Geneva Conventions of 12 August 1949**, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), madde 57, 8 Haziran, 1977, http://www.icrc.org/ihl.nsf /WebList?ReadForm&id=470&t=art, (e.t.14.02.2012).

[193] **Protocol Additional to the Geneva Conventions of 12 August 1949**, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), madde 52, 8 Haziran, 1977, http://www.icrc.org/ihl.nsf /WebList?ReadForm&id=470&t=art, (e.t.14.02.2012).

[194] **Protocol Additional to the Geneva Conventions of 12 August 1949**, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), madde 55, 8 Haziran, 1977, http://www.icrc.org/ihl.nsf /WebList?ReadForm&id=470&t=art, (e.t.14.02.2012).

[195] **Protocol Additional to the Geneva Conventions of 12 August 1949**, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), madde 56, 8 Haziran, 1977, http://www.icrc.org/ihl.nsf /WebList?ReadForm&id=470&t=art, (e.t.14.02.2012).

[196] Howard S. Dakoff, **Note, The Clipper Chip Proposal: Deciphering the Unfounded Fears That Are Wrongfully Derailing Its Implementation**, J. Marshall L. Rev., Vol. 29, Num:2, 1996, s.475–479.

[197] **Protocol Additional to the Geneva Conventions of 12 August 1949**, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 Haziran, 1977, http://www.icrc.org/ihl.nsf /WebList?ReadForm&id=470&t=art, (e.t.14.02.2012).

[198] Eric Talbot Jensen, **Cyber Warfare and Precautions Against the Effects of Attacks**, Texas Law Review, Vol. 88:1533, s.1542.

getirdikleri takdirde, sivil nesneler olarak saldırılara karşı korunabilmekte, ancak sivil bir hedefin ne zaman saldırıya uğradığını anlamak her zaman çok açık olamamaktadır.[199]

Hükümetler, yazılım ve donanım programlarının çoğunu ticari tedarikçilerden edinmekte, bu programların çoğu sivil şirketler tarafından korunmakta, hükümet yazılım ve donanımlarını imal eden ve bakımını yapan bu şirketlerin de hedef haline gelmeleri mümkün olmakla birlikte Amerika'nın siber yeteneklerine sürekli bir saldırı durumunda, bu sivil şirketler destek ve bakım için çağırılmaktadır.[200] Hükümet siber sistemlerinin bakımını ve siber ürünlerin güncellemesini yapmakla yükümlü bu sivil siber şirketlerin kullandıkları binalar ve nesneler düşman tarafından hedef haline gelebilecektir. Eğer sivil bir bilgisayar şirketi, hükümet siber sistemleri üretiyor, sistemlerin bakımını yapıyor ya da destekliyorsa; düşman tarafından I No.lu Ek Protokol madde 52'ye göre hedef olarak görülebilecektir.[201]

Belirtilen askeri hedeflerin her biri, birbirine bağlı-bağımlı siber dünyada, sivil nesnelerle iç içe geçme özelliğine sahiptir. Belirtilen sivil nesneler direkt olarak hedef alınamamakta, fakat hükümet bilgisayarları ya da yönlendiricileri imal eden şirket, bunları sivillere satmak amacıyla da üretmektedir.[202]

9.2.2. I No.lu Ek Protokol Madde 58 (c) Kapsamında Alternatif Sorumluluklar

Maddede üç ana kavram; "mümkün olan azami ölçüde", "diğer gerekli önlemler" ve "onların (savaşan tarafların) kontrolü altındaki" vurgulanmaktadır.[203] "Mümkün olan azami ölçüde" ifadesi, taraflara, bu ihtara özne olanları da koruma yükümlülüğü getirmekte, her şeyin her zaman korunamayacağını fark etmek, bir karar metodu geliştirmeyi gerektirmektedir. Bazıları kritik ülkesel altyapıları en baş öncelik olarak belirlerken, bu kategori madde 58'in öngördüğü hatlardan da geniş olabilmektedir.[204] Her devlet neyin mümkün olduğuna kendisi karar vermelidir ancak şu unutulmamalıdır ki; ifadede yer alan kavram "azami (maksimum)" şeklindedir.[205]

---

[199] Martin C. Libicki, **Cyberdeterrence and Cyberwar**, Rand Corporation, The U.S.A, 2009, s. 153.

[200] JENSEN, s. 1543.

[201] **12 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek** Uluslararası Silahlı Çatışmaların Kurbanlarının Korunmasına İlişkin (1) No.lu **Protokol,** 8 Haziran 1977, http://www.kizilay.org.tr/hukuk/sayfa_y azdir.php?t=-Ulusal.ve.Uluslararasi.Sozl esmeler-CENEVRE.EK.1.PROTOKOL, (e.t.06.02.2012).

[202] JENSEN, s. 1544.

[203] **12 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek Uluslararası Silahlı Çatışmaların Kurbanlarının Korun masına İlişkin (1) No.lu Protokol,** 8 Haziran 1977, http://www.kizilay.org.tr/hukuk/sayfa_yazdir.php?t=-Ulusal.ve.Uluslararasi. Soz lesmeler-CENEVRE.EK.1.PRO TOKOL, (e.t.06.02.2012).

[204] **Official Records Of The Diplomatic Conference On The Reaffirmation And Development Of Internatio nal Humanitarian Law Applicable In Armed Conflıcts**, Geneva (1974–1977), pt. 1, at 3, 1978, http://www.lo c.gov/rr/frd/Mi litary_Law/RC-dipl-conference-records.html, (e.t.06.02.2012).

[205] **12 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek Uluslararası Silahlı Çatışmaların Kurbanlarının K orunmasına İlişkin (1) No.lu Protokol,** 8 Haziran 1977, http://www.kizilay.org.tr/hukuk/sayfa_yazdir.php?t=-Ulusal.ve.Uluslararasi. Sozl esmeler-CENEVRE.EK.1.PROTOKOL, (e.t.06.02.2012)

[205] **Official Records Of The Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts**,

Hükümet hareketlerini kısıtlamayı amaçlayan ikinci ifade, sivillerin ve sivil nesnelerin korunmasını içermekte, buna göre madde, hükümetlere; sadece kendi kontrolleri altında olan sivilleri ve sivil nesneleri korumayı öngörmektedir; örneğin askeri kontrol altına girmiş olan sivillerin düşman tarafından yapılabilecek saldırılara karşı korunması askeri idarenin görevi olarak belirlenmektedir.[206] Bilgisayarlar, ağlar, sistemler, yönlendiriciler vb. zorunluluk altında hükümet kontrolünde olmalıdır. Bu zorunluluk şartının anlamı; bir düşman tarafından gerçekleştirilen bir siber saldırıda hükümet, operasyonlarının devamını güvenlik altına almak için, belirli bir bilgisayar ağını, kontrolü altına almalı ve kontrolü altında tutması şeklindedir.[207] Hükümet ağın kontrolünü ele aldığında, sivil iletişim trafiği de dâhil, bütün ağı koruma zorunluluğunu kabul etmiş sayılmaktadır.

Madde 58 (c) hükümetlere, "diğer gerekli önlemleri" alma yükümlülüğü getirmektedir. Bu ifade iki sebeple önemlidir: Birincisi; "diğer" ifadesi, sadece ayırt ederek koruma altına almayı değil, bundan daha fazlasının gerekli olduğunu yansıtmakta, hükümet; sadece hangi ağların kendi kontrol ve koruması altına girdiğini belirlemekte, alınması gereken diğer önlemleri almadan, görevini yerine getirmiş sayılmamaktadır.[208] Hükümet bir kez, koruma zorunluluğunu kabul ettiği zaman, diğer tedbirleri de almak zorundadır.

İkinci olarak "önlemler" kavramı önemlidir çünkü önlemler sadece saldırılara yanıt olarak verilen hareketleri değil, önceden alınması gereken tedbirleri de içermekte, ansızın gerçekleşen bir siber saldırıda, hükümet bu zorunluluğu tepkici bir sorumluluk olarak almamakta bunun yerine, potansiyel bir saldırıya karşı tedbir almak durumundadır.[209]

Hükümet, silahlı bir saldırı meydana geldiği zaman, hangi siber yeteneklerini garanti altında tutmayı istediğini belirlemeli, hangi sivil sistemlerin, şirketlerin, ağların vs. bu işlevi sağlayacağına karar vermeli ve bu kararları vererek, kendi kontrolü altına girecek sivilleri ve sivil nesneleri korumak için gerekli adımları atmalıdır.[210] Bu sistemlerin saldırıya uğramasına kadar geçen süre, madde 58'deki ve silahlı çatışma hukukunun zorunluluklarına tabi değildir. Acil eyleme hazır olunmalı ve gerektiğinde seri bir şekilde uygulanmalıdır.

9.3. Ayrım Kuralları Altında Potansiyel Siber Saldırıların Meşruluğu

Bazı askeri operatörler geleneksel saldırıların meşru askeri hedeflerin, siber savaşlarda da meşru askeri hedefler olduğuna inanmaktadırlar.[211] Uluslararası İnsancıl Hukukun yasaklamalarının, kullanılan silahın ya da savaşın türüne bağlı olmadığı ve tartışmasız bir şekilde bu durumun siber sa-

---

Volume 1, Federal Political Department, (Geneva, 1974 -1977), Bern, 1978, http://www.loc.gov/rr/frd/Military_Law/pdf/RC-records_Vol-1.pdf, (e.t.11.0 2.2012)

206 JENSEN, s.1553.

207 JENSEN, s.1554.

208 **12 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek Uluslararası Silahlı Çatışmaların Kurbanlarının Korunmasına İlişkin (1) No.lu Protokol,** 8 Haziran 1977, http://www.kizilay.org.tr/hukuk/sayf a_yazdir.php?t=-Ulusal.ve.Uluslararasi. Soz lesmeler-CENEVRE.EK.1.PROTOKOL, (e.t.06.02.2012).

209 JENSEN, s.1554.

210 JENSEN, s.1555.

211 Bradley Graham, **Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia**, The Washington Post, 8 Kasım 1999, sec. A, s. 1.

vaşlarda da uygulanması gerektiği savunulmaktadır.[212] Bazı siber silahların kullanımına izin verilmesi bu ayrımın kurallarında görülebilirken, bu kurallar diğer kullanım türlerini yasaklamakta, hava savunma ağı gibi yüksek sivil kayıp riski taşıyan operasyonlarda, ayrımın kuralları askeri operasyonları tanımlamada büyük bir rol oynayacak gibi görünmektedir. [213] Uluslararası İnsancıl Hukuk, minimum seviyede, askeri komutanların sadece nereye saldırı yapacaklarını bilmelerini değil, bir saldırının yapacağı yankıları da öngörmelerini beklemektedir ve yelpazenin diğer ucunda, Uluslararası İnsancıl Hukukun, doğrudan ve kasti şekilde sivillerin yaralanmasına ve büyük yıkımlara neden olabilecek siber saldırıları yasaklama eğiliminde olduğu görülmektedir.[214] Bu çeşit saldırı örneklerinin hava trafik kontrol sisteminin bozularak sivil uçakların çarpışmasına neden olabilecek eylemler ya da sivil veya yaralı askerlerin yanlış kan grubu nakilleri almalarına neden olabilecek tıbbi veritabanı yolsuzluğunu içermesi örnek olarak verilebilir.[215] Uluslararası İnsancıl Hukuk, çevreye ciddi zarar verebilecek ya da doğal afetlerin oluşmasını tetikleyecek ihlallerde bulunulmasını 1 Nolu Ek Protokol ile yasaklamıştır.[216]

9.3.1. Tarafsızlık Hukuku ve İnternet Kullanımı Yoluyla Yönetilen Siber Savaşlar

Tarafsızlık hukuku, devletlerin muharipleri aracılığıyla çatışmalara katılmadan ilişkilerini sürdürerek, savaş ve barışın birlikte var olmasını düzenlemektedir. Tarafsızlığı düzenleyen birincil kaynak olan Lahey Konvansiyonları, savaşanların haklarını ve ödevlerini ana hatlarıyla belirterek, tarafsız devletlerin savaş zamanı tarafsızlıklarını sürdürebilmelerini sağlamaktadır.[217] Konvansiyonlar tarafsız bir devletin topraklarının dokunulmaz olduğunu dikte etmekte, tarafsız devletlere ihlallere neden olan savaşçıları önlemek üzere gerek duyulduğunu belirtmekte ayrıca tarafsızlık hukuku ayrıca sınırlı iletişim istisnasını da tanımlamaktadır. 1907 5. Lahey Konvansiyonu m.8'e göre: "Tarafsız devlet, şirketlere ya da gerçek kişilere ait telgraf, telefon kabloları ya da kablosuz haberleşme aparatlarını sınırlamak ya da yasaklamak çağrısında bulunmaz. Tarafsız devlet kısmen savaşanların bu araçları kullanmasına izin verir" fakat 1907 5. Lahey Konvansiyonu, bu istisnanın bilgi toplayan uydu görüntüleri, hava durumu ve navigasyon sistemleri gibi dijital sistemlerin iletişim altyapısının ötesinde geçerli olduğunu öngörmemektedir.[218]

Sınır ötesi siber saldırılar yapmak için internetin kullanılması tarafsızlık kurallarını ihlal etmektedir.[219] Bazı görüşlerin aksine, bir muharip tarafsız bir devletin internet ağına siber saldırı başlattığında, fiziksel saldırı olmasa dahi, tarafsızlık hukukunu ihlal etmekle birlikte tarafsız devletlerin internet ağına

---

[212] Knut Dörmann, **Computer Network Attack and International Humanitarian Law**, International Committee of the Red Cross, 19 Mayıs 2001, para. 29, http://www.icrc.org/eng/resources/documents/misc/5p2alj.htm, (e.t.06.02.2012).

[213] KELSEY, s.1438.

[214] GRAHAM, s.1.

[215] Lawrence t. Greenberg et al., **Information Warfare and International Law 12**, National Defense University Press, 1998, s.10, http://www.dodccrp.org/ files/ Greenberg_Law.pdf, (e.t.06.02.2012).

[216] KELSEY, s.1436.

[217] **Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land**, The Hague, 18 Ekim 1907, http://www.icrc.org/ihl.nsf/full/200?opendocument, (e.t.06.02.2012).

[218] KELSEY, s.1442.

[219] KELSEY, s.1443.

düzenlenen sınır ötesi siber saldırılar Uluslararası İnsancıl Hukuku da ihlal etmektedir.[220] ABD Hava Kuvvetleri, silahları; öldürmek, yaralamak, etkisiz hale getirmek ya da mülkiyete zarar vermek amaçlı kullanılan araçlar olarak tanımlamaktadır.[221] Siber silahlar; siber saldırılarla askeri ve sivil hedefleri yok edebilmesine rağmen, insanları doğrudan değil dolaylı olarak etkilemektedir.[222] Uluslararası İnsancıl Hukuk, tarafsız devletin tarafsızlık görevi ile uyumlu olarak, siber saldırıları önlemek için görev almasını içermesine rağmen, bu görevin kapsamı değişkenlik arz edebilir. 5. Lahey Konvansiyonu m.5, tarafsız bir devletin kendi topraklarındaki tüm ihlalleri önlemek üzere mutlak bir görevi olduğunu vurgulamaktadır.[223] Ancak tarafsız devletler, bu tür saldırıları tespit etmeleri için etkin bir yönteme sahip değildir. Tarafsız devlet ihlali tespit etmiş olsa bile, internetin sahip olduğu bu yapı altında, diğer devletlerin bilgisayar sistemleri ile tüm bağlantıları koptuğu sürece, bir devletin siber saldırıları önlemesi mümkün değildir. Bu durumun tutarsızlığı, meşru internet iletişiminin bozulmasına yol açabilir.[224]

9.4. Bazı Durumlarda Siber Silahların Kullanımının Geleneksel Savaş Metotları Yerine Teşvik Edilmesi

Siber savaş, Uluslararası İnsancıl Hukuk için bir sorun teşkil etmektedir çünkü ayrım ilkelerinin geçerli tanımı ve tarafsızlık kavramı oldukça dardır, bu sebeple mevcut kurallara siber savaşın riayet etmesi mümkün değildir, ancak yasaklanmış siber silahların kullanımı devletlere düşük seviyede sivil nesnelere fiziksel zarar ve insan yaşamında düşük maliyetli bir darbe olasılığı sunmaktadır.[225] Sivil ve asker ölümlerinin azalmasıyla aynı zamanda hızla zafere ulaşma avantajları, siber savaşı karar alıcılar için cazip bir politika seçeneği haline getirmekte, bu silahların gelişiminin önlenmesi yerine, ayrım ve tarafsızlık kavramları, devletlerin bazı durumlarda siber silahları kullanmak üzere teşvik edilmesi için geliştirilmelidir.[226]

Devletler I Nolu Ek Protokolü; kesin askeri avantajlara dar kapsamda odaklandığı ve ithalat endüstrileri gibi ekonomik hedefleri de içeren savaş yeteneğinin sürdürülebilmesine çok az önem verdiği için yoğun şekilde eleştirmişlerdir.[227] Siber silahlar, Uluslararası İnsancıl Hukukun devletleri izlemeye teşvik edeceği şeklinde üçüncü bir yol sunmakta ve eğer siber savaş, eğer kurallara uygun bir şekilde sınırlanırsa, sivillerin hayatlarını kaybetmelerinden ve sivil nesnelere zarar verilmesinden kaçınılarak, savaşanların hedef listesini

---

[220] Lawrence t. Greenberg et al., **Information Warfare and International Law 12**, National Defense University Press, , 1998, s.10, http://www.dodccrp.org/files/Greenberg_Law.pdf, (e.t.06.02.2012).

[221] Department. of the Air Force, Policy Directive 51–4, Compliance with the law of armed conflıct para.6.5, 1993, .http://www.icrc.org/ihlnat.nsf/6fa4d35e5e3025394125673e00508143/cfaff63edde42523c1256a8e00342cf b!OpenDocument, (e.t.06.02.2012).

[222] KELSEY, s.1444.

[223] **Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. The Hague, 18 October 1907**, http://www.icrc.org/ihl.nsf/full/200?opendocument, (e.t.06.02.2012).

[224] KELSEY, s.1443.

[225] KELSEY, s.1446.

[226] KELSEY, s.1447.

[227] **Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia**, para. 40, 8 Haziran 2000, 39 I L M 1257., http://www.icty.org/sid /10052, (e.t.06.02.2012).

genişletecek bazı hareketlere izin verebilmektedir.[228] Bu silahların potansiyel öldürücü etkileri nedeniyle, konvansiyonel silahlara uygulanan aynı kısıtlayıcı kuralları siber savaşa da uygulamak yerine, Uluslararası İnsancıl Hukuk, devletlere siber silahların yayılması yönünde daha fazla esneklik sunmaktadır.[229]

Tarafsızlığın anlamı değişkendir ve savaşanlar ve tarafsız devletler internetin geçerli yapısı altında, Uluslararası İnsancıl Hukuku uygulamakta önemli zorluklarla karşılaşmakta, tarafsız ve savaşan devletlerin Uluslararası İnsancıl Hukuk tarafından ele alınan görevlerinin kapsamının değişmesi gerekmektedir.[230] Uluslararası İnsancıl Hukuk, tarafsızlık prensibi ilkesine saygı gösterilmesini korumalı ve tarafsız devletlere siber silahların kullanımından doğan gerçekçi olmayan limitlerden sakınmalarını sağlarken, tarafsızlıklarını sürdürebilmeleri için de etkin bir yol sunmalıdır.[231]

Siber savaşın yönetilmesi için yeni kurallar geliştirilmelidir, fakat yeni bir antlaşmanın yapılması gerekli ve mümkün görünmemekle birlikte başka analizler de Uluslararası İnsancıl Hukuk kurallarının benzer şekilde genişletilmesini savunmakta, böylece uluslararası bir andlaşmadan kaynaklanmak yerine bu normlar teamül, davranış kuralları ya da angajman (*rules of engagement*) kuralları ile değişmelidir görüşü ortaya çıkmaktadır.[232] Sürecin gelişmesi yoluyla kuvvet komutanlarının bir saldırının olası meşru sonuçlarını düşünmesi bu normları geliştirecek bir yol olabilir. Bu süreçler, öngörülebilirliğin farklı seviyelerindeki fiziksel altyapıya yapılan saldırıları, komutanların saldırının çeşitli etkilerini araştırmak üzere Uluslararası Hukuk Kurallarının siber savaşta uygulanmasını ve bu savaşların yönetilmesi için yeni angajman kuralları geliştirilmesini gerektirmekte, devletler, savaşlarda siber silahların konuşlandırılması ile Uluslararası İnsancıl Hukuk kurallarının nasıl değiştiğini araştırmalılar ve böylece ortak devlet uygulamaları ortaya çıkmaya başlayacaktır. [233]

10. ULUSLARARASI HUKUK BAĞLAMINDA SİBER ÇATIŞMA ÜZERİNDE EGEMENLİK SÖYLEMİ

Bilgi savaşının uluslararası hukuk bağlamında analiz edilme çabaları 1990'da başlamış ve bundan sonra dünya çapında askeri, akademik, hükümetsel ve kurumsal yorumcular kişisel ve örgütsel fikirlerini açıklamışlardır.[234]

Siber suç durumunda olaylar yerel kolluk kuvvetlerince tam anlamıyla araştırılamamakta ya da iç ceza sistemi içinde yargılanamamakta ve karşılıklı hukuki yardım antlaşmaları ile INTERPOL (*International Criminal Police Organization*) gibi çok taraflı örgütlerden rücu bulmaktadır.[235] Uluslararası hukuk sisteminin doğası, BM Şartı rejimi altında egemen merkezli bir yaklaşı-

---

[228] KELSEY, s.1448.

[229] KELSEY, s.1447.

[230] KELSEY, s.1448.

[231] KELSEY, s.1449.

[232] Davis Brown, **A Proposal for an tnternational Convention To Regulate the Use of Information Systems in Armed Conflict**, Volume 47, Number 1, Winter 2006, s.201–202, http://www.harvardilj.org/wp-content/uplo ads/2010/10/HILJ_47-1_Brown. pdf, (e.t.06.02.2012).

[233] KELSEY, s.1449.

[234] Sean Kanuck, **Sovereign Discourse on Cyber Conflict Under Intemational Law**, Texas Law Review Association, Symposium: Law at the Intersection of National Security, Privacy and Technology: II. Cybersecurit y and Network Operations, Vol. 88:1571, 2010, s.1571.

[235] INTERPOL, **Secure Global Police Communications Services**, https://www.interpol. int/Public/ICPO/corefu nctions/secu recom.asp, (e.t.06.02.2012).

mın üstünlüğünü tanımakta, ulusal düzenlemelerin yanı sıra Uluslararası Telekomünikasyon Birliği himayesinde kurulan potansiyel kullanıcılar arasında elektromanyetik frekansların tahsisi ve yetkisiz müdahalelerin yasak olduğu belirtilmektedir.[236] Örneğin Küba, kendi topraklarında izinsiz yabancı televizyon ve radyo yayınları yapılmasını, ulusal egemenlik ve vergilendirme sözleşmelerinin açık ihlali olduğunu iddia etmektedir.[237]

Yabancı mahkemeler Amerikan internet servis sağlayıcılarına Avrupa websitelerinden belli bir materyal filtrelenmesini düzenlemiş, Şangay İşbirliği Örgütü üyeleri (Çin, Kazakistan, Kırgızistan, Rusya, Tacikistan ve Özbekistan) kendi anlaşma bölgesinde bilişimsel içeriklerin kontrolü için gerekçe teklif etmiş, Çin ve Katar "serbest bilgi akışı, ulusal egemenlik ve güvenliğin korunmasının gerektiği durumlarda garanti altına alınmalıdır" ve "her devlet kendi iç mevzuatına göre kendi siber uzayını yönetmek hakkına sahiptir" ilkelerini korumuştur.[238]

Bu alanda bugüne kadar en çok dikkat çeken belgeler arasında Avrupa Konseyi Siber Suç Konvansiyonu, küresel bir siber güvenlik kültürünün oluşturulmasına ve bilgi teknolojilerinin kötüye kullanılması suçuna ilişkin 2. ve 3. Komite'nin beş BM Genel Kurul kararı bulunmaktadır.[239] Siber uzaydaki potansiyel askeri eylemler ulusal güvenlik endişelerini arttırmakta, böylece bazı devletler çok taraflı antlaşmalar yoluyla bu endişeleri gidermeye çalışmaktadırlar.[240] 1998 yılından beri BM Genel Kurulu Birinci Komitesi (görevi uluslararası güvenlik ve silahsızlanma işlerini kapsamaktadır), uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeler başlıklı yıllık bir kararı geçirmiştir. Bu karar ile BM Genel Sekreteri, uluslararası bilgi güvenliği üzerinde BM üyesi devletlerin resmi görüşünü sağlamak üzere devletleri davet etmektedir.[241] Zamanla örf ve uluslararası hukukun oluşumunda katkıda bulunan bir rol oynayabilmelerine rağmen, 2009 yılı boyunca toplam 42 devlet tarafından sunulan 78 yanıttan sadece "kendi sınırlarının ötesine taşınan kontrol ötesi bir ulusal bakış açısı ile" şekilde kalmış, BM Genel Kurulu'nun 2005'ten 2009 yılı kararları boyunca, ikinci bir BM hükümet uzmanları grubu 2009–2010 boyunca uluslararası bilişim güvenliğini dikkate almak üzere toplanmıştır.[242]

BM Silahsızlanma Araştırmaları Enstitüsü, 2007 yılında üç aylık bir dergiyi bu konuya adayarak, uluslararası bilişim güvenliğinin daha da araştırılması amacıyla 1999 ve 2008'deki görüşmelere sponsor olmuş, birçok SCO, NATO ve Avrupa Güvenlik ve İşbirliği Teşkilatı gibi bölgesel örgütler, uluslararası bilişim güvenliği sağlamak amacıyla siber saldırılara karşılık vermek üzere yasal tedbirlerin alınması için diyaloglar başlatmıştır.[243] BM ve bölgesel girişimlerin pek çoğundan henüz somut sonuçlar alınamamış olsa da (SCO

---

[236] KANUCK, s.1574.

[237] KANUCK, s.1573.

[238] KANUCK, s.1575.

[239] Council of Europe, **Convention on Cybercrime**, opened for signature:11 Kasım 2001, Europ. T.S. No. 185, http://conve ntions.coe.int/treaty/en/treaties/html/185.htm, (e.t.07.02.2012).

[240] KANUCK, s.1581.

[241] KANUCK, s.1582.

[242] KANUCK, s.1580.

[243] KANUCK, s.1583.

hariç), uluslararası toplumun egemen uluslararasındaki siber çatışmaları giderek artan yasal dikkate layık bir endişe olarak görülmektedir.[244]

10.1. Devletin Uluslararası Sorumluluğu

Uluslararası alanda, kendilerinden üstün bir otoriteye tabi olmayan eşit sujeler arasındaki uyuşmazlıklarda, adil ve barışçıl neticeler elde edilmesinde, sorumluluk hukukunun etkin bir şekilde işlemesi oldukça önem taşımaktadır.[245] Devletin uluslararası sorumluluğu ile ilgili temel ilke Uluslararası Hukuk Komisyonu'nun 2001 yılı çalışmalarının ilk maddesinde: " Bir devletin uluslararası nitelikteki her haksız fiil, o devletin sorumluluğunu doğurur" şeklinde belirtilmektedir.[246] Devletin bir uluslararası haksız fiilinin mevcut olması için iki unsurdan ilki; söz konusu davranışın uluslar arası hukuka göre devlete isnat edilebilir olması gerekmekte, ikinci olarak ise; devletin bir fiilinden ötürü sorumluluğunun doğabilmesi için bu davranışın sorumluluğu söz konusu edilecek devlet için hâlihazırda uyulması gereken ve uluslararası hukuktan doğan bir yükümlülüğün ihlalini oluşturmalıdır.[247] Uluslararası Hukuk Komisyonu'na göre, ihlalden ötürü sorumluluğu doğan devletin, sorumluluğundan kaynaklanan yükümlülüklerinin somut olarak doğabilmesi, gerçekte bunları yerine getirebilmesi için zararın mevcudiyeti gereklidir; böylece zarar somut olarak mevcut değilse devletin sorumluluğu soyut olarak mevcuttur, fakat somut bir zarardan söz edildiğinde, devletin sorumluluğundan doğan onarım yükümlülüğü somut olarak gerçekleşebilecektir.[248]

Devlet yönetimi ile uluslararası teamül hukuku oluşumunda etkin bir rol oynamanın yanı sıra, egemen devletler, kabul edilen yasal yükümlülüklere uyarak, kendi ulusal çıkarlarını korumaya çalışmakta ve egemen bir devletin kontrolü ne kadar arzu edilmiş olsa da, halka açık ulaşılabilir teknoloji, devletin tam etkili kanuni yaptırımlarının ve ulusal güvenlik prosedürlerinin eylem kabiliyetini geride bırakmaktadır.[249] Siberuzay üzerinde egemen devletin otorite uygulamak için yaygın iradesine rağmen, hiçbir devlet şu anda bilgi ve iletişim ağlarından çıkan istenmeyen aktiviteleri caydıramamak, engelleyememek ya da tespit edememekte; bu sınırlama, devletin etkilerinin devlet sorumluluğu ilkesinin uygulanması önünde ve devlet dışı aktörler için kritik bir engel oluştur-

---

[244] Pan Guang, **The SCO's Success in Security Architecture (**highlighting confidence building, cooperation against destabilizing transborder elements, and the maintenance of regional security and stability as general successes of the SCO), http://epress.anu.edu.au/sdsc/architecture/mobile_devices/ch04.html, (e.t.07.02.2012).

[245] Hakkı Hakan Erkiner, Devletin Haksız Fiilinden Kaynaklanan Uluslararası Sorumluluğu, 12 Levha Yay., , 1. Baskı, İstanbul, 2010, s.76. Ayrıca bkz. Elif Uzun, Milletlerarası Hukuka Aykırı Eylemlerinden Dolayı Devletin Sorumluluğu, Beta Yay., 1. Basım, İstanbul, 2007.

[246] **Report of the International Law Commission on the work of its fifty-third sessio**n, DOCUMENT A/56/10, madde 1, (23 Nisan–1 Haziran ve 2 Temmuz–10 Ağustos 2001), s.32, http://untreaty.un.org/ilc/reports/ 2001/2001report.htm, (e.t.13.02.2012).

[247] ERKİNER, s.10. Ayrıca bkz. **Report of the International Law Commission on the work of its fifty-third sessio**n, DOCUMENT A/56/10, madde 2, (23 Nisan–1 Haziran ve 2 Temmuz–10 Ağustos 2001), s.32, http://untreaty.un.org/ilc/reports/ 2001/2001report.htm, (e.t.13.02.2012).

[248] ERKİNER, s.11.

[249] KANUCK, s.1590.

maktadır.[250] 2010 yılı Ocak ayında BM hükümet uzmanları grup müzakerelerinde Çin; egemen devletlere, iç siberuzayını ve ilgili altyapılarını serbest tutmak amacıyla saldırıdan, bozulmadan, tehditten ve sabotajdan korumak üzere gerekli yönetim tedbirleri alarak sorumluluklara ve haklara sahip olmalarını önermiştir.[251] Hindistan bu konu tartışmalarına daha açıktır: "Ağa bağlı bir toplum oluşturma ve küresel ağ ekonomisinin bir parçası olan ulus devletler, başkaları tarafından, gizlice veya açıkça başka bir ulus devletin ICT altyapısının hedefi olur veya saldırıya uğrarsa, kendi ICT altyapılarını sadece koruma gereksinimi farkına varması değil, aynı zamanda ICT'lerin kötüye kullanılmamasının sağlanması sorumluluğunun olması önemli olacaktır".[252] İki seçkin uluslararası hukuk bilim adamı olan Antonio Cassese ve Ian Brownlie'ye göre, devlet dışı aktör eylemlerine sorumluluk yükleyen uygun hukuki analiz, egemenin sergilediği yeterli tedbir ya da ihmal derecesine dayanmakta, teşebbüs edilen zararı önlemek üzere devlet yasal bir yükümlülüğü yerine getirememesinden dolayı eyleminden sorumlu tutulamamaktadır.[253] Siber bağlam dışında ILC: "Menşe devlet, önemli sınır ötesi zararların görünmesini engellemek için veya her hangi bir olay riskini en aza indirmek için tüm uygun önlemleri alacaktır. Siber normların üzerinde herhangi bir uluslararası fikir birliği olmaması, devletin siberuzayda yeterli özeni gösterip göstermediğine ya da zararı önlemek için uygun önlemleri alıp almadığına karar verilmesini zorlaştırmaktadır" şeklinde açıklamada bulunmuştur. [254]

SONUÇ

Somut örneklerine sık sık rastlamamıza ve varlığı artık inkâr edilemez olmasına rağmen, siber savaş ya da saldırı kavramı, soyutluğunu korumaya devam etmektedir. Siber savaş; bireyler arası ve bireylere karşı işlenebilecek bir suç da olmakla beraber, devletler arası ya da devletlere karşı uygulanan faaliyetleri kapsamaktadır. Bu nedenle de savaş hukukunun ya da genel anlamda uluslararası hukukun alanına girmektedir. Öte yandan, günümüz dünyasında artık, uluslararası hukuktan söz edebilmek için mutlaka devlet aktörünün yer alması gerektiği fikri kaybolmaktadır. Ortaya çıkan pek çok aktör de, eskiden devletlerin sahip olduğu güç ve yetkiye sahip olarak ya da saldırıya maruz kalarak bu arenada aktif bir rol oynamaktadır.

Siber savaşa dair pek çok devlet yeni bir düzenleme gereğine işaret etse de ortak bir paydada henüz böyle bir adım atılabilmiş değildir. Devletler kendi güvenliklerini korumak isterken, bir yandan da ciddi bir tehditle karşılaşmamışken, yetkilerinin kısıtlanmasını istememektedirler. Teknolojik anlamda en güçlü olan devletler, bu sistemlere bağımlılıkları sebebiyle aslında büyük kayba uğratılabilecek, saldırıya en açık devletler olma konumunda yer almaktalar. Siber suçların işlenmesi, fakir ya da daha eğitimsiz toplumlar için de mümkünken, büyük boyutlarda zarar görme ihtimali, her türlü altyapısı bakımından teknolojiye bağlı diğer devletlere göre daha düşüktür.

Küresel anlamda bakıldığında, siber suçlar bakımından henüz yolun başında gibi görünülse de, her gün işlenen suçlar, yaptırımsız kalmaya devam

---

[250] Paul Rosenzweig, **National Security Threats in Cyberspace 2**, 2009, s.14, http://www.americanbar.org/cont ent/dam/ab a/migrated/natsecurity/threats_in_ cyberspace.authcheckdam.pdf, (e.t.07.02.2012).

[251] KANUCK, s.1591.

[252] KANUCK, s.1591. Daha fazla bilgi için bkz. India's Contribution to the Report of the U.N. Group of Govemmental Experts on Information Security 3 (Ocak 2010).

[253] Antonio Cassese, **International Law**, Oxford University Press:2001, s.81.

[254] KANUCK, s.1592.

ettikçe ve uygulayıcılarına çıkar sağladıkça artmaya devam etmektedir. Devletler de koruma amaçlı örgütlenmelerini artırmakla beraber, olası durumlarda saldırı silahını kullanmaya yönelik çalışmaya devam etmekteler. Henüz siber savaşı ya da suçları kapsayan ortak bir hukuki zemin sağlanamamış olsa da, ilerleyen zamanda bunun her devlet hatta her etkin aktör için bir zorunluluk haline geleceği oldukça aşikârdır.

KAYNAKÇA

KİTAPLAR

AKMAN, Toygar, **Sibernetik: Dünü, Bugünü, Yarını**, Kaknüs Yay., İstanbul, 2003.

ALFORD, Lione1.D., **Cyber Warfare: A New Doctrine and Taxonomy**, CrossTalk: The Journal of Defense Software Engineering, Vol. 14 No. 4, Nisan 2001, http://www.ldalford.com/technical_writing.htm, (e.t.02.02.2012).

AMATO, Ivan, **Lying With Pixels, Seeing is No Longer believing**. Tech. Rev., Temmuz 2000, http://www.technologyrevie w.com/Infotech/12115/?a=f, (e.t.29.01.2012).

ARKIN, William M., **When Seeing and Hearing Isn 't Believing**, Wash. Post.Com, 1 Şubat 1999, http://www.washingtonp ost.com/wp-srv/national/ dotmil/arkin020199.htm, (e.t.29.01.2012).

A Strategic Approach to Protecting SCADA and Process Control Systems, IBM Global Services, Temmuz 2007, s.1–13, http://www935. ibm.com/services/us/iss/pdf/scada_ whitepaper.pdf, (e.t.28.01.2012).

BEAL, Vangie, Webopedia, **The Difference Between a Virus, Worm and Trojan Horse**, 06.29.2010, Son güncelleme: 03.29.2011, http://www. webopedia.com/DidYouKnow/Internet/2004/virus.asp, (e.t.29.01.2012)

BERG, Paul, **Air Force Cyber Command: What It Will Do and Why We Need It**, Air & Space Power Journal, 20 Şubat 2007, http://www.airpower. au.af.mil/apjinternational/apj-s/2007/1tri07/bergeng.html, (e.t.28.01.2012).

BILLO, Charles, Welton Chang, **An Analysis of the Means and Motivations of Selected Nations States**, Institute For Security Technology Studies At Dartmouth College, Kasım 2004. http://www.ists.dartmouth.edu/ docs/execsum.pdf, (e.t.29.01.2012).

BRADLEY, Graham, **Washingtonpost.com:Bush Orders Guidelines for Cyber-Warfare**, Washington Post, 7 Şubat 2003, http://www.washingtonpost. com/ac2/wpdyn/A381102003Feb6?language=printer, (e.t.28.01.2012).

BRADLEY, Tony, **Pandora's Box**, Antionline Newsletter #7, Nisan/Mayıs 2003, s.15–16, http://www.Antionline.com/news le tter/aonewsletter7.pdf, (e.t.28.01.2012).

BRENNER, Susan W., Leo L. Clarke, **Conscription and Cyber Conflict: Legal Issues, 3rd International Conference on Cyber Conflict**, CCD COE Publications, Estonia, 2011.

BYRES, Eric, **The Myths and facts behind Cyber Security Risks for Industrial Control Systems**, British Columbia Insti tute Of Technology A Polytechnic Institution, http://www.nealsystems.com/downloads/Myths%2 0and%2 0Facts%20for%20 Control%20System%20Cyber-security.pdf, (e.t.30.01.2012).

CAHILL, Thomas P., Konstantin Rozinav ve Christopher Mule, **Cyber Warfare Peacekeeping**, Proceedings of the 2003 IEEE Workshop on Information Assurance United States Academy, ISBN 0-7803-7808-3/03, 2003.

CASSESE, Antonio, **International Law**, Oxford University Press:2001.

CHEN, Thomas M., "Stuxnet, The Real Start of Cyber Warfare?", IEEE Network, Kasım/Aralık 2010, s.1–3.

CLAUSEWITZ, Carl von, **On War**, (editör ve çeviren: Michael Howard and Peter Paret), Princeton University Press, New Jersey, 1989.

COATES, J.F., **What's next? Foreseeable terrorist acts**, The Futurist 36 (5), 2002, s.23–26.

COLEMAN, Kevin, Department of Cyber Defense, **An organization who's time has come!**, Technolytics, Kasım 2007. http://www.technolytics.com/ Dept of_Cyber_Defense.pdf, (e.t.10.02.2012).

COLEMAN, Kevin, **Inside DPRK's Unit 121**, Defencetech.org., 24 Aralık 2007, http://defensetech.org/2007/12 /24/inside-dprks-unit-121/, (e.t. 29.01.2012).

COLEMAN, Kevin, **Russia's Cyber Forces**, Defencetech.org., 27 Mayıs 2008, http://defensetech.org/2008/05/2 7/russias-cyber-forces/, (e.t.29.01.2012).

COLEMAN, Kevin, **The Cyber Arms Race Has Begun**, 28 Ocak 2008, s.1–4, http://www.csoonline.com/article/216991/c oleman-the-cyber-arms-race-has-begun, (e.t. 28.01.2012).

Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Yves Sandoz (editör), 1987.

Cyberwar The Threat From The Internet, The Economist, 3–9 Temmuz 2010.

Çalışma Grubu 4, **E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları,** Türkiye Bilişim Derneği.

DAKOFF, Howard S., **Note, The Clipper Chip Proposal: Deciphering the Unfounded Fears That Are Wrongfully Derailing Its Implementation**, J. Marshall L. Rev., Vol. 29, Num:2, 1996, s.475–479.

DAVIS, Brown, A Proposal for an tnternational Convention To Regulate the Use of tnformation Systems in Armed Conflict, Volume 47, Number 1, Winter 2006, s.201–202, http://www.harvardilj.org/wp-content/uploads/ 2010/10/HILJ_47-1_Brown.pdf, (e.t.06.02.2012).

DAVIS, Joshua, Hackers take Down the Most Wired Country in Europe, Wired Magazine: Issue 15.09, http://www.wired.com/politics/security/magazine/1509/ff_estonia?currentPa ge=all, (e.t.28.01.2012)

DECI, E.L., R.M. Ryan, **Intrinsic Motivation and Self-determination in Human Behavior**, Plenum Press, New York, 1985, http://www.google.com.tr/ books?hl=tr&lr=&id=p96WmnER4QC&oi=fnd&pg=PA1&dq=Dec i+E.T, +Ryan, +R. M+1985+Intrinsic+Motivation+and+Selfdetermination+in+Human+Behavior &ots=3cGTx2vc 23&sig=eG5tcI60CDo0grCtd w9xai0Qw38&redir_esc=y#v= onepage&q&f=false, (e.t.29.01.2012).

DEIBERT, Ron, Rafal Rohuzinski, **Tracking GhostNET: Investigating a Cyber Espionage Network**, Information Warfare Monitor, JR02–2009, http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network, (e.t.28.01.2012).

DENNING, Dorothy E., **Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy**, 1999, http://www.iwar.org.uk/cyberterror/resources/denning.htm, (e.t. 28.01.2012).

DENNING, Dorothy E., **Hacktivism: an Emerging Threat to Diplomacy**, American Foreign Service Association, 25.06.2007, www.a fsa.org/fsj/sept00/Denning.cfm, (e.t.10.02.2012).

DENNING, Dorothy E., **Is Cyber Terror Next?**, Social Science Research Council, http://essays.ssrc.org/sept11/ essays/denn ing.htm, (e.t.02.02.2012).

DODGE, Martin, Rob Kitchin, **Mapping Cyberspace**, Routledge, London, 2001.

DÖRMANN, Knut, **Computer Network Attack and International Humanitarian Law**, International Committee of the Red Cross, 19 Mayıs 2001, http://www.icrc.org/eng/resources/documents/misc/5p2alj.htm, (e.t.06.02.2012).

DROGIN, Bob, **Russians seem to be Hacking ınto Pentagon Sensitive information taken-but nothing top secret**, Los Angeles Times, 7 Ekim 1999, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/1999/10/07/MN5855 8.DTL, (e.t. 28.01.2012).

ENGİNSOY, Umit, Burak Ege Bekdil, **Turkey Raises Emphasis On Cyberspace Defense**, Defense News, 15 Ağustos 2011, http://www. defensenews.com/story.php?i=7388376&c=FEA&s=SPE, (e.t. 03.01.2012).

ERKİNER, Hakkı Hakan, Devletin Haksız Fiilinden Kaynaklanan Uluslararası Sorumluluğu, 12 Levha Yay., , 1. Baskı, İstanbul, 2010.

GRAHAM, Bradley, **For a description of hesitancy to use CNA during Operation "Allied Force", "Military Grappling with Rules for Cyber Warfare: Questions Prevented Use on Yugoslavia"**, Washington Post, 8 Kasım 1999, http://www.washingtonpost.com/wp-srv/WPcap/1999-11/08/ 011r-110899-idx.html, (e.t. 05.01.2012).

GRAHAM, Bradley, **Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia**, The Washington Post, 8 Kasım 1999, sec. A.

GREENBERG, Andy, **America's Hackable Backbone**, 08.22.07, http:// www.forbes.com/2007/08/22/scada-hackers-infrastruc ture-tech-security-cx_ag_0822hack.html, (e.t. 28.01.2012)

GREENBERG, Lawrence t., et al., **Information Warfare and International Law 12**, National Defense University Press, , 1998. http://www.dodccrp.org/files/Greenberg_Law.pdf, (e.t.06.02.2012).

GRYC, Wojciech, **Cyber Warfare, Peace Magazine**, 2009.

GUANG, Pan, **The SCO's Success in Security Architecture (**highlighting confidence building, cooperation against destabilizing transborder elements, and the maintenance of regional security and stability as general successes of the SCO), http://epress.anu.edu.au/ sdsc/architecture/ mobile_devices/ch04.html, (e.t.07.02.2012).

HIGGINS, Kelly Jackson, **Permanent Denial-of-Service Attack Sabotages Hardware**, Dark Reading, 19 Mayıs 2008, http://archive.cert.uni-stuttgart.de/isn/2008/05/msg00102.html, (e.t.29.01.2012).

HILDRETH, Steven A., **Cyberfare Warfare 11**, Congressional Research Service Report For Congress No. RL30735, 19 Haziran 2001. http://www.fas.org/irp/crs/RL30735.pdf, (e.t.28.01.2012).

HIRSHLEIFER, J., **The bioeconomic causes of war**, Managerial and Decision Economics 19 (7/8), 1998, s.457–466, http://time.dufe.edu.cn/ spti/article/hirshleifer/hirshleifer170.pdf, (e.t.29.01.2012).

JANCZEWSKI, Lech J., Andrew M. Colarik, Managerial Guide for Handling Cyber-Terrorism and Information Warfare, Idea Group Publishing, The U.S.A, 2005.

JENSEN, Eric Talbot, **Cyber Warfare and Precautions Against the Effects of Attacks**, Texas Law Review, Vol. 88:1533.

JONES, Andrew, **Cyber Terrorism: Fact or Fiction**, Computer Fraud and Security, 2005.

JOYNER, C. Christopher, Catherine Lotdonte, **Information Warfare as International Coercion: Elements of a Legal Framework**, 12 EUR. J. INT'L L. 825–841, 2001. http://www.ejil.Org/pdfs/12/5/1552.pdf (e.t.29.01.2012).

KABAY, M. E., **Industrial Espionage, Part 8: China and Titan Rain, Network World**, 10 Kasım 2005, http://www.networkworld.com/newsletters/ 2005/1107sec2.html?page=2), (e.t.28.01.2012).

KANUCK, Sean, **Sovereign Discourse on Cyber Conflict Under Intemational Law**, Texas Law Review Association, Symposium: Law at the Intersection of National Security, Privacy and Technology: II. Cybersecurity and Network Operations, Vol. 88:1571, 2010.

KELSEY, Jeffrey T.G., **Hacking into International Humanitarian Law: The Principles of Disdinction and Neutrality in the Age of Cyber Warfare**, Michigan Law Review, Vol. 106 No:7, 2008.

KNIERIM, Tammy M., Lou Anne DeMattei ve Sebastian M. Convertino, **Flying and Fighting in Cyberspace**, Maxwell Paper No.40Air War College, Temmuz 2007. http://aupress.au.af.mil/digital/pdf/paper/mp_0040_conve rtino_demattei_knierim_flying_fighting_cyberspace.pdf, (e.t.30.01.2012).

LANGNER, Ralph, **Stuxnet: Dissecting a Cyberwarfare Weapon**, Focus, Mayıs/Haziran 2011.

LASKER, John, **U.S. Military's Elite Hacker Crew**, WIRED, 18 Nisan 2005, http://www.wired.com/politics/security/news/ 2005/04/67223, (e.t. 28.01.2012).

LAKHANI, K.R., R.G. Wolf, In: J. Feller, B. Fitzgerald, S. Hissam, K. R. Lakhani (Editörler), **Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects**, MIT Press, 2005, http://ocwmit.edu/courses/sloan-school-of-management/15-352-managing-innovation-emerging-trends-spring-2005/readings/lakhaniwolf.pdf, (e.t.29.01.2012).

LAPPIN, Yaakov, **Reuters Admits to More Image Manipulation**, YNETNEWS.COM, 7 Ağustos 2006, http://www.ynetn ews.com/articles/0, 7340, L-3287774, 00.html, (e.t.29.01.2012).

LEWIS, James A., **Computer Espionage, Titan Rain and China,** Center for Strategic and International Studies - Technology and Public Policy Program, Aralık 2005, s.1–2, http://csis.org/files/media/csis/pubs/051214_china _titan_rain. pdf, (e.t. 28.01.2012).

LEYDEN, John, **'Electronic Jihad' fails to materialise**, 26 Ağustos 2004, http://www.theregister.co.uk/2004/0 8/26/cyberfu d/, (e.t.02.02.2012).

LIANG, Qiao, Wang Xiangsui, **Unrestricted Warfare**, Beijing: PLA Literature and Arts Publishing House, Şubat 1999, http://cryptome.org/ cuw.htm, (e.t.02.02.2012).

LIBICKI, Martin C., **Cyberdeterrence and Cyberwar**, Rand Corporation, The U.S.A, 2009.

LIBICKI, Martin, **What is Information Warfare**, Strategic Forum 28, Institute for National Strategic, Studies, Mayıs 1995, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA394692, (e.t.02.02.2012).

LINDENBERG, S., **Intrinsic motivation in a new light**, Kyklos 54 (2/3), 2001, s.317–342, http://www.ppsw.rug.nl/~lindenb/documents/articles/ 2001_LindenbergIntrinsic_motivation_in_a_new_light.pdf, (e.t.29.01.2012).

MILLS, Elinor, **Google wants ability to 'combine' your user data**, CNET News, 25 Ocak 2012, http://www.zdnetasia.com /google-wants-ability-to-combine-your-user-data-62303592.htm, (e.t. 28.01.2012).

MILLS, Elinor, **Report: Turkish hackers breached U.S. Army servers**, 29 Mayıs 2009, http://news.cnet.com/8301-1009_3-10252375-83.html, (e.t.28.01.2012).

ÖZKIŞLALI, Gizem, **Küreselleşme, İnternet ve Terörizmin Değişen Yüzü; Siber Terörizm**, Yüksek Lisans Tezi, Ankara, 2008.

PARKS, Raymond C., David P. Duggan, **Principles of Cyber-warfare**, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5–6 Haziran 2001, http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20 WEBREVIEW/P rinciplesCYBER%20WARFARE.pdf, (e.t.02.02.2012).

POWER, Richard, Dario Forte, **"Ten years in the wilderness—a retrospective Part 2: Cyber Security = National Security"**, Computer Fraud&Security: War&Peace in Cyberspace, Şubat 2006.

RHO, Jennifer J., **Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute**, 7 Cffl. J. INT'L L.695, 2006–2007.

ROSENZWEIG, Paul, **National Security Threats in Cyberspace 2**, 2009, http://www.americanbar.org/content/dam/ab a/migrated/natsecurity/ threats_in_cyberspace.authcheckdam.pdf, (e.t.07.02.2012).

SCHAAP, Arie J., **Cyber Warfare Operations: Development and Use Under International Law**, Air Force Law Review, Vol. 64, 2009.

SCHMITT, Michael N., **Wired warfare: Computer network attack and jus in bello**, RICR Juin IRRC Haziran 2002 Vol. 84 No. 846. http://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf, (e.t.08.08.2011).

SCHWARTZ, Peter, **Warrior in the Age of Intelligent Machines**, Wired Magazine, Nisan 1995, http://www.wired.com/wire d/archive/3.04/pentagon_ pr.html, (e.t.02.02.2012).

SCOTT, Roger D., **Territorially Intrusive Intelligence Collection and International Law**, 46 A.F. L. Rev. 217, 1999.

SHARMA, Amit, "Cyber Wars: A Paradigm Shift from Means to Ends", Strategic Analysis, 34:1, 2010, http://dx.doi.org/10.1080/ 09700160903354450, (e.t.20.01.2012).

SHAY, Shaul, **Netwars and Networks**, Mark Last ve Abraham Kandel (editör), Fighting Terror in Cyberspace içinde (33), World Scientific Publishing, The U.S.A, 2005.

SINROD, Eric J., William P. Reilly, **Cyber-Crimes: A Practical Approach To The Application Of Federal Computer Crime Laws**, Santa Clara University School of Law, Volume 16, Num.2, Mayıs 2000, s.12–16, http://www.sinrodlaw.com/CyberCrime.pdf, (e.t.29.01.2012).

SPIEKER, Heike, **Civilian Immunity**, in Crımes of War 84, 84 (Roy Gutman & David Rieff eds. 1999), s.84, http://www.crimesofwar.org/a-z-guide/civilian-immunity/, (e.t.14.02.2012).

STRELSOV, A.A., **International information security: description and legal aspects**, icts and international security. http://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2642.pdf, (e.t.10.02.2012).

STRELTSOV, A.A., **International Information Security: Description and Legal Aspects**, DISARMAMENT F., 2007 (Issue 3). http://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2642.pdf, (e.t.08.02.2012).

Sun Tzu, The Art of War, çeviren: Samuel B. Griffith, Oxford University Press, Oxford, 1963.

SWARTZ, Jon, **Crooks slither into Net's shady nooks and crannies; Crime explodes as legions of strong-arm thugs, sneaky thieves log on,** USA Today, 21 Ekim 2004, www.usatoday.com/printedition/money/20041021/cybercrimecover.art. htm, (e.t.10.02.2012).

TÜTÜNCÜ, Ayşe Nur, İnsancıl hukuka Giriş, Beta Yay., İstanbul, 2006.

TRAYNOR, Ian, **Russia accused of unleashing cyberwar to disable Estonia**, The Guardian, http://www.guardian.co.uk/wo rl d/2007/may/17/topstories3.russia, (e.t. 28.01.2012)

TREMLETT, Giles, **Turkish arrests intensify global war between hacker activists and police**, The Guardian, 13 Haziran 2011, http://www.guardian.co.uk/technology/2011/jun/13/ turkish-arrests-global-war-hackers-police, (e.t. 03.01.2012).

Türk Asya Stratejik Araştırmalar Merkezi, **Siber Terörizm Raporu**, Stratejik Rapor No: 2 Aralık 2004.

Türkçe Sözlük, Türk Dil Kurumu, 9. Baskı, Ankara, 1998.

UZUN, Elif, Milletlerarası Hukuka Aykırı Eylemlerinden Dolayı Devletin Sorumluluğu, Beta Yay., 1. Basım, İstanbul, 2007.

VERTON, Dan, **Lack of Incident Reporting Slows Cybercrime Fight**, 31 Ekim 2002, http://computerworld.com/securityto pics/security/cybercrime/story/0, 10801, 75532, 00.html, (e.t.10.02.2012).

WALKER, George K., Information Warfare and Neutrality, Vanderbilt Journal of Transnational Law, 2000, http://findarticl es.com/p/articles/mi_hb3577/is_5_33/ai_n28809531/, (e.t.06.02.2012).

WALKER, Jeffrey K., **The Demise of the Nation-State, The Dawn of New Paradigm Warfare, and a Future for the Profession of Arms**, 51 A.F. L. REV. 323, 2001, s.337–38, http://www.afjag.af.mil/shared/media/document/AFD-081204-028.pdf, (e.t.06.03.2012).

WATTS, Sean, Combatant Status and Computer Network Attack, 3 Ağustos 2009, Virginia Journal of International Law, Vol. 50, No. 2, s. 392–393, 2010, http://ssrn.com/abstract=1460680, (e.t.08.02.2012).

WEARDEN, Graeme, **Cyberterrorists poised to attack', warns Labour peer**, 28 Nisan 2005, http://www.silicon.com/tec h nology/security/2005/04/28/cyberterrorists-poised-to-attack-warns-labour-peer-391 29961/, (e.t.02.02.2012).

WLINGFIELD, Thomas C., **The Law Of Information Conflict: National Security Law In Cyberspace 17**, Aegis Research Corp., 2000.

WILLIAMS, P., **Organized crime and cybercrime: synergies, trends, and responses**, 13 Ağustos 2001, Office of International Information Programs, U.S. Department of State, http://usinfo.state.gov, (e.t.05.01.2012).

WILSON, Clay, **Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress**, CRS Report for Congress, Order Code RL32114, 17 Ekim 2003. http://fpc.state.gov/documents/organization/45184.pdf, (e.t.02.02.2012).

WOLTAG, Johann-Christoph, Cyber Warfare, Max Planck Encyclopedia of Public International Law, Rüdiger Wolfrum (editör), Oxford University Press, 2010.

ELEKTRONİK KAYNAKLAR

Air Force Policy Directive 10–7, 6 Eylül 2006, http://www.survivalebooks.com/free%20manuals/2006%20US %20Air%20Force%20INFORMATION%20OPERATIONS%2027p.pdf, (28.01.2012).

A Proposal for an International Convention on Cyber Crime and Terrorism, Ağustos 2000, http://www.iwar.org.uk /law/resources/cybercrime/stanford/cisac-draft.htm, (e.t.02.02.2012).

Birleşmiş Milletler Antlaşması (BM Şartı), http://www.belgenet.com/arsiv/sozlesme/bmsarti-01.html, (e.t.30.01.2012).

CERT Coordination Center, http://www.cert.org/tech_tips/denial_of_service.html, (e.t.29.01.2012).

Convention on Cybercrime, Council of Europe, http://conventions.coe.int/ Treaty/en/Treaties/html/185.htm, (e.t.30.01.2 012).

Convention on Prohibitions or Restrictions on tbe Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, 10 Ekim 1980, S, TREATY Doc. No. 103–25 (1994). 1342 U.N.T, S. 137, http://www.icrc.org/eng/resources/documents/publication/p0811.htm, (e.t.08.02.2012).

Convention Conceming the Rights and Duties of Neutral Powers in Naval War, madde 10, 18 Ekim 1907, http://www.icr c.org/ihl.nsf/FULL/240, (e.t.11.02.2012).

Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 Ağustost 1949, madde 4 (A) (2), http://www.icrc.org/ihl.nsf/FULL/375, (e.t.07.02.2012).

Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, 12 August 1949, madde 28, http://www.icrc.org/ihl.nsf/full/380, (e.t.07.02.2012).

Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, 18 Ekim 1907, http://www.icrc.org/ihl.nsf/full/200?opendocument, (e.t.06.02.2012).

Council of Europe, **Convention on Cybercrime**, opened for signature:11 Kasım 2001, Europ. T.S. No. 185, http://conve ntions.coe.int/treaty/en/treaties/html/185.htm, (e.t.07.02.2012).

Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, United Nations General Assembly, A/RES/58/199, Fifty-eighth session, 30 January 2004, http://www.itu.int/ITU-D/cyb/cybersecurit y/docs/UN_resolution_58_199.pdf, (e.t.12.02.2012).

Department of Defense, **Dictionary of Military and Associated Terms Joint Publication 1–02**, (JP 3–13), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, (e.t. 28.01.2012).

Department. of the Air Force, Policy Directive 51–4, Compliance with the law of armed conflıct, 1993, .http://www.icrc.org/ihlnat.nsf/6fa4d35

e5e3025394125673e00508143/cfaff63edde42523c1256a8e00342cfb!OpenDocument, (e.t.06.02.2012).

Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, 8 Haziran 2000, 39 I L M 1257., http://www.icty.org/sid/10052, (e.t.06.02.2012).

Geneva Convention Relative To The Treatment Of Prisoners Of War of 12 Ağustos 1949 (Geneva Convention III), http://protection.unsudanig.org/data/legal/Third%20Geneva%20Convention%20 (POW), %2019 49.pdf, (e.t.02.02.2012).

Hacker Attacks in US Linked to Chinese Military: Researchers, 12 Aralık 2005, http://seclists.org/isn/2005/ Dec/0059.html, (e.t.29.01.2012).

http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf?OpenElement, (e.t.31.01.2021).

http://www.digitalbroadcasting.com/storefronts/pvimage.html, (e.t.29.01.2012).

http://www.fbi.gov/publications/leb/2002/june2002/june02leb.htm, (e.t.10.02.2012).

http://www.itu.int/net/about/basic-texts/constitution/chaptervi.aspx, (e.t.31.01.2012).

http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf, (e.t. 28.01.2012).

http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf, (e.t.31.01.2012).

ICRC, **International Humanitarian Law - Treaties & Documents**, http://www.icrc.org/ihl.nsf/WebART/1952 00034?Ope nDocument, (e.t.29.01.2012).

Information Assurance – the Achilles' Heel of Joint Vision 2010?, 2 Mart 1999, http://www.airpower.au.af. mil/airchr onicles/cc/ashley.html, (e.t.02.02.2012).

INTERPOL, **Secure Global Police Communications Services**, https://www.interpol.int/Public/ICPO/corefunct ions/secu recom.asp, (e.t.06.02.2012).

Introduction to Computer Viruses, S0PH0S.COM, 26 Mayıs 1998, http://www.sophos.com/en-us/press-office/press-releases/1998/05/va_virusesintro.aspx, (e.t.29.01.2012).

Joint Chiefs Of Staff, Joint Publication 1-02, Department Of Dhf. Directive Of Military &Assoc'D Terms, 12 Nisan 2001, s.190, http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02 (01).pdf, (e.t.29.01.2012).

Joint Doctrine for Information Operations, Joint Pub. 3–13, 9 Ekim 1998, s.1–136, http://www.c4i.org/jp3_13.pdf (e.t.29.01.2012).

Joint Publication 3–13, **Information Operations**, 13 Şubat 2006, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, (e.t.30.01.2012).

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257, July 8, http://ww w.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&p3=4&case=95, (e.t.14.02.2012).

M/Cyclopedia of New Media, Digital Manipulation, http://www.fourandsix.com/photo-tampering-history/, (e.t.29.01.2012).

Official Records Of The Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Volume 1, Federal Political Department, (Geneva, 1974 -1977), Bern, 1978, http://www.loc.gov/rr/frd/Military_Law/pdf/RC-records_Vol-1.pdf, (e.t.11.02.2012).

On Bush's Watch, **U.S. Suffered Its "Electronic Pearl Harbor**, 3.18.2010, Güncelleme: 5.25.2011, http://www.huffingt onpost.com/2009/ 11/10/on-bushs-watch-us-suffere_n_352204.html, (e.t.30.01.2012).

Photo Alteration, http://www.espionageinfo.com/Pa-Po/Photo-Alteration.html, (e.t.10.02.2012).

Photo Tampering throughout History, http://www.fourandsix.com/ photo-tampering-history/, (e.t.29.01.2012).

Proceedings of European Conference on Information Warfare and Security 2002, 2003, http://books.google. com.tr/b ooks?hl=tr&id=EvsP IeM4w5AC&q=cyber#v=onepage&q=conferences&f=false, (e.t.02.02.2012).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 Haziran 1977, http://www.icrc.org/ihl.nsf/full/470?op endocument, (e.t.07.02.2012).

Reducing On-line Credit Card Fraud, Web Developers Journal, http://www.webdevelopersjournal.com/article s/card_fra ud.html, (e.t.10.02.2012).

Report of the International Law Commission on the work of its fifty-third session, DOCUMENT A/56/10, madde 1, (23 Nisan–1 Haziran ve 2 Temmuz–10 Ağustos 2001), http://untreaty.un.org/ilc/reports/2001/200 1report.htm, (e.t.13.02.2012).

SearchSecurity.com, **Definitions, IP Spoofing**, http://searchsecurity. techtarget.com/definition/IP-spoofing, (e.t.29.01.2012).

SearchSecurity.com, **Trojan Horse**, http://searchsecurity. techtarget.com/definition/Trojan-horse, (e.t.29.01.2012)

Security for the Next Generation, The National Security of the United Kingdom, Güncelleme:2009, Cabinet Office, Haziran 2009, http://www.official-documents.gov.uk/document/cm75/7590/7590.pdf, (e.t.02.02.2012).

Statute of the International Law Commission, 1947, http://untreaty. un.org/ilc/texts/instruments/english/statute /statute_ e.pdf, (e.t.07.02.2012).

Techterms.com, The Tech Terms Computer Dictionary, **Malware**, http://www.techterms.com/definition/malwar e, (e.t.29.01.2012).

The Guardian, 15 Ağustos 2003, http://www.guardian.co.uk/news/ 2003/aug/15/informer, (e.t.02.02.2012).

The Secretary-General, **Developments in the Field of Information and Telecommunications in the Context of International Security**, delivered to the General Assembly, U, N, Doc. A/62/98, 2 Temmuz 2007, http://www.disarmament. un.org/library.../a-62-98.pdf, (e.t.08.02.2012).

The White House, **Remarks By The President On Securing Our Nation's Cyber Infrastructure**, Office of the Press Secretary, 29 Mayıs 2009, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyberinf rastructure, (e.t.29.01.2012).

Turkey conducts cyber terror drill, Hurriyet Daily News, 27 Ocak 2011, http://www.hurriyetdailynews.com/n.P?n=turke y-conducts-cyber-terror-drill-2011-01-27, (e.t. 03.01.2012).

U.S. Department Of Defence, **Information Operations Roadmap 1**, 30 Ekim 2003, s.1–72, http://www.gwu.edu/~nsarc hiv/NSAEBB/NSAEBB177/ info_ops_roadmap.pdf, (e.t.28.01.2012).

U.S. Department of Defense, Directive IR. 3600.1, **Information Operations**, 14 Ağustos 2006, http://www.Fas.org/irp/do ddir/dod/info_ops.pdf, (e.t.29.01.2012).

White House. **Cyberspace Policy Review**, 2009, http://www. whitehouse.gov/assets/documents/Cyberspace _Pol icy _ Review_final.pdf, (e.t.08.02.2012).

12 Ağustos 1949 Tarihli Cenevre Sözleşmelerine Ek Uluslararası Silahlı Çatışmaların Kurbanlarının Korunmasına İlişkin (1) No.lu Protokol, 8 Haziran 1977, http://www.kizilay.org.tr/hukuk/sayf a_yazdir.php?t=-Ulusal.ve.Uluslararasi.Sozl esmeler-CENEVRE.EK.1.PROTOKOL, (e.t.06.02.2012).