ISSN: 2587-1218

SİBER ÇATIŞMALARIN TANIMLAMA SORUNU

Gül Nazik ÜNVER[♣]

"Bir Tanım Seçmek Bir Nedeni Savunmaktır."
Charles Leslie Stevenson (1908-1979)

Özet

Son yirmi yılda yaşanan gelişmeler, insan yapımı yeni bir çatışma alanı ortaya çıkarmıştır. Kara, deniz, hava ve uzay alanlarında silahlı çatışmaların yanı sıra, farklı siyasal aktörler arasındaki çatışmalar, artık siber uzayda yer almaya başlamıştır. Siber çatışmalar, çeşitli değişkenlerin -teknolojik, sosyal ve entelektüel- değişen ilişkilerinden dolayı ortaya çıkmaktadır. Belirli bir kuvvet, eğilim, hareket veya politikadaki değişim, siber çatışmayı oluşturabilir. Siber çatışmalar farklı nedenlere bağlı olarak zaman zaman artışlar ya da azalmalar göstermektedir. Siber çatışmaların tanımlanmasındaki sorunlar hakkında kesin bir değerlendirme yapmak zor olsa da, siber operasyonların daha önemli hale gelmesi sadece bir zaman meselesi olmaktadır. Yapılacak her tanımlama, siber çatışmaların bir boyutunu dışarıda bırakacaktır.

Bu çalışmanın ana amacı, dijitalleşen dünyada siber çatışmaların tanımlama sorunları hakkında "NATO Uluslararası Siber Çatışma Konferanslarını" incelemekte ve siber çatışmaların hem teknik hem de toplumsal bakış açılarındaki unsurlarının kapsamlı bir analizine dayanmaktadır. Son olarak çalışma, en ciddi tehdidi getiren ve etkisi kitle imha silahları ile karşılaştırılabilir olabilen, modern savaşın en gelişmiş biçimi olarak siber çatışmayı değerlendirmek için bir fırsat sunmaktadır.

Anahtar Kelimeler: Siber Uzay, Siber Çatışma, İnternet, Siber Terörizm, Dijitalleşme.

♣ Doktora Adayı, Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler ABD, gulunver@outlook.com.

Abstract

The developments in the last two decades have revealed a new area of human-made conflict. Armed conflicts in land, sea, air and space areas, as well as conflicts between different political actors, are now beginning to take place in cyberspace. The cyber conflicts arise due to the changing relations of various variables - technological, social and intellectual. Any change in a particular force, tendency, movement, or policy can create a cyber conflict which occasionally increase or decrease depending on different reasons. While it is difficult to make a definitive assessment of the problems with identifying cyber conflicts, it is only a matter of time before cyber operations become more important. Every definition to be made will exclude a size of cyber conflicts.

The main aim of this work is to examine the "NATO International Conference on Cyber Conflicts" on the identification problems of cyber conflicts in the digitalizing world and to rely on a comprehensive analysis of the elements of both cyber space and cyber conflicts. Finally, the study presents an opportunity to evaluate cyber conflict as the most advanced form of modern warfare, which brings the most serious threat and can be comparable to weapons of mass destruction.

Keywords: Cyber Space, Cyber Conflict, Internet, Cyber Terrorizm, Digitization.

1. Giriş

Uluslararası ilişkiler teknolojiden genellikle derin bir şekilde etkilenmiştir. Okyanustan geçen yelkenli gemiler, 16-18. yüzyıllarda Avrupa'nın genişlemesini sağlamıştır. Telgraf 19. yüzyıl imparatorlukların gelişmesinde katkıda bulunmuştur. Uçak, radyo ve televizyon 20. yüzyılda uluslararası ilişkilerin etki alanını değiştirmiştir. İnternet ise dünya için yeni bir dizi fırsat ve risk ortaya çıkarmaktadır. Bilgi (IT) sistemleri, insanların hem birebir hem de birden çok iletişim kurma yeteneğinde bir kuantum sıçraması oluşturmaktadır. İnternetin diğerlerinden temel farkı, değişikliklerin daha hızlı gerçekleşmesidir. İnternet eylemcilerin bilgileri toplamasına ve yayınlamasına, diyaloga girmesine, eylemlerini koordine etmesine ve gücü elinde bulunduranlara lobi yapmasına izin vermektedir.

Siber çatışma, siber bilgi savaşı, suç faaliyetleri (terörizm dahil), gizli operasyonlar ve önleyici askeri güç kullanma kabiliyetleri, uluslararası toplumun bunları yönetmek için kararlaştırılmış kurallar oluşturma kapasitesinden daha hızlı yayılmaktadır. Siber yetenekler daha hızlı ortaya çıkabilir ve gelişebilir; nükleer santraller ve silahlar, hava taşımacılığı, radyo vb. gibi öncekilere göre daha kapsamlı ve hızlı bir şekilde yayılabilir. Siber yetenekler, önceki teknolojilere göre coğrafi olarak daha az sınırlıdır. Bununla birlikte, devletlerin ve toplumların doğal çıkarları, bu yeni kabiliyetleri yönetmeye yönelik normların ve kuralların, uygulamalarının kusurlu olmasına rağmen, teklif edilmesi, müzakere edilmesi ve nihayetinde üzerinde anlaşmaya varılması gerektiğini dikte etmektedir. Zira, çoğu devlet ve toplum için tehdit edici faaliyetlerin tehlikeleri ve maliyetleri çok ağır olacaktır. Son on yıl boyunca, küresel sosyal ve politik manzaralar, Bilgi ve İletişim Teknolojilerinin (BİT) devrimci gelişimi tarafından değişime uğramaktadır. Yeni Bilgi ve İletişim Teknolojileri, ağ merkezli savaş doktrini ve alışılmamış, bilgi ve asimetrik savaşın ortaya çıkmasıyla diğer yolların yanı sıra savaşları da önemli ölçüde etkilemiştir. Siber savaş, askeri düzeyde bilgiye dayalı çatışmayı ifade ederken, ağ bağlantılı savaş çoğunlukla düşük yoğunluklu çatışmalarla ilişkilendirilen toplumsal mücadeleler için geçerlidir (Brose, 2015: 26).

Uluslar, gelecek çatışmaları daha fazla kontrol altına almak için tıpkı daha geleneksel savaşların anlaşmalar, sözleşmeler ve normlar yoluyla sınırlandırıldığı gibi giderek daha fazla çatışmaya yönelmektedir (Cycon, 2011: 21). Ancak, eski anlaşmaların ne kadar iyi tutacağı, siber uzayın ve siber çatışmaların doğası gereği ne icat edilmesi gerektiği hala bilinmemektedir. Günümüzde gelişmiş ulusların karşılaştığı siber çatışmaların çoğunda, bir aktörün siber uzayda düşmanca müdahaleleri seçmeyi tercih etmesini engellememekte, ancak çok başarılı olan müdahaleleri durdurmaya zorlamaktan alıkoymaktadır (Cycon, 2012: 126).

1999 Kosova operasyonu, NATO'nun siber çatışma ile ilgili ilk deneyimi olarak etkili olmuştur. NATO'nun Kosova Savaşı esnasında mail sunucuları hedef alınmıştır. Bu çatışma sırasında, her taraftaki eylemciler ve saldırganlar örgütü yaymak ve / veya propaganda yapmak için kullanılmasının yansıra temel hedef NATO'nun hava saldırısını durdurmak olmuştur. Ayrıca, dikkate değer bir dizi web sitesi protesto ve propaganda amaçları için hırsızlıklar ve bozulmalar yaşanmıştır. Bazı durumlarda, hacktivistler virüs yüklü ekler göndermiştir. Çatışmanın hemen önündeki partilerin ötesinde, Belgrad'daki Çin

Büyükelçiliği'nin kazara ABD'yi bombalaması sonrasında Çin'den hackerlar dâhil olmuştur (Denning, 2001: 239-240).

Estonya'ya yönelik 2007'deki siber saldırı, siber çatışmada NATO'nun en bilinen olayı olmuştur. Sovyet savaş anıtının taşınma kararının alınması ile birlikte saldırılar başlamış, Estonya'daki etnik Ruslar protestolar için sokaklara çıkmışlardır. Protestolar çevrimiçi olarak yayılmıştır (Erendor, 2017:114-133). Tallinn'deki NATO Kooperatifi Siber Savunma Merkezi'nin (CCDCOE) Rain Ottis (2010: 72) raporuna göre; "Siber saldırıların Estonya'daki insanlara doğrudan etkileri minimal olmuş ve çoğu durumda var olmamıştır. Altyapı hizmetleri kalıcı olarak etkilenmiştir." Bununla birlikte, saldırılar hem Estonya hem de NATO için "uyandırma çağrısı" olmuş ve her ikisi için de politikadaki değişikliklere yol açmıştır (Lawson, 2012: 3). 2013 yılında gerçekleşen Uluslararası Siber Çatışma Konferansı'nda, Kalm; siber çatışmanın ve siber suçun tanımları üzerine tartışma çok fazla olduğundan, aralarında ayrım yapmamıştır. Aksine, herhangi bir siber çatışmanın teknoloji tarafından sağlanan suç eylemlerinden oluştuğunu varsaymıştır. Farklı suç eylemleri farklı örgütsel yapılar gerektirdiğinden siber uzayda gizli ağlar çeşitli biçimlerde olabilir (Kalm, 2013: 218). Devlet destekli siber suç örgütleri siber çatışma bağlamında en ağır tehditleri uyguladıkları için diğer türden gizli ağlara maruz kalan pek çok özellikten yoksun kalmışlardır. Devlet destekli siber suçlar çoğunlukla casusluk ve teknik operasyonları içerdiğinden, önemli miktarda kaynak gereklidir (Kalm, 2013: 224).

Çatışma, çok boyutlu ve çok kapsamlı bir kavram olarak disiplinden disipline farklı tanımlara sahiptir. Yapılacak her tanımlama, çatışmanın bir boyutunu dışarıda bırakacaktır (Akyeşilmen, 2013: 449). Genel itibariyle çatışma terimi ifade, görüş, menfaat, gaye veya değerler arasındaki karşıtlık veya uyumsuzluktur. Çatışmaların iki yönü vardır. Bunların birincisi taraflar arasındaki menfaat ya da fikir uyuşmazlığıdır. Diğeri ise bu anlaşmazlıkların fiziki müdahaleye başvurma ya da tartışmalar yoluyla gözlemlenebilir "çatışma davranışı" olarak ortaya konmalarıdır. Çatışma davranışı sergilemek, iletişim aracılığıyla veya güç kullanarak tarafların ihtilaflarını dile getirmeleri anlamına gelmektedir (Tekin, 2013: 87). Çatışma terimi ile ilgili yapılan tanımlamaların ortak noktası, aslında mücadele eden en az iki tarafın varlığı, bu iki taraf arasında bir tür karşılıklı bağımlılığın bulunması ve tarafların amaçlarına ulaşmasında diğer tarafın önleyici bir unsur olduğu algısının oluşmasıdır (Akyeşilmen, 2015: 42-43). Siber uzayda bireyler ve aktörler giderek yaygınlaşırken,

yaşanan her çatışma sorun haline gelmiştir. Bu nedenle konu ile ilgili literatür taraması yapılmakta ve çalışmanın yanıt aradığı temel sorular şu şekilde sıralanmaktadır:

Siber alanda sayısız çatışma varken ve giderek farklı türde çatışmalar ortaya çıkarken bu disiplinin tanımlanamaması sorun teşkil eder mi? Ya da genel bir tanım yapılması, giderek genişleyen siber uzayda yeterli kalabilir mi? Çatışma ne zaman başlamıştır? Şu an çatışmanın durumu nedir?- hangi safhadadır? United Nations Development Programme (UNDP)'ye göre çatışma çok boyutlu bir fenomen olduğundan tek bir faktörle açıklanamamaktadır. Siber çatışmayı etkileyen ve zorlaştıran en önemli unsur aslında sayılamayacak kadar çok olan, herkese göre değişebilen ve aysberg misali büyük bir kısmı görünmez olan nedenlerdir (Akyeşilmen, 2013: 9-10).

"NATO Uluslararası Siber Çatışmalar Konferansında" siber çatışmaları önlemek ve barışçıl bir çözüm bulmak adına ne gibi çalışmalar yapmaktadır? Peki devlet egemenliğinin ve hukuki yaptırımın oldukça güçlü olduğu iç meselelerde/sorunlarda siber çatışmalar tanımlanamaz olması nasıl açıklanabilir? Siber çatışmalar devletlerarasındaki çatışmalar seviyesini artırıyor mu?, yoksa *siber olayın ya da anlaşmazlığın türü ve şiddeti temelinde farklı çatışma ya da işbirliği dinamikleri var mıdır?* Siber kötülük, (DDoS) saldırılarının yalnızca devletlerarasındaki çatışma-işbirliği dinamiklerini etkilediği görülmüştür (Maness and Valeriano, 2015: 2). Her ne kadar bazı teorisyenler siber çatışma ve siber savaşı epistemolojik farklılıklarına bakılmaksızın birçok kez beraber aynı cümlede, hatta çoğu kez birbirinin yerine dahi kullanmaktadır. *Bu kadar geniş yelpazeye sahip bir alanı kapsayan çatışma yönetimine göre siber çatışma nedir? Çatışmanın çeşitleri var mı? Siber Çatışma sınıflandırılabilir mi? Siber çatışma, ulus-devletlerde ne gibi zararlara sebep olmaktadır?* Bu sorular gibi daha fazla pek çok soruya cevaplar verilmeye çalışılacaktır.

Siber uzayda şiddet içerikli kafa karışıklıklarının değerlendirilmesinin üzerinde durulduğu "Conflict Barometer"'de iddia edilen taraflar arasındaki somut eylemler ve iletişim, araçların nitel ve nicel göstergelerini ve şiddetin sonuçlarını birleştirerek değerlendirmektedir. Bu yaklaşım, özellikle şiddetlerle ilgili olarak, daha geniş ve daha ayrıntılı bir ampirik temele ilişkin politik karışıklıkların analizini vermektedir. Bu, sunulan söz konusu bilginin doğruluğunu, güvenilirliğini ve tekrarlanabilirliğini daha da geliştirmeyi amaçlamaktadır. Bu nedenle siber çatışmayı incelerken, 2017 yılına kadar Heilderberg Enstitüsü'nde yapılan

(Conflict Barometer 1992'den bu yana, çatışma süreçlerine odaklanarak örneğin savaşın zayiatının tamamen nicel eşiklerinden ziyade siyasi anlaşmazlıkları analiz etmiştir.) uluslararası çatışmaları ele almak gerekmektedir (https://hiik.de/conflict-barometer/, er.tar.: 22.04.2018). Çalışma siber çatışmada devletlerin karşılaşabileceği ve siber operasyonların rol oynayabileceği bir dizi yüzleşme ve karmaşıklık ihtimallerine anlam çıkarmak için geniş bir tarih yelpazesinden analojileri araştırmaktadır. Dahası siber çatışma olaylarını, bunlara dâhil olan aktörleri ve araştırmacılar tarafından yararlı olacak şekilde tanımlamaların ötesinde yaşanan sorunlara ilişkin inceleme yapmaktadır. Bu çalışmanın amacı, siber çatışmanın NATO'nun ele almaya çalıştığı güçlüklere karşı genel bir bakış sağlamaktır. Çatışma tanımlanabilir mi / tanımlanamaz mı, çatışmanın çeşitleri ve sınıflandırılması üzerine kısaca değinilmektedir. Ardından ilgili kuruluşlar, ilkeler ve faaliyetler dâhil olmak üzere, NATO'nun mevcut siber çatışmayla ilgili duruşunun kısa bir özetini sunmaktadır. Son olarak, NATO'nun siber çatışmanın ortaya çıkmasına tepki verme girişimlerinde karşılaştığı zorlukların sadece bir kısmını vurgulamaya çalışmaktadır.

Çatışma Nedir? (Siyasi, Ekonomik, Kültürel Açıdan Siber Çatışma)

İnternetin gelişiminin ilk zamanlarında siber saldırılar çoğunlukla nispeten küçük bilgisayar korsanlarına prestij kazandırmak amacıyla gerçekleştirilmiştir. Ancak son 20 yılda siber saldırılar hızla gelişmiştir. Suçlular giderek finansal kazanımlar elde etmek için siber saldırılardan yararlanmışlardır. Hacktivistler siyasi hedeflerini ilerletmek için dijital grevlere güvenmişlerdir. Devletler güvenlik politikalarını gerçekleştirmek için siber saldırıları kullanmaya başlamışlardır. Ama siber çatışmalar neden bu kadar çekici olmaktadır? Siber uzay, onu özellikle saldırganlar için çekici bir alan haline getiren benzersiz özellikler sunmaktadır. Bu tartışmanın üç yönü öne çıkmaktadır: ilişkilendirme sorunu, coğrafi mesafenin ilgisizliği ve nispeten düşük maliyetler. Temel internet protokolleri kurulduğunda, kullanıcı topluluğu çok kısıtlı olduğundan güvenlik endişe vermemiştir. İnternetin geliştirilmesinin amacı, ağın parçaları çalışmadığı zamanlarda bile varış noktasına bilgi verebilecek esnek bir iletişim ağı kurmak olmuştur. Dolayısıyla, bir mesajın göndericisini güvenilir bir şekilde doğrulamaya veya alınan yol verisini takip etmeye gerek yoktu. Bu nedenle, özellikle bir saldırının nereden geldiğini belirlemek teknik olarak zor olmaktadır. Ayrıca, bir saldırının belirli bir konumdan / ülkeden geldiğine dair makul bir kanıt olsa bile,

onu kimin yaptığını bilmenin neredeyse hiçbir yolu yoktur (bireysel bir hacker, suçlular veya bir devlet ajanı). Siber saldırıların teknik olarak nerden geldiği ve kimin/kimlerin yaptığı belirsiz olduğundan, çoğu zaman teknik olmayan akıl yürütme (örneğin saldırının gerçekleştiği ve kimin bundan yararlanacağı) ile desteklenmektedir (Conflict Barometer, 2017: 36-38).

Çatışma kavramsal açıdan genelde uzun süren bir anlaşmazlık veya tartışma olarak tanımlanmaktadır. İki ya da daha fazla aktör çatışıyorsa, ciddi bir anlaşmazlık ya da tartışma konusu olabilir. Bu tür çatışma süreçleri henüz anlaşmaya varılmazsa kanlı çatışmaya / savaşa dönüşebilmektedir. Siber çatışmalar için ortak bir tanım yoktur. Giderek yaygınlaşmasına rağmen farklı uluslar / kuruluşlar tarafından farklı şeyler anlamına geldiği anlaşılmaktadır. Bu durum göz önüne alındığında, ulusların / devletlerin ve farklı kurumların siber çatışma terimini nasıl yorumlayacağını ve siber çatışmalara nasıl yaklaştığını gösteren tek bir tanım bulunmamaktadır. Amerika ve Rusya'da ortak ifade edilen siber çatışma tanımı; karşılıksız siber saldırıların yeniden meydana geldiği ulus devletler ve / veya örgütlü gruplar arasında ve / veya aralarında gergin bir durum olarak tanımlanmaktadır (Godwin vd., 2014: 38). Rusya ve Amerika Birleşik Devletleri gibi iki ülke tarafından siber çatışmanın kritik terminoloji tanımları üzerinde anlaşmalar yapmak, Doğu-Batı köprüsü daha önce bulunmadığı bir atılımdır. Aynı zamanda, kültürel ve politik bakış açılarının eşitsizliği ile anlaşma sağlanabiliyorsa, o zaman tanımların farklı kültürler ve politik görüşlere sahip başka ülkeler tarafından kullanılabileceği de ileri sürülebilir (Godwin vd., 2014: 64). Nicholson'a göre çatışma, çarpışma rotası anlamına gelir; aynı zamanda mevcut görüşe, duruşa veya pozisyona muhalefet anlamına da gelir (Nicholson, 1992).

Aşırı ve dinsel bir perspektiften bakıldığında, çatışma insanın iki doğasından birini temsil eder: "kötülük". İşbirliği, tam tersi, insanın "iyi" doğası olan ikincisini temsil eder. Çatışma böylece anlaşmazlık, öfke, kavga, nefret, yıkım, ölüm veya savaşta kendini gösterir. Siyasi veya sosyal ortamı şekillendirme kapasitesine sahip, herhangi bir tavizsiz tavır çatışmasıyla sonuçlanacaktır. Açgözlülük, öz-merkezlilik, hoşnutsuzluk, kıskançlık, kibir, kabalık, dokunulmazlık, diğer eylemlerin yanı sıra, insan ilişkilerinin bir kopuşunu üretme yeteneğine sahiptir. Bir bakıma, bu ahlaksızlık, insanın "çatışma doğasının" doğuştan gelen nitelikleridir. Çatışma, çoğu zaman sona eren farklı ya da benzer siyasi grupların çapraz amaçlarının bir gösterisidir (Folarin, 2013:3).

Siber suçun doğası hakkında konuşamayız, ancak devletler ve bağlı kuruluşlar arasındaki uluslararası etkileşimlerin doğasıyla ilgili olarak, uluslararası rakipler arasındaki siber ihtilafın doğasına doğrudan beslenen bu olayları analiz etmek için bir tarih, kaynak ve yöntem vardır. Siber çatışma devletler veya bireyler tarafından devletlere karşı kullanılan bir dış politika aracıdır (Maness and Valeriano, 2015: 3). 2011'de ABD hükümeti, geleneksel askeri araçlarla cezalandırılabilen bir savaş eylemine benzer bir siber olayı ilan etmişti. Bu önemli bir adım oldu. Çünkü siber uzayda, kinetik bir formda fiziksel olmayan bir olaya karşı tepkiye izin vermektedir. Çatışma daha sonra siber uzaydan geleneksel formlara geçmiştir (Maness and Valeriano, 2015: 4). Siber operasyonlar, siber suçlar ve bir devletin diğerine karşı yönelttiği diğer siber faaliyetler, artık normal ilişkilerde çatışma ve çatışmanın bir parçası olarak kabul edilmektedir. Clarke ve Knake'nin (2012: 1) iddia ettiği gibi, "siber savaş, patlayıcılar, mermiler ve füzelerle daha geleneksel mücadelenin gerçekleşme olasılığını artırabilir." Clarke ve Knake, siber tartışmayı dönüşümsel olarak şekillendiğini belirterek; "böyle bir çatışma dünya askeri dengesini değiştirir. Böylece politik ve ekonomik ilişkileri temelde değiştirme potansiyeline sahip olabileceği güvenilir bir olasılık var olur", demiştir (Clarke and Knake, 2012: 32). Kello, siber alanın, politik bozukluk ve stratejik istikrarsızlık için mükemmel bir üreme alanı olduğunu belirtmiştir. Bir başka tanım ise siber çatışma terimini, bilgisayar aracılı ortamlarda siyasal çatışma olarak ifade etmiştir. İki biçim alır: etnik (dini hayatta olduğu gibi siber uzayda savaşan iki etnik veya dini grup) ve sosyopolitik (düşmanca kurumlara karşı toplumsal hareketler) (Karatzogianni, 2005: 7-8). "Gerçek" politik çatışmaları analiz etmek için, siyaset bilimcileri "Çatışma Kuramı" ve "Uluslararası Çatışma Analizi"ni geliştirmişlerdir. Çatışma teorisini kullanma sorunu, siber çatışmanın iki önemli parametresini tam olarak açıklayamamasından kaynaklanmaktadır: sosyopolitik boyutu (interneti düşman kurumlara karşı kullanan sosyal hareketler ya da muhalifler) ve çatışmanın bir ortamın (internet) içinde ya da internet aracılığıyla gerçekleşmesidir. Toplumsal hareketlerin siber kavgalara nasıl karıştığını, Bilgi ve İletişim Teknolojilerinin kullanımından nasıl etkilendiğini anlamak için, teorisyenlerinden halihazırda var olan teorik araçları kullanmaları mantıklı olacaktır (Karatzogianni, 2005: 196- 197).

İnternetin yapısı ağ grupları için idealdir (merkezi otoritesi olmayan küresel bir ağ olduğundan) ve yönetişim (yönetim yok), zaman ve mekân (kısaltma), ideoloji (bilgi ve

erişim özgürlüğü), kimlik (çokluk) ve temel olarak gözetim ve kontrol, sınırlar ve aygıtlara karşı bir muhalefet deneyimi sunmuştur. Bununla birlikte, grupların inanç ve örgüt sistemlerinin hiyerarşik aygıtlara (ulus, din, partiler ve liderlerle özdeşleşme) yöneldiği etno-dini siber kavgalarda, bu ağ formu her zaman açık değildir. Sosyo-Politik Siber Çatışma'da bilgi ve iletişim teknolojilerinin etkisi; a. Yapıları harekete geçirme (internet, katılım, işe alım, taktik, hedefleri kullanarak ağ hareket tarzı), b. Çerçeveleme Süreçleri (sorunlar, strateji, kimlik, internetin bu süreçler üzerindeki etkisi), c. Siyasi fırsat yapısı (internetin bu yapının bir bileşeni olarak), d. bilginin özgür dolaşımını sağlamak amacıyla hackerler tarafından gerçekleştirilen siyasal internet saldırılarıdır. Etno-dini siber çatışmalar: a. Etnik / dini bağlantı, şovenizm, ulusal kimlik, b. Dâhil etme ve dışlama söylemleri, c. Bilgi savaşı, internetin bir silah, propaganda ve mobilizasyon kaynağı olarak kullanılması d. Çatışma çözümü, yasal ve örgütsel çerçeveye, tarafların ve sorunların sayısına, iktidarın dağıtılmasına ve değer ve inançların içeriğine bağlıdır (Karatzogianni, 2005: 198- 201).

Son yirmi yıl içinde yapılan sayısız olay, kötü niyetli kodun, her türlü amaç için, her türden sayısal sistemi tahrip eden ve bozan bir araç olarak büyük bir potansiyele sahip olduğunu göstermiştir. Suçluların ve ülkelerin benzer şekilde, kötü amaçlı yazılım kampanyası için gerekli tüm araçları satın alabilecekleri çevrimiçi pazarlar vardır. Kötü amaçlı yazılımlara erişim artık her zamankinden daha kolay olduğundan, aktif savunma veya doğrudan suç için kötü amaçlı kod kullanımı, ulus devletler için büyük bir hayranlık uyandırmaktadır. Ancak, siber tartışma literatürü, kötü niyetli kodların ulus devletler tarafından dağıtımının sorunlu olduğunu belirtmektedir (Cycon, 2014: 72). Eskiden, devletlerarasında çeşitli biçimlerde karışıklıklar olsa da, örgütlü organlar öncü roldeyken, bireyler artık sınırlı bir boyutta bile, uzak ve güvenli konumlardan daha güçlü, daha büyük yapılara karşı çalışabilirler. Resmi veya gayri resmi gruplar, suç ya da siyasi etkinlik tarafından harekete geçirilen plan belirleme, hedeflerine ulaşma ya bazı finansal ya da politik kârlar elde etme konusunda iyi bir fırsat bulmak için siber boyutta hareket etmektedirler (Cycon, 2014: 142). Siber çatışmalar, gerçek hayat çatışmaları ile paralel (aynı amaçlar, aynı hedefler doğrultusunda) olarak hareket edebilir ve katılımcı grupların doğasını ve çatışmalarını açığa çıkarabilir (Karatzogianni, 2009: 3). Siber savaşın çizgileri bulanık olabilir. ABD eski Ulusal İstihbarat Başkanı Joel Brenner; "ABD'de bizler savaşı ya tam ölçekli bir savaş ya da barış içinde bir açma-kapama düğmesi olarak düşünmeye eğilimliyiz." demiştir. "Gerçek farklıdır. Artık nadiren savaş açacak uluslararasında sürekli bir çatışma durumundayız... Alışmak zorunda

olduğumuz şey, Çin gibi, hatta savaşta olmadığımız ülkelerin bile bizimle yoğun bir şekilde iletişim halinde olmalarıdır." Bu, siber savaşın, sürekli çatışmanın aslında doğrudan açık şiddet ile sonuçlanmadığı Soğuk Savaş gibi daha gayri resmi çatışma kavramlarıyla daha çok ortak noktası olabileceği yerler olabilir (Singer P. W. and Allan Friedman, 2014: 121). Uluslararası hukuk amaçları için "siber savaş", "siber düşmanlık" ve "siber çatışma" kavramları resmi olarak tanımlanmamıştır. Var olan tek antlaşma tanımı Şangay İşbirliği Örgütü'dür ve daha geniş bir "bilgi savaşı" kavramı ile ilgilidir. Bilgi sistemleri, süreçleri ve kaynaklarına zarar vermek; siyasi, ekonomik ve sosyal sistemleri zayıflatmak; kitlesel beyin yıkamayı, toplumu ve devleti yıkmak için bilgi alanında iki ya da daha fazla devlet arasında yüzleşme olarak ve de devleti, karşı tarafın çıkarları doğrultusunda karar almaya zorlamak gibi tanımlama mevcuttur (Melzer, 2012: 3).

Çatışma Çeşitleri

Çatışmayı, birçok alanda nasıl kullanıldığına bağlı olarak tanımlamanın farklı yolları vardır. Bu nedenle çatışma, farklı varlıkların karşıt fikirlerine ve eylemlerine aittir, dolayısıyla uzlaşmaz bir duruma yol açmaktadır. Çatışma hayatın kaçınılmaz bir parçasıdır. Her birimiz kendi görüşümüze, düşüncelere ve inanç gruplarına sahibiz. Bu nedenle, sıklıkla kendimizi farklı senaryolarda çatışıyor buluyoruz; Diğer bireyleri, insan gruplarını veya kendi içimizdeki mücadeleyi içerebilir. Dolayısıyla çatışma, eylem ve kararlarımızı bir şekilde etkilemektedir (Conflict Barometer, 2016: 6-8). Çatışma farklı nedenlerle ortaya çıkar ve insan toplumunda farklı çatışma çeşitleri vardır.

Kişilerarası çatışma, iki birey arasındaki çatışmayı ifade etmektedir. Bu, tipik olarak insanların birbirinden nasıl farklı olduğuyla ortaya çıkmaktadır. İnsanlar, uyumsuz seçimler ve görüşler ile sonuçlanan çeşitli kişiliklere sahipleridir. Görünüşe göre, kişisel gelişime yardımcı olabilecek veya başkalarıyla ilişkileri geliştirebilecek doğal bir durumdur. Ayrıca, bu tür çatışmaları yönetmek için ayarlamalar yapmak gerekmektedir. Ancak, kişilerarası çatışmanın çok yıkıcı hale gelmesi durumunda, bir arabulucuyu aramak, çözüme kavuşturmak için yardımcı olacaktır. *İçsel çatışma* bir bireyde gerçekleşir. Bu deneyim kişinin aklında gerçekleşir. Dolayısıyla, bireyin düşüncelerini, değerlerini, ilkelerini ve duygularını içeren psikolojik bir çatışma türüdür. İç mücadelelerinizi deşifre etmekte

zorlanırsanız, bu tür çatışmanın ele alınması oldukça zor olabilir. Huzursuzluğa ve tedirginliğe yol açmaktadır. Hatta depresyona bile neden olabilir. Depresyon geçiren kişi durumdan çıktığında, daha güçlü hale gelebilir. Böylece, deneyim kendi kişisel gelişiminde, bireye yardımcı olacak olumlu bir değişim ortaya çıkarmaktadır. *Grup içi çatışma*, bir takım bireyler arasında gerçekleşen bir çatışma türüdür. Bu bireyler arasındaki uyumsuzluklar ve yanlış anlaşılmalar gruplar arası bir çatışmaya yol açmaktadır. Kişilerarası anlaşmazlıklardan (örneğin, ekip üyelerinin gerilim yaratabilecek farklı kişilikleri vardır) ya da görüş ve fikirlerdeki farklılıklar ortaya çıkmaktadır (örneğin, bir sunumda, ekip üyeleri, bir başkan tarafından sunulan kavramların hatalı olduğu için görüş ayrılıkları). Bir takım içinde, çatışma olarak hedeflerine ulaşmalarına izin verecek olan kararların ortaya çıkmasında yardımcı olabilir. Ancak, çatışmanın derecesi üyeler arasındaki uyumu bozarsa, çözümlenebilmesi için farklı bir gruptan bazı ciddi rehberliğe ihtiyaç duyulacaktır (Folarin, 2013:5-7). Uyuşmazlık sorunları olacaktır. Çünkü çıkar farklılaşır ve çatışır, bu da anlaşmazlıklara veya çatışmalara yol açabilir. Bir grup içindeki farklı takımlar arasında bir yanlış anlaşılma ortaya çıktığında *gruplararası çatışma* yaşanır. Rekabet ayrıca gruplar arası çatışmanın ortaya çıkmasına da katkıda bulunmaktadır. Bir grup tarafından kendi kimliklerini oluşturan bir gruba karşı bir rekabet içerebilir. Ya da bir grup tarafından belirlenen sınırlara karşı bir rekabet içerebilir (Evans, 2013). Bilgi ve İletişim Teknolojilerinin artan önemi göz önüne alındığında, tarafların, siber uzayın belirli yönlerinden faydalanmak için çeşitli araçlar ve teknikler kullanarak rakiplerine karşı avantaj elde etmek isteyecekleri şaşırtıcı değildir. Mesela, hangi çatışma sorunlarının (bölgesel, ideolojik vb.) ya da çatışma şiddetlerinin (şiddet veya şiddet içermeyen) siber uzayda yankılanıp yankılanmadığını bilmiyoruz. Giderek artan siber olay sayısı göz önünde bulundurulduğunda, araştırmacıların, araştırmaları ve işbirlikleri yetersiz kalmaktadır (Conflict Barometer, 2017: 37). Çatışma bazıları için bir sorun gibi görünebilir. Ancak bu, çatışmanın nasıl algılanması gerektiği değildir. Öte yandan, büyüme için bir fırsattır ve gruplar veya bireyler arasında açılma için etkili bir araç olabilir. Bununla birlikte, çatışma üretkenliği geri çekmeye ve daha fazla anlaşmazlığa yol açmaya başladığında, bir çözüme ulaşmak için çatışma yönetimine ihtiyaç duyulacaktır (Conflict Barometer, 2015: 6).

Uluslararası İlişkilerde Siber Çatışmalar

Siber çatışma, ulus devletler için hızla değişen stratejik bir sorunu temsil etmekte ve onun etkilerini yönetmek için yeterli bir politika çerçevesinden yoksun kalmaktadır. Estonya,

Suudi Arabistan, İran ya da en son ABD başkanlık seçimleri gibi olaylar, siber saldırıların kritik hizmetleri tehlikeye atabileceğini, ekonomilere zarar verebileceğini, demokratik devletlerin temel sütunlarını zedeleyebileceğini ve resmi devlet çatışması düşüncesine ulaşabileceğini göstermiştir. Siber alan birden fazla ulusal, idari ve yargı sınırlarını aşar ve ticari kurumlardan bireylere, siber suçlulardan terörist gruplara kadar geniş bir yelpazede devlet dışı aktörleri bir araya getirmektedir. Devletler siber uzayda en güçlü ve aktif unsurlar olmaya devam etmektedir. Devletler uluslararası çatışma için yeni bir arena geliştirmişlerdir. Bu durum, ulus devletlerin siber suçluların kendi çıkarlarını daha da ileri götürmeleriyle açıklığa kavuşmaktadır. Siber alanın tekilliğini ve devletlerarası çatışmadaki rolünü anlamak için, onun yapısını değerlendirmek gerekir. Bunun nedeni, kaçınılmaz olarak siber saldırıların içine gömülmüş karmaşıklığın, mekânın kendisinin özelliklerinden kaynaklanmasıdır. Siber çatışmalar genellikle ticari işlemler için tasarlanan teknolojiler içinde gerçekleşir ve gelişir; bağımsız, anonim olarak ve dünya çapında bağlantıyı desteklemek için oluşturulmuşlardır. Bu alanın siber çatışmanın geliştiği bağlamda olması, çözüm üretmenin zorluğunu ya da sadece bu konuya standartlaştırılmış cevapları yansıtmaktadır.

Çatışmayı önlemek için bir dizi tanımlama girişimleri yapılmıştır. Çatışma önlemleri, politik bir itiraz bağlamında bir akıl yürütme aktörü tarafından gerçekleştirilen eylemler ve iletişimdir. Bunlar, belirlenmiş kurallara aykırı düzenlemelerin prosedürleri dışında ya da uluslararası düzeni veya devletin temel işlevini tehdit ederse, tanımlanabilir bir iddia için kurucu niteliktedir. Oluşturulan düzenleyici prosedürler, çatışma yönetimi aktörleri tarafından kabul edilen çatışma yönetimi mekanizmaları olarak tanımlanmaktadır. Örnekler arasında seçim ve muhakeme işlemleri bulunmaktadır. Düzenlenmiş tüzük prosedürleri, fiziksel şiddet kullanımı veya tehdidine başvurmadan gerçekleştirilmelidir. Devlet fonksiyonları, bir nüfusun güvenliğini, bir bölgenin bütünlüğünü ve belirli bir politik, sosyoekonomik veya kültürel düzenin güvenliğini sağlamayı içerir (Conflict Barometer, 2017: 6). Sınır ötesi siber olayların ve çatışmaların yönetimi, genellikle devlet kurumları ve özel olarak sahip olunan bilgi altyapısından sorumlu kuruluşlar arasında kapsamlı ve ayrıntılı bilgi paylaşımı gerektirmektedir. Siber olayların araştırılması ve yönetimi için verilerin sadece olayların seyri ve olayların arka planı hakkında detaylar değil, aynı zamanda hedefler üzerinde gerçek zamanlı raporlama ve sunucu günlüklerinin ayrıntılarından oluşmaktadır.

Bu, iyi trafiği kötülükten ayırt etmeyi mümkün kılmakta, düşman IP adreslerini engellemekte ve saldırıların kökenini izlemektedir (Tikk, 2010: 24).

İnternet altyapısının pratikte oldukça dayanıklı olduğu kanıtlanmıştır. İş dünyasında internetin bozulmasını ya da özel verilerin kaybolmasıyla yok olacak çok şey olduğu için, güvenlik çözümleri, hackerlar, sahtekarlar ve siber-sabotajcıların bir adım ötesine geçmektedir. Ancak bu, yalnızca büyük Bilişim Teknolojisi şirketlerinin (Microsoft, Cisco, Google, Yahoo v.d.) çoğu kez hükümetlerle yakın işbirliği içinde çalıştığı sürekli yenilik ve yatırımla elde edilir. Bununla birlikte, internetin bütünlüğüne yönelik gelecekteki tehdidin, düşman saldırıları gibi, giderek daha fazla sayıda ve daha geniş dosyaları dolaşarak, kapasite üzerindeki kısıtlamalardan gelmesi muhtemeldir (Wescott, 2008: 2).

Siber çatışmalar, teknik bilgi birikimine sahip siber savaşçılar tarafından bit ve bayt kullanan ağlar üzerinden de mücadele edilir. Siber çatışma, taktik düzeyde hızlıdır; Birler ve sıfırlar gerçekten ağ hızında seyahat ediyorlar. Siber çatışmalar düzensiz çatışmalar olma eğilimindedir. Bu tür bulanık ve belirsiz koşullarda siber çatışma kavramını tanımlamak, neredeyse her zaman bir sorun haline gelmektedir (Healey, 2016: 43-44). Mevcut belirsizlik, hükümetler arasında gerçek siber tehdit hakkında kafa karışıklığına yol açmaktadır. EastWest Enstitüsü tarafından "Siber Uzay için Cenevre ve Lahey Sözleşmelerinin Oluşturulması" başlıklı bir raporda, "İkili barışa karşı savaş paradigmasının İnternet Çağının karmaşıklıkları için çok basit olması mümkündür." Raporda, mevcut politika araçlarının nasıl kullanılacağı ve daha da önemlisi, uluslararası hukukun uygulanabilirliğinin açıklığa kavuşturulması için "üçüncü bir savaş dışı yöntem" geliştirilmesi önerilmektedir. Siber saldırıları kategorize etmek için iki basit kritere dayanan bir sistem önerilmektedir: etki ve niyet. Siber uzaydaki herhangi bir eylem, bu iki model aracılığıyla değerlendirilebilir. Kötü şöhrete sahip Stuxnet saldırıları gibi siber uzayda çeşitli yüksek profilli eylemleri değerlendirmek, savaş metaforunun bu olaylara uygulanamaz hale geldiği oldukça açıktır. Stuxnet'in niyeti politik bir unsura sahip olsa da (örneğin İran rejimini müzakere masasına dönmeye zorlamak), ölümcül bileşen eksiktir. Bu saldırılarda hayatlar kaybedilmiş olsa bile, temel amaç sabotaj, uluslararası alanda "kabul edilen" bir eylem ve kendi içinde çatışma, bir politik savaş biçimiydi (Gady, 2012). Birçok ülke için siber çatışmayla yüzleşmenin en önemli adımı, tercih edilen ulusal güvenlik sonuçları konusunda çok daha açık olmaktır. Bir hükümetin rekabet halindeki kamuoyu hedefleriyle karşı karşıya kaldığı durumlarda, kararları

netleştirmek için net bir ulusal siber stratejide bunlar öncelikli olmalıdır (Ünver, 2017: 110-111; Cycon, 2016: 45).

Uluslararası siber koruyucular ve olay ekipleri arasındaki etkileşimler çoğunlukla teknik, diplomatik ve politik ilişkilere dayanmaktadır. Özellikle kritik altyapılar, bilgisayar sistemlerinde meydana gelen olaylar ile ilgili ulusal güvenlik kaygısı alanıdır. Böyle bir olayın bir örneği, Ülke B hükümeti tarafından eylemleri protesto eden A Ülkesi bireylerinin "vatansever" çabaları olacaktır. Bu bireyler, B Ülkesinin hükümet veya kritik altyapı bilgisayar sistemlerine girebilir. Alternatif olarak protestocular, B ülkesinin hükümetini, finansal ve medya bilgisayar sistemlerini, o kadar fazla elektronik trafiğe maruz bırakacaklarını, sistemlerin kullanılamayacak kadar yavaşlatabilmeyi koordine edebilir. İlişkilerinin niteliğine bağlı olarak, A Ülkesi, B Ülkesine siyasi veya yasayı uygulama sağlama konusunda isteksiz olabilir. Ek bir karmaşık faktör, internetin yapısı ve doğası gereği, A Ülkesinden bir protestocunun kötü niyetli faaliyetinin, ani bir şekilde çatışmanın ötesinde telekomünikasyon sistemleri aracılığıyla gerçekleştirilebilmesidir (örneğin, sadece A ve B ülkelerinde değil, aynı zamanda X, Y ve Z ülkelerinde). Diğer ülkelerin B ülkesine yardım etmesini gerektiren ortak bir uluslararası yasa yoktur ve bu nedenle yardımda başarısızlığa dair hiçbir sorumluluk yoktur. Siber olaylar silahlı çatışma olarak tanımlanabilir ve belirli bir ülkeye atfedilebilirse, o zaman B Ülkesi uluslararası insancıl hukuk çerçevesinde eylemler başlatabilir. Özellikle NATO'nun hukuksal olarak almış olduğu kararlar bu noktada etkili olmaktadır. Ayrıca şu anda uluslararası anlamda oluşturulmaya çalışılan hukuk kuralları da bu anlamda önemlidir. Geleneksel çatışmaların siber bileşenleri içermesine rağmen, bugüne kadar hiçbir bağımsız siber olayın (fiziksel çatışmaya bağlı olmayan) silahlı çatışmalar olarak kabul edilmediği veya belirli ülkelerin desteğine yeterince atfedilmediği belirtilmelidir. Savaş paradigması dışında, uluslararası toplum, siber tehditleri veya ulusal güvenliği etkileyen olayları yönetmek için yaygın kabul görmüş bir çerçeveye sahip değildir. Dahası her bir ülke işbirliği sağlayabilsin diye, asgari siber olaylara müdahale yeteneğine sahip olan uluslararası bir anlaşma bulunmamaktadır. Çok uluslu siber olaylara müdahale çabalarını koordine eden tek bir örgüt yoktur (Dion, 2010: 71-73).

Çatışmanın Sınıflandırılmasında Hukuki Boyut

Modern savaşta "çatışmanın sınıflandırılması", yani belirli düşmanlıkların bir hukuk meselesi olduğu çatışma türünün tanımlanması olarak sorunlu olduğu şeklinde birkaç

uluslararası insancıl hukuk konusu görülmektedir. Söz konusu çatışmanın sınıflandırılması, her zaman uluslararası insancıl hukuk analizinde, çatışmanın niteliği geçerli yasal rejimi belirlediği için ilk adımdır (Schmitt, 2012: 245). Siber çatışma yeni olmayabilir, ancak eski de değildir. Diğer büyük, yıkıcı küresel eğilimlerde olduğu gibi, geleneksel uluslararası normların hala uygulandığı, ister geçerli olsun, isterse de değişiklikler olsun, ya da tamamen yeni normların icat edilmesinin gerekip gerekmediği konusunda sıkıntı veren sorular vardır. En önemli normlardan biri, devletlerin Lahey Sözleşmesi'nin güvence altına aldığı hak ve sorumluluklarla uluslararası yardıma cevap olarak tarafsız kalabilmeleri olmuştur. Siber gizliliğin doğası gereği, bu türden yasal norm, değiştirilmiş bir siyasi tarafsızlık normundan daha az yararlı olabilir. İnternet protokolleri siber saldırıları herhangi bir sayıdaki tarafsız ülke üzerinden yönlendirmektedirler. Siber anlaşmalar genellikle uluslararası hukuku tetikleyecek kadar yıkıcı değillerdir ve savaşanların kimliği veya uyruğu açık olmayabilir (Cycon, 2012: 22). Buna göre, uluslar, resmi bir anlaşma yükümlülüğü olup olmadığına bakılmaksızın, siber saldırıları durdurmak ve makul adımlar atmak için politik baskı altında olabilirler (Karatzogianni, 2009: 5-6).

"Uluslararası olmayan silahlı çatışma", bir devlet ile "örgütlü" silahlı grup arasındaki çatışmalar belirli bir yoğunluk seviyesine ulaştığında ortaya çıkar. Yoğunluk ayrıca şiddet seviyesinin ayaklanma veya sivil rahatsızlıklardan daha yüksek olmasını gerektirir (Cycon, 2017: 137-138). Yaralanma veya hasar tek başına yeterli değildir. Bireyler tarafından yürütülen siber operasyonlar, yetersiz bir şekilde örgütlenmedikleri için hak kazanamazlar. Çevrimiçi olarak organize edilen gruplar, duruma göre değerlendirilebilir, ancak geleneksel organizasyon kriterleri, onların hak kazanmalarını zorlaştırır. Buna göre sınıflandırma, önemli bir konudur. Örneğin, Eski Yugoslavya Uluslararası Ceza Mahkemesi (ICTY), ilk örneği olan Tadiç'te uluslararası olmayan çatışmanın uluslararasılaştırılmasına yönelik kriterler ile mücadele etmiştir. On yıldan kısa bir süre sonra, ulus ötesi terörizm sınıflandırma konuları dikkat çekmiştir. Bu uluslararası nitelikte terörizm olmuştur (Schmitt, 2012: 246). Sınırları aşmış ya da uluslararası olmadığından, bir devletin bir diğerine karşı düşmanlıklarla karşı karşıya gelen güçlerini içermediğinden mi (ya da hiç silahlı çatışma oldu mu)? Gürcistan 2008, Litvanya 2008, Radyosuz Avrupa / Radyo Özgürlük 2008 gibi siber olaylar, birbiriyle çelişen bakış açılarının, aynı ya da hatta benzer yasal sonuçları desteklemeyen farklı arka plan sistemlerinden ve deneyimlerinden ortaya çıkmaya eğilimli olduğu anlayışını pekiştirmiştir. Sonuç olarak, öykünün farklı yönlerini ve farklı türde siber faaliyetlerini

sistematik olarak kategorize etme yeteneğini göz önünde bulundurma yeteneği, yasal perspektiften çok büyük bir öneme sahiptir.

Gelecekte siber çatışma, sınıflandırmayı daha fazla karmaşıklaştıracaktır. Siber operasyonlar, tipik olarak silahlı çatışmalarla ilişkilendirilen fiziksel hasara neden olmadan, geniş toplumsal ve ekonomik zararı üretme potansiyeline sahiptir. Bunlar aynı zamanda doğal olarak sınır-ötesidir, dolayısıyla coğrafi faktörlere dayanan sınıflandırma yaklaşımlarını engellemektedirler. Dahası, kitlesel saldırılar tek bir kişi tarafından veya tamamen online olarak organize edilen bir grup tarafından başlatılabilir. Bu, bir devletin silahlı kuvvetlerinin veya tipik askeri operasyonları gerçekleştirebilecek bir grubun katılımına bağlı olan geleneksel çatışmaların tersi bir durumdur. Siber çatışmaların ortaya çıkışı, devam eden kinetik çatışmanın sınıflandırmasını hiçbir şekilde değiştirmemektedir. Paradigmatik örnek, Gürcistan ve Rusya arasındaki 2008 uluslararası silahlı çatışma sırasında "vatansever korsanların" yürüttüğü siber operasyonlardır (Schmitt, 2012: 250). Ülkelerin, ne hazırlığa ne de şansa sahip olamayacakları unutulmamalıdır. Zira ülkeler, siber olay yanıtları, yasaların uygulanması, gerekli olabilecek iç ve hükümetler arası koordinasyon için yeteneklerine göre değişmektedir (Dion, 2010: 71).

Bugüne kadar devletler, devam eden silahlı çatışma bağlamı dışında yürütülen herhangi bir siber operasyonu, uluslararası ya da uluslararası olmayan silahlı çatışma olarak nitelendirmekten kaçınmışlardır. Siber operasyonlar gelecekte, kaçınılmaz olarak devletler için zorlu çatışma sınıflandırma zorluklarını sunacaktır (Wingfield and Tikk, 2010: 22). Uluslararası silahlı çatışmayla ilgili olarak, devlet dışı aktörler tarafından gerçekleştirilen siber operasyonların atfedilmesi, geçmişte kinetik eylemlerin devletlere atfedilmesinden daha fazla sorun oluşturacaktır. Uluslararası olmayan silahlı çatışma bağlamında örgütlü bir silahlı grup olarak nitelendirme, sanal organizasyonun yapıları, araçları, yaygınlığı arttıkça ve geliştikçe, giderek karmaşıklaşacaktır. Devletlerin ve devlet dışı aktörlerin, siber altyapıya ve bağımlılık yaratan siber operasyonlara daha fazla bağımlı hale gelmesiyle, söz konusu devletin uygulamalarının mevcut eşiğin düşmesine neden olması beklenebilir. Siber silahlı çatışma yasası devam eden bir çalışmadır ve yakın gelecek için de öyle kalacaktır (Schmitt, 2012: 259-260).

Sonuç Yerine: Siber Çatışma Eğilimi

Siber çatışmayı etkileyen birçok sebep olabilir. Çoğu zaman bunları takip etmek zor olmaktadır. Siber çatışmanın izlenmesi siber alanın boyut, bant genişliği ve hacim bakımından artmasına paralel olarak günümüzde en büyük zorluklardan biri olmaya devam etmektedir. Buna ek olarak, siber aktörlerin eşiğin altında faaliyet göstermeye yönelik artan kararlılığı, yetkisi olmayan eylemlerin istenilen kesinlik ve gösterilebilirlik düzeyleriyle tanımlanmasını daha da zorlaştırmaktadır. Kalıcı ve yaygın izleme için bir olay olduğu kabul edilebilir. Bununla birlikte, ciddi sabotaj ve casusluk faaliyetlerinin tespiti, kısmen, mevcut tarih ve operasyonel kısıtlamaların biraz ötesinde, uzun bir zaman dilimi boyunca trafiğin akışına bağlıdır. Bu, siber alanın canlı ve modern ölçekte ele alınması, daha fazla araştırma için şüpheli faaliyetler algılaması ve tasarlanmış siber izleme altyapılarındaki araştırmalar için hayati önem taşımaktadır.

Pek çok araştırmacı, ağ izlerinden elde edilen bilgilere bağlı olarak tamamen internet altyapısının doğası gereği siber çatışma atfedilmesinde ve belirlenmesinde çok az şey yapılacağını iddia etmektedir. Bu nedenle, teknik çözüm verilerini bağlamsal analiz ve akıllı hizmetlerden elde edilen bilgilerle birleştiren yaklaşımlara ihtiyaç vardır. Siber çatışma atfedilmesi (özellikle yavaş faaliyetler) için etkili bir yöntemdir ve farklı koşullar altında etkinliğinin araştırılması sağlanmaktadır (Cycon, 2012: 407-408). Sadece siber alanda değil, suç ve hukuk bilimleri gibi diğer alanlarda da her tür aktör yetiştirmek için kullanılabilir. Mevcut bir yasal rejim veya çerçeve ile açıkça ilişkilendirilemeyen bir eylemden herhangi bir hukuki sonuca varmak siber çatışma için oldukça karmaşık olabilir. Bu nedenle pratik bir bakış açısı, ilgili yasal rejimin uygulanması açısından "neyin ne olduğunu" açık bir şekilde anlaşılması büyük önem taşımaktadır. Bilgisayar bilimleri ve bilişim teknolojileri, hukuk, stratejik, politik konular, sosyal ve ekonomik kaygılar ve insan davranışsal modellemelerini siber uzaya göre incelemektedir. Siber çatışmada çatışma aşamaları arasındaki etkileşimin dinamikleri, kinetik çatışmalarda bilinen aşamaları her zaman takip etmeyebilir. Tanım olarak, siber uzay, belirli bir atıfta başarısızlığa yol açan anonim saldırılara izin verir. Esasen, geleneksel yanıt yöntemleriyle çözülemeyecek kadar belirsizliği taşıyan eylemlerin olasılığını açmıştır. İlişkilendirme konusundaki belirsizlik, etkin devlet misillemesini felce uğratmış ve devlet çatışmasında ve uluslararası güvenlikte yeni bir paradigma ortaya çıkarmıştır. Bu belirsizlik, hem "saldırganlar" hem de "savunanlar" olarak adlandırılan güçlü siyasi etkilerin kaynağıdır. Çatışma ve orantılı tepki gibi birçok geleneksel çatışma kavramı,

siber savaşla başa çıkmak için yeniden uyarlanmalı ya da tamamen değiştirilmelidir. Saldırıların atfedilmesindeki yapısal belirsizlik, olası teminatların kapsamı ve devlet altyapısı ve kritik hizmetler üzerindeki olası etki, siber çatışmanın yönetilmesi ve yönlendirilmesi için özel ilkeler ve kurallara duyulan ihtiyacın yeni bir savaş türü olduğunu doğrulamaktadır. Siber çatışma hâlihazırda ele almaya hazır olmadığımız çok çeşitli olasılıklar sunmaktadır. Devletler arasındaki gelecekteki ilişkiler kuvvetli bir şekilde gelişmeli ve bu sayede siber çatışmaların varlığı azalmalıdır. Mevcut devlet uygulamaları, siber saldırıların ne ölçüde savaş eylemleri olarak tasarlanacağını ve hangi şiddetin diplomatik veya hatta askeri tepkiyi tetiklemeleri gerektiğini belirleyecektir. Bu nedenle, birbirine bağlı bir dünya gerçekliğinde, bu sınırlar yakında çatışma yönetiminde en hassas konulardan biri haline gelebilir. Siber çatışma artık sadece yükselen bir olay değil, yeni bir savaş alanı olmaktadır. Gelecekte siber çatışma devletlerin nasıl davrandığını, işbirliği yaptığını, yanıt verdiğini ve nihayetinde savaşı nasıl sürdürdüğünü yeniden tanımlayacaktır.

KAYNAKÇA

____ in Heidelberg, [https://hiik.de/conflict-barometer/bisherige-ausgaben/?lang=en].

____The EastWest Institute, [https://www.eastwest.ngo/issues/cyberspace].

Akyeşilmen Nezir ve Yılmaz Ensaroğlu, (2013). "Sonuç Yerine: Barış Sürecinde Yoldaki İşaretler", Nezir Akyeşilmen (ed.), *Barışı Konuşmak: Teori ve Pratikte Çatışma Yönetimi*, 1. Baskı, Ankara: ODTÜ Yayıncılık, ss. 444-460.

Akyeşilmen Nezir, (2015). "Çatışma Analizi: Hak-temelli Stratejik Barış Modeli", Ertan Efegil ve Esra Pakin Albayrakoğlu (ed.), *Türkiye'nin Yakın Havzasındaki Devlet İçi Çatışmaların Analizleri*, İstanbul: Gündoğan Yayınları, ss. 39-74.

Akyeşilmen Nezir (ed.), (2013). *Barışı Konuşmak: Teori ve Pratikte Çatışma Yönetimi*, 1. Baskı, Ankara: ODTÜ Yayıncılık.

Brangetto,P., M. Maybaum, J. Stinissen (Eds), (2014). *6th International Conference on Cyber Conflict*, Talinn: CCD COE Publications, http://www.ccdcoe.org/cycon/2014/proceedings/cyconBOOK2014.pdf.

Brose Robert, (2015). "Cyberwar, Netwar, and the Future of Cyberdefense", *7th International*

Conference on Cyber Conflict: Architectures in Cyberspace, M.Maybaum, A.-M.Osula, L.Lindström (Eds), Talinn: CCD COE.

Clarke,Richard and Robert Knake, (2012). *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco; Reprint edition.

Conflict Barometer. (2011). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 20, Germany: Printed in Heidelberg.

Conflict Barometer. (2012). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 21, Germany: Printed in Heidelberg.

Conflict Barometer. (2013). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 22, Germany: Printed in Heidelberg.

Conflict Barometer. (2014). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 23, Germany: Printed in Heidelberg.

Conflict Barometer. (2015). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 24, Germany: Printed in Heidelberg.

Conflict Barometer. (2016). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 25, Germany: Printed in Heidelberg.

Conflict Barometer. (2017). *Disputes, Non-Violent Crises, Violent Crises, Limited Wars, Wars*, HIIK, No. 26, Germany: Printed in Heidelberg.

Czosseck, C., E. Tyugu and T. Wingfield (Eds.), (2011). *3rd International Conference on Cyber Conflict*, https://ccdcoe.org/sites/default/files/multimedia/pdf/2011_Proceedings_0.pdf.

Czosseck, C., R. Ottis and K. Ziolkowski (Eds.), (2012). 4th International Conference On Cyber Conflict, ,https://ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf.

Daban, Cihan, (2016). "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi", *Siber Politikalar Dergisi*, Cilt: 1, Sayı: 1, [http://cyberpolitikjournal.org/wp-content/uploads/2017/02/Journal_Dergi_pdf.pdf].

Denning Dorothy, (2001). "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", In Arquilla J., Ronfeldt D. (eds) *Networks and Netwars: The Future of Terror, Crime, and Militancy*, pp. 239-288.

Erendor M.E., "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu", *Cyberpolitik Journal*, vol.1, no.1, pp.114-133, 2017.

Evans, Brad, (16.08.2013). Types of Conflict – Four Classifications, [http://www.typesofconflict.org/types-of-conflict].

Folarin, Sheriff F. (2013). Types and Causes of Conflict, Readings in Peace and Conflict Studies, [http://eprints.covenantuniversity.edu.ng/3241/1/Folarin%2025.pdf].

Gady, Franz-Stefan. (08.06.2012). *A Reality-Based Model for Cyber Conflict*, https://www.eastwest.ngo/idea/reality-based-model-cyber-conflict.

Geers Kenneth, (2011). Strategic Cyber Security, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn: CCD COE Publication.

Godwin, James, Andrey Kulpin, Karl F. Rauscher and Valery Yaschenko (Eds.), (2014). *Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2*, USA: The EastWest Institute, https://www.files.ethz.ch/isn/178418/terminology2.pdf.

Healey Jason and Karl Grindal, (2013). *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, Cyber Conflict Studies Association.

Healey Jason, (2016). "Winning and Losing in Cyberspace", *8th International Conference on*
Cyber Conflict: Defending the Core, N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.), Talinn: CCD COE.

Kalm Kaarel, (2013). "Illicit Network Structures in Cyberspace", 5th International Conference On Cyber Conflict, K. Podins, J. Stinissen and M. Maybaum(Eds), Talinn: NATO.

Karatzogianni, Athina (2005). *The Politics of Cyberconflict: Ethnoreligious Conflicts in Computer Mediated Environments*, PhD thesis, England: University of Nottingham, [http://eprints.nottingham.ac.uk/12112/1/423635.pdf].

Karatzogianni Athina, (2009). "Introduction: New Media and the Reconfiguration of Power in
Global Politics", *Cyber Conflict and Global Politics*, Athina Karatzogianni (Eds), NYC: Routledge.

Kosenkov Alexander, (2016). "Cyber Conflicts as a New Global Threat", https://pdfs.semanticscholar.org/a00e/3cba13b99b0acee9817002a925bba7ec646d.pdf.

Krishnamurti, J. (2002). *Çatışma Üzerine*, çev. Nurgül ve Deniz Demirdöven, 1. Baskı, İstanbul: Ayna Yayınevi.

Lawson Sean, (2012). "NATO & Cyber Conflict: Background & Challenges." Presented at The Shadow NATO Summit III. 14-15 May. George Washington University. Washington, D.C.

Lin, Herbert, (2013). "Cyber Conflict and National Security", Robert Art and Robert Jervis

(Eds.), *International Politics: Enduring Concepts and Contemporary Issues*, Eleventh Edition, USA: Pearson, pp. 476-489.

Maeve Dion , (2010). "Different Legal Constructs for State Responsibility", https://ccdcoe.org/cycon/sites/default/files/LegalProceedings2010.pdf.

Maness, Ryan C. and Brandon Valeriano, (2015). "The Impact of Cyber Conflict on International Interactions", SAGE: Armed Forces & Society, pp. 1-23.

Maybaum, M., A.-M.Osula and L.Lindström (Eds), (2015). *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Talinn: CCD COE, http://www.ccdcoe.org/cycon/2015/proceedings/CyCon_2015_book.pdf.

Melzer Nils, (2012). "Cyber operations and jus in bello", *Confronting Cyberconflict*, Vignard Kerstin (Eds), UNIDIR, http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf.

Nicholson, M. (1992). *Rationality and the Analysis of International Conflict*, England: Cambridge University Press.

Perkovich, George and Ariel E. Levite, (2017). *Understanding Cyber Conflict:14 Analogies*, Washington, DC: Georgetown University Press.

Pissanidis, N., H. Rõigas, M. Veenendaal (Eds.), (2016). *8th International Conference on Cyber Conflict: Defending the Core*, Talinn: CCD COE, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2016_book.pdf.

Podins, K., J. Stinissen and M. Maybaum(Eds.), (2013). *5th International Conference On Cyber Conflict*, http://www.ccdcoe.org/cycon/2013/proceedings/cyconBOOK2013.pdf.

Rõigas, H., R. Jakschis, L. Lindström and T. Minárik (Eds), (2017). *9th International Conference on Cyber Conflict: Defending the Core*, Talinn: CCD COE, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2017_book.pdf.

Schmitt Michael, (2012). "Classification of Cyber Conflict", *Journal of Conflict & Security Law*, Vol. 17 No. 2, pp. 245–260.

Sharma Amit, (2009). *Cyber Wars: A Paradigm Shift from Means to Ends, Conference on Cyber Warfare 16-19 June*, https://ccdcoe.org/cycon/sites/default/files/VirtualBattlefield.pdf.

Singer P. W. and Allan Friedman, (2014). *Cyber Security And Cyber War What Everyone Needs To Know*, NYC: Oxford University Press.

Tekin Segah, (2013). "Çatışma Dili: Bir Söylem Analizi", Nezir Akyeşilmen (ed.), *Barışı*

Konuşmak: Teori ve Pratikte Çatışma Yönetimi, 1. Baskı, Ankara: ODTÜ Yayıncılık, ss. 87-107.

Tikk Eneken, (2010). "IP Addresses Subject to Personal Data Regulation" https://ccdcoe.org/cycon/sites/default/files/LegalProceedings2010.pdf.

Ünver Gül Nazik, (2017). "Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları", *Cyberpolitik Journal 2* (4), pp. 104-129.

Vignard, Kerstin, (2011). *Disarmament Forum: Confronting Cyberconflict*, Swirzerland: UNIDIR

Westcott, Nicholas, (July 2008). "Digital Diplomacy: The Impact of the Internet on International Relations", *Oxford Internet Institute*, Research Report 16.

Wingfield Thomas and Eneken Tikk, (2010). "Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen", https://ccdcoe.org/cycon/sites/default/files/LegalProceedings2010.pdf.

[https://www.project-syndicate.org/commentary/new-norms-to-prevent-cyber-conflict-by-joseph-s--nye-2017-08?barrier=accesspaylog].

[http://www.iapss.org/wp/2017/09/07/cyber-conflict/].