Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik
International Cybersecurity Norms and Responsible Cyber Sovereignty

Article *in* İstanbul Hukuk Mecmuası / Istanbul Law Review · April 2021

DOI: 10.26650/mecmua.2021.79.1.0010

CITATION
1

READS
152

1 author:

Tuba Eldem
Fenerbahce University
22 PUBLICATIONS **63** CITATIONS

SEE PROFILE

İSTANBUL ÜNİVERSİTESİ YAYINEVİ

İstanbul Hukuk Mecmuası, 79 (1), 347-378

DOI: 10.26650/mecmua.2021.79.1.0010
http://dergipark.gov.tr/iuhfm
http://mecmua.istanbul.edu.tr/tr/_

İstanbul Hukuk Mecmuası

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

Başvuru: 22.05.2020
Revizyon Talebi: 06.10.2020
Son Revizyon: 12.01.2021
Kabul: 16.02.2021

Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik

Tuba Eldem*

Öz

Başlangıçta, devlet düzenlemesi ve müdahalesinden arınmış kişiler-arası özgür ve açık bir iletişim, haberleşme ve paylaşma alanı olarak tahayyül edilen siber alan kısa sürede ulusal ve küresel siyasetin temel bir konusu haline gelmiştir. 2007'de Estonya'ya, 2008'de Gürcistan'a ve 2010'da İran'a yönelik devlet-destekli olduğu iddia edilen siber operasyonlar, siber güvenliğin ulusal ve uluslararası bir güvenlik meselesine dönüşmesinde önemli rol oynamıştır. Her ne kadar siber diplomasi ve uluslararası hukuk, siber alanın militerleşmesini geriden takip etse de son on yılda uluslararası siber güvenlik normların benimsenmesi amacıyla birçok uluslararası girişim olmuştur. Bu makale, Martha Finnemore ve Kathryn Sikkink (1998) tarafından geliştirilen normların yaşam döngüsü modeli çerçevesinde Birleşmiş Milletler'in silahsızlanma ve uluslararası güvenlik konuları ile ilgilenen Birinci Komitesi'nde yirmi yıldan uzun bir süredir uluslararası güvenlik bağlamında devletlerin siber teknoloji kullanımlarına yönelik sürdürülen müzakerelere odaklanarak uluslararası siber güvenlik normlarının ortaya çıkışına ve siber alana ilişkin uluslararası rejimlerin oluşumunun ilk aşamasına, yani norm yaşam döngüsünün başlangıcına ışık tutmayı amaçlamaktadır. Makale, Birleşmiş Milletler'in Birinci Komitesi altında görev yapan Açık Uçlu Çalışma Grubu'nun 2021 yılındaki nihai raporunun siber alanda sorumlu devlet davranışına ilişkin normların ilk aşamadan ikinci aşamaya geçmesi bakımından kritik öneme sahip olduğunu iddia edecektir.

Anahtar Kelimeler

Uluslararası siyaset, Uluslararası normlar, Uluslararası siber güvenlik, Birleşmiş milletler, Uluslararası örgütler, Siber alan, Enformasyon güvenliği, Uluslararası hukuk, Siber savaş, Siber normlar, Uluslararası siber güvenlik normları

International Cybersecurity Norms and Responsible Cyber Sovereignty

Abstract

Initially envisioned as a free and open communication space between people, free from state regulation and intervention, cyberspace has become a fundamental subject of national and global politics over the last decade. Allegedly state-sponsored cyber operations against Estonia in 2007, Georgia in 2008 and Iran in 2010 played an important role in turning cybersecurity into a national and international security issue. Although the development of cyber diplomacy and international cybersecurity law were left behind the militarization of cyberspace, nevertheless, there have been many international initiatives to adopt international cybersecurity norms in the past decade. Within the framework of the life cycle model of the norms developed by Martha Finnemore and Kathryn Sikkink (1998), this article aims to shed light on the emergence of international cybersecurity norms by focusing on the negotiations held at the First Committee of the United Nations for more than twenty years. The article argues that those negotiations held under the First Committee dealing with disarmament and international security issues indicate the first stage of the formation of international rules related to cyberspace, and the negotiations to be completed under the UN Open-Ended Working Group in 2021 is critical for the transition of international cybersecurity norms from the first to the second stage.

Keywords

International politics, International norms, International cyber security, United nations, International organizations, Cyberspace, Information security, International law, Cyber war, Cyber norms, International cybersecurity norms

* **Sorumlu Yazar:** Tuba Eldem (Dr. Öğr. Üyesi), Fenerbahçe Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, İstanbul, Türkiye - Research Fellow, the Center for Applied Turkey Studies (CATS) of the German Institute for International and Security Affairs (SWP). E-posta: tuba.eldem@fbu.edu.tr ORCID: https://orcid.org/0000-0001-6264-255X

Atıf: Eldem T, "Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik" (2021) 79(1) İstanbul Hukuk Mecmuası 347. https://doi.org/10.26650/mecmua.2021.79.1.0010

Extended Summary

Cyberspace has increasingly been subjected to highly sophisticated, large-scale, and often allegedly state-sponsored cyber operations. An important question that arises here is how the basic power rivalries that provide this increase in offensive cyber abilities will affect diplomatic efforts to prevent conflict in cyberspace. Over the past decade, many states have begun to develop their national cyber capabilities, defined cybersecurity strategies, and started to establish cyber defense commands within their military structures that can fight in cyberspace. Although the development of cyber diplomacy and the application of international law left behind the militarization of the cyberspace, the international community has, nevertheless, agreed on an international framework comprising four elements: the application of international law to cyberspace, the adoption of the norms of responsible state behavior in times of peace, the development of confidence-building measures as a way to reduce cyber conflict, and capacity building to enable states to better protect themselves from destructive or unbalancing cyber activity. All members of the UN General Assembly have repeatedly reaffirmed this framework, which was included in three consecutive UN Group of Governmental Experts (GGE) reports in 2010, 2013 and 2015. The norms recommended by the UN GGE in 2015 to provide an 'open, safe, stable, accessible and peaceful cyberspace for all' were supported by many multilateral and multi-stakeholder international and regional platforms. Disagreements on how to apply international law to cyberspace and the scope of cyber sovereignty prevented the UN GGE from reaching a consensus at its last meeting in 2017, representing a short pause in the life cycle of international cybersecurity norms. Yet, a new process started by the approval of the two rival motions by the UN General Secretariat in 2018 and two different groups [a new GGE and a new Open-Ended Working Group (OEWG)] were established in 2019 with a similar mandate.

The OEWG, which allows all states and stakeholders to participate, has the potential to play a critical role in spreading these norms to wider audiences by producing concrete recommendations on what responsible state behavior in cyberspace means in practice and how they can be implemented. As a matter of fact, diplomatic negotiations within the OEWG may contribute to the formation of an inter-state agreement on what behaviors are considered appropriate in cyberspace. When it comes to the compliance of states with norms, the shared recognition of norms is more important than their official validity. Considering that the effectiveness of the norms depends on how and where these norms are accepted, which actors participate in international interactions and where and how often they interact with, the OEWD with its wide multi-stakeholder structure, has the potential to increase the social recognition and legitimacy of these norms. The literature reveals that acceptance of norms depends on actors being part of the process of building socially structured

meanings of such norms. The negotiations carried out in the OEWG allows more states to become part of the process and participate in the conceptualization and implementation of international cybersecurity norms. The OEWG has, therefore, the potential not only to provide broader international recognition of these norms and principles, but also to increase the degree of legitimacy of these norms depending on the degree of persuasion created by the negotiations. Finally, given the voluntary nature of the existing norms, the lack of a binding framework and an institutional mechanism to oversee the implementation of these norms, their implementation will ultimately depend on political will. Only a belief maintained by the states that it is in their interests will motivate them to allocate the necessary resources to enforce the norms, share their experiences and hold each other responsible.

Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik

Başlangıçta, devlet düzenlemesi ve müdahalesinden arınmış kişiler-arası özgür ve açık bir iletişim, haberleşme ve paylaşma alanı olarak tahayyül edilen siber alan kısa süredae küresel siyasetin temel bir konusu ve siyasi, sosyal, ekonomik ve askeri gücün temel unsurlarından biri haline gelmiştir. 2007'de Estonya'ya, 2008'de Gürcistan'a ve 2010'da İran'a yönelik gerçekleştirilen devlet-destekli olduğu iddia edilen siber saldırılar, siber güvenliğin ulusal ve uluslararası bir güvenlik meselesine dönüşmesinde önemli rol oynamıştır. Kuzey Atlantik Antlaşması Örgütü (NATO), Estonya'daki saldırıdan hemen sonra Estonya'nın başkenti Tallinn'de bir Siber Savunma Mükemmeliyet Merkezi kurmuş ve 2016 yılındaki Varşova Zirvesi'nde siber alanı; kara, hava, deniz ve uzaya eşit bir savaş ve etki alanı olarak kabul etmiştir.[1] Böylece, NATO siber saldırıyı içine alan bir siber savunma strateji geliştirirken, üye devletler de askeri yapıları içinde siber alanda savaşabilecek birlikler tesis etmeye başlamışlardır. Bugün, yüzden fazla devlet siber kabiliyetini oluşturmuş ve elliden fazlası ulusal siber stratejilerini tanımlamıştır.[2] Otuzdan fazla ülke, çoğunlukla "enformasyon operasyonları" ve "enformasyon savaşı" terimlerini kullanarak, siber operasyonlar ve saldırgan siber savaş programları için askeri doktrinler geliştirmiştir.[3]

Her ne kadar siber diplomasi, siber alanın militerleşmesini geriden takip etse de son on yılda küresel siber normların benimsenmesi amacıyla birçok uluslararası girişim olmuştur. Bu makalenin amacı, Martha Finnemore ve Kathryn Sikkink tarafından geliştirilen norm yaşam döngüsü modeli çerçevesinde siber normların ortaya çıkmasına ve siber alana ilişkin uluslararası rejimlerin oluşumunun ilk aşamasına, yani norm yaşam döngüsünün başlangıcına ışık tutmaktır.[4] Geçtiğimiz on yılda, uluslararası toplum, uluslararası kurallara dayalı düzenin ve uluslararası hukukun siber alanda devlet davranışına rehberlik etmesi gerektiğini açıkça ortaya koymuştur. Birleşmiş Milletler'in (BM) silahsızlanma ve uluslararası güvenlik konuları ile ilgilenen Birinci Komitesi, bu tartışmalar için erken ve önemli forumlardan biri olmuştur. BM üye devletleri, Birinci Komite altında 1999'dan beri süren müzakerelerde uluslararası hukukun siber alana uygulanabilirliği, barış zamanında gönüllü sorumlu devlet davranış normları, siber olaylardan kaynaklanan çatışma riskini azaltmaya yardımcı olacak güven artırıcı önlemler ve gelişmekte olan ülkelerin siber saldırılara etkin bir şekilde cevap verebilmesi için kapasitelerinin geliştirilmesi üzerine kurulu bir uluslararası çerçeve etrafında giderek daha fazla birleşmiştir. BM Genel Kurulunun

---

1 NATO, Warsaw Summit Communiqué: Issued by the Head of States and Governments participating in the meeting of the North Atlantic Council in Warsaw on 8-9 July 2016, Madde 70, https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en Erisim Tarihi 20 Kasım 2019.

2 Melissa E. Hathaway ve Alexander Klimburg, 'Preliminary Considerations: On National Cyber Security' , içinde: A Klimburg (der) *National Cyber Security Framework Manual* (NATO CCD COE Publication, 2012) 2.

3 ibid 2;Ronald J. Deibert ve Rafal Rohozinski, 'Risking Security: Policies and Paradoxes of Cyberspace Security' (2010) 4 (1) *International Political Sociology* 16, 17.

4 Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change' (1998) 52 (4) International *Organization* 894-905.

tüm üyeleri, 2010, 2013 ve 2015 yıllarında birbirini izleyen üç BM Hükümet Uzmanları Grubu (*Group of Governmental Experts- HUG*) Raporu'nda yer alan bu çerçeveyi defalarca teyit etmiştir.

Bu makale, BM müzakerelerinin siber savaşa yönelik olan siyasi-askeri eksenini ele alarak, siber alanda sorumlu devlet davranışına ilişkin normların ortaya çıkma sürecine odaklanacaktır. Her ne kadar siber normların tanımı konusunda net bir görüş birliği olmasa da bu makalede, uluslararası siber normlar devletlerin enformasyon ve iletişim teknolojilerini, bir başka deyişle siber teknolojileri, kullanırken uymaları beklenilen davranış standartlarını ifade etmektedir. Buradan hareketle, BM Birinci Komitesi altında sürdürülen müzakerelerde ortaya çıkan "sorumlu siber egemenlik" normu, kendi ülkelerindeki siber teknolojiler üzerinde egemenlik yetkisine sahip olan devletleri siber alanda uluslararası yanlış eylemler içine girmemesi ve bu tür eylemler için vekiller kullanmaması konusunda yükümlü kılan bir davranış standardı olarak tanımlanabilir. Her ne kadar var olan uluslararası hukuk kuralları üzerine inşa edilmiş olsa da normun kendisi henüz hukuki bağlayıcılık kazanıp kurumsallaşmamıştır. Bu bağlamda, bu makale, siber alanda sorumlu devlet davranış normlarını geliştirmek için 2019'un sonbaharında başlayan ve BM Hükümet Uzmanları Grubu'na paralel olarak devam eden Açık-Uçlu Çalışma Grubu'nda (*Open-Ended Working Group*) sürdürülen müzakerelerin siber normların yaşam döngüsündeki ilk safhadan ikinci safhaya geçmesinde kritik aşamayı oluşturduğunu iddia edecektir.

Makale, siber alana ilişkin temel kavramların ve çalışmaya rehberlik eden uluslararası normların yaşam döngüsü modelinin tanımlanması ile başlamaktadır. II. Bölüm, Rusya Federasyonu (Rusya) ve Amerika Birleşik Devletleri'ni (ABD) siber alanda iki önemli norm girişimcisi olarak ele alacak ve uluslararası siber güvenliğin iki devlet tarafından farklı şekillerde tanımlandığı üzerinde duracaktır. III. Bölüm, norm girişimcilerinin siber normların ortaya çıkması için etkin bir örgütsel platform olarak kullandıkları BM Birinci Komitesi'nde siber alanın siyasi ve askeri boyutlarıyla ilgili yürütülen müzakerelerin tarihsel bir analizini sunarak siber normların yaşam döngüsünün başlangıcına ışık tutacaktır. IV. Bölüm, 2019 yılında kurulan Açık-Uçlu Çalışma Grubu'nda sürdürülen müzakerelerin siber normların kritik aşamayı geçip genel geçerlilik kazanmasındaki önemi üzerinde duracaktır. Bu bağlamda, makale uluslararası siber güvenlik hukuku alanında Türkçe dilindeki akademik literatüre siber normların ortaya çıkma süreci ve bu normların içeriği hakkında katkı sunmayı hedeflemektedir. Nitekim yeni gelişmeye başlayan söz konusu literatür, siber teknolojilerin savaş ve savunma sektöründeki dönüştürücü etkisini araştırmış,[5]

[5] Şirin Duygulu, *Dönüşen Savaşların Değişen Araçları* (SETA, 2019).

çeşitli siber güçlerin siber güvenlik stratejilerini incelemiş[6], siber savaşı uluslararası sistem ve güvenlik açısından[7] ve hukuki bir terim olarak ele almış[8] ve uygulanma sorunu üzerinde durmuştur.[9] Fakat geçtiğimiz son yirmi yıl içinde Birleşmiş Milletler bünyesinde ortaya çıkan birtakım gönüllü, bağlayıcı olmayan uluslararası siber güvenlik normları konusuna değinmemiştir. Bu makale söz konusu literatürdeki bu boşluğu doldurmayı hedeflemektedir.

Uluslararası Siber Normlar ve Kavramlar

Siber alan kavramı, siber hukuk ile ilgili temel unsurdur, çünkü siber normların oluşturulabileceği çerçeveyi ortaya koymaktadır. Her ne kadar günlük dilde internetle ile eşanlamlı kullanılsa da aslında siber alan internetten kapsamı daha geniş olan bir kavramdır. Siber alan kavramını, ilk defa William Gibson'ın Neuromancer adlı kitabında bilgisayar ağları arasındaki büyük bir bağlantı ağının aracılık ettiği insan-makine ilişkilerinde temel bir dönüşümü tanımlamak için kullanmıştır.[10] Önek olarak siber, elektronik ve bilgisayar tabanlı teknolojiyi ifade etmektedir.[11] Dolayısı ile siber alan tüm telekomünikasyon ve bilgisayar ağları, SCADA ve diğer komuta ve kontrol sistemleri gibi donanım ve elektronik aletlerin belirli bir iş yapmasını sağlayan yazılımlar da dahil olmak üzere tüm enformasyon altyapılarını ve bu altyapılar aracılığı ile ortaya çıkan sanal bilgi ve insanlar-arası etkileşim ortamının toplamını ifade etmektedir.[12] Literatür, siber alanı fiziksel, mantıksal ve bilişsel katmanlardan oluşan çok-katmanlı bir alan olarak kavramsallaşmaktadır.[13] Buna göre mekanik, elektriksel, manyetik ve optik iletişim hatlarını kullanan yönlendiriciler, kablolar, cep telefonu kuleleri ve uydulardan oluşan makineler siber alanın fiziksel

---

6 Şener Çelik, 'Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme' (2013) 15 (1) *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 137-175; Ali Burak Darıcılı, "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi", *Ulisa: Uluslararası Çalışmalar Dergisi*, Cilt 1, No 1, 2017, s. 1-24.

7 Vahit Güntay, 'Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği' (2017) 6 (2) *Güvenlik Bilimleri Dergisi* 81-108.

8 Mehmet Yayla, 'Hukuki Bir Terim Olarak —Siber Savaş' (2013) 104 TBB Dergisi 177-202.

9 Şeyda Türkay, 'Siber Savaş Hukuku ve Uygulanma Sorunsalı' (2013) 71 (1) *Journal of Istanbul University Law Faculty* 1177-1227..

10 William Gibson, *Neuromancer (*Ace Science Fiction Books, 1984).

11 Tim Maurer, 'Cyber Norm Emergence at the United Nations, – An Analysis of the UN's Activities Regarding Cyber-security' (2011) *Belfer Center Discussion Paper* #2011-11, 8 https://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf 20 Kasim 2019

12 United Kingdom National Security Strategy 2016-2021 75 https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 Erişim Tarihi 20 Kasim 2019; United States National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), 2008, 3; United States National Security Council, *Cyberspace Policy Review: Securing America's Digital Future* (Cosimo Incorporated, 2010) 1.

13 United States Government, *US Army Joint Publication JP 3-12 Cyberspace Operations,* (CreateSpace Independent Publishing Platform, June 2018) 1-3 https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf Erişim Tarihi 20 Kasim 2019; Benzer yaklasimlar icin bakiniz: Nazli Choucri ve David D. Clark, 'Who Controls Cyberspace?' (2013) 69 (5) *Bulletin of the Atomic Scientists* 21–31; Nazli Choucri ve David D. Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma (*The MIT Press, 2019).; David Clark, Characterizing Cyberspace: Past, Present and Future' (2010) MIT/CSAIL Working Paper; Ronald J. Deibert, Rafal Rohozinski ve Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War' (2012) 43 (1) *Security Dialogue* 3–24.

altyapı katmanını oluşturmaktadır.[14] DNS ve ISP gibi iletişim trafiğini çalıştıran mantıksal talimatlar ve yazılımlar kod katmanını, "stratejik iletişim" veya askeri alanda "enformasyon operasyonları" olarak adlandırılan videolar, görüntüler, sesler ve metinlerin dolaştığı alan ise fikirsel ya da bilişsel katmanı oluşturmaktadır.[15]

Siber operasyon kavramı, siber alan içinde ya da aracılığıyla önceden belirlenen hedeflere ulaşmak için siber alan yeteneklerinin kullanılmasını ifade etmektedir.[16] Bu tür operasyonlar, herhangi bir yazılım, bellenim veya donanım kombinasyonu da dahil olmak üzere herhangi bir cihaz, bilgisayar programı veya tekniği aracılığıyla yürütülebilir.[17] Siber alana yönelik operasyonlar, bilgisayar ağ operasyonları aracılığı ile siber alanın fiziksel altyapısı veya enformasyonun saklandığı ağ ve sistemlerden oluşan kod tabakasını hedef alırken, siber alan aracılığı ile gerçekleştirilen enformasyon operasyonları ise siber alanın bilişsel katmanını hedef almaktadır. Saldırgan siber operasyonlar, hedeflenen bilgisayar, enformasyon sistemleri veya ağlarını manipüle etme, erişime engelleme, sekteye uğratma, işlevini bozma veya yok etme amacıyla gerçekleştirilen işlemleri ifade etmektedir.[18] Fiziksel altyapı ve ağları hedef alan bu operasyonlar, kişilerin yaralanması veya ölmesi ile sonuçlanıyorsa veya nesnelere hasar veya tahribat yaratması bekleniyorsa, siber saldırı olarak tanımlanır.[19] Son zamanlarda siber alanın belirgin bir rol oynadığı birçok uluslararası çatışma vakaları yaşansa da bunların hiçbiri uluslararası hukuk altında siber saldırı olarak tanımlanmamış, kınama ve inkar politikaları ile sonuçlanmıştır. Örneğin, Nisan 2007'de Estonya'da, dünyanın dört bir yanından milyonlarca bilgisayar hacklenerek bir botnet olarak bir araya getirilmiş ve bu bilgisayarlar eşzamanlı olarak ülkenin kamu kurumlarına, telekomünikasyon, bankacılık ve finans gibi kritik altyapı sektörlerine yönelik geniş çaplı bir hizmet dışı bırakma (Distributed Denial of Service / DDoS) saldırısı gerçekleştirmiştir.[20] 2008'de Gürcistan[21], 2014'de Ukrayna kinetik savaşa eşlik eden benzer siber operasyonlara tanık olmuştur. Kırım Savaşı sürecinde Ukrayna'nın mobil telefon iletişim ve internet altyapıları saldırıya uğramış ve büyük oranda çökmüş, bürokrat ve milletvekillerine ait akıllı cep telefonlarının tamamı hacklenmiş, silahlı kuvvetler de dahil olmak üzere resmi devlet sitelerine ve medya kuruluşlarına yönelik olarak Estonya ve Gürcistan'dakine benzer hizmet-

14 Deibert, Rohozinski ve Crete-Nishihata (n 13) 5.

15 Ibid 6.

16 United States Government (n 13) vii.

17 ibid 4

18 ibid 4

19 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare (*Cambridge University Press, 2013) 30.

20 Stephen Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses' (2011) 4 (2) *Journal of Strategic Security* 49-60.

21 Deibert, Rohozinski ve Crete-Nishihata (n 13).

dışı bırakma saldırıları düzenlenmiştir.[22] Diğer yandan, Aralık 2015'de Ukrayna'nın en büyük üç elektrik dağıtım şirketinin kontrol sistemlerine düzenlenen ve ülkede yedi saat boyunca elektrik verilmesini engelleyen siber-fiziksel saldırılar dünyadaki elektrik güç şebekesini hedef alan ilk başarılı siber operasyon olarak tarihe geçmiştir.[23] Siber alanda fiziksel hasara yol açan ilk siber operasyon örneği ise 2010'daki Stuxnet virüsü aracılığı ile İran'ın Natanz'daki ana nükleer zenginleştirme merkezindeki santrifüjlerde fiziksel tahribata yol açan operasyondur ve bu özelliği ile uluslararası hukukta siber saldırı tanımını karşılamaya en yakın adaydır.[24]

Siber alanın fiziksel altyapısı veya bilginin saklandığı ağ ve sistemlerden oluşan kod tabakasını hedef alan bilgisayar ağ operasyonlarının yanında siber alanının bilişsel ya da fikirsel katmanını hedef alan enformasyon operasyonlarının sayısı da son yıllarda gittikçe artmaktadır. Siber alan aracılığı ile gerçekleştirilen enformasyon operasyonları, devlet veya devlet dışı organize aktörler tarafından stratejik ve/veya jeopolitik bir sonuç veya rekabet avantajı elde etmek için enformasyon kullanımı ve yönetimini içermektedir.[25] Son birkaç yıla baktığımızda bu operasyonların özellikle seçim dönemlerinde ya da referandum süreçlerinde gerçekleştiği görülmektedir. 2016 yılında ABD[26] ve 2017 yılında Fransa[27] cumhurbaşkanlığı seçimlerinde ve 2016'da İngiltere'de Brexit[28] referandum süreçlerinde devlet-destekli olduğu iddia edilen enformasyon operasyonları gerçekleştirilmiştir. Siber alanda veya siber alan aracılığı ile devlet-destekli ve devlet-dışı aktörler tarafından gerçekleştirilen bilgisayar ağ operasyonları ve enformasyon operasyonların sayısının artması ve niteliğinin gelişmesi uluslararası toplumda siber alanı düzenlemeye yönelik birtakım normların benimsenmesi yönündeki talepleri arttırmıştır.

Siber normlar, en basit ve geniş haliyle, siber alan için geçerli olan normları ifade etmektedir. Sosyal bilimlerde yaygın olarak kabul edilen görüşe göre, normlar "neyin yapılıp neyin yapılamayacağını, neyin onaylanıp, onaylanmadığını belirten sosyal

[22] Glib Pakharenko, "Cyber Operations at Maidan: A First-Hand Account", icinde Kenneth Geers (der.), Cyber War in Perspective: Russian Aggression against Ukraine (*NATO CCD COE Publications*, 2015) 59-66; Azhar Unwala ve Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict", (2015) 1 (1) *Military Cyber Affairs*.

[23] Julia E. Sullivan ve Dmitriy Kamensky, 'How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid' (2017) 30 (3) *The Electricity Journal*, 30-35.

[24] James P. Farwell ve Rafal Rohozinski, "Farwell J P ve Rohozinski R, 'Stuxnet and the Future of Cyber War' (2011) 53 (1) *Survival* 23-40; Ryan Jenkins 'Is Stuxnet Physical? Does It Matter?' (2013) 12 (1) *Journal of Military Ethics* 68-79, Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare' (2013) 22 (3) *Security Studies* 365-404.

[25] Robert Chesney ve Danielle Citron, 'Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics' (January / February 2019) *Foreign Affairs* 147–155; Barrie Sander, 'Democracy under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections' (2019) 18 (1) *Chinese Journal of International Law* 1–56.

[26] Stephen McCombie, Allon J. Uhlmann ve Sarah Morrison, 'The US 2016 Presidential Election & Russia's Troll Farms' (2020) 35 (1) *Intelligence and National Security* 95-114; Nigel Inkster, 'Information Warfare and the US Presidential Election' (2016) 58 (5) *Survival* 23-32.

[27] Emilio Ferrara, 'Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election' (2017) 22 (8) *First Monday*.

[28] United Kingdom Parliament Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Final Report, Eighth Report of Session 2017–19,* HC 1791, London: House of Commons, 2019; Philip N. Howard ve Bence Kollan, 'Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum' (2016) *ArXiv, abs/1606.06356*,

davranış standartlarıdır".[29] Bir başka deyişle, normlar "toplu taşıma araçlarında koltuğun yaşlılara verilmesi" veya "sinemada gürültü yapılmaması" gibi sosyal beklentilere uygun davranış standartlarını ifade etmektedir. Normlar, ilke ve yasalardan farklıdır. Bir grubun veya kurumun değerlerini ve vizyonunu yansıtan ilkeler, aktörlerin belirli bir hedefe ulaşmak için hangi eylemleri gerçekleştirmeleri gerektiğini tanımlamaz. İlkelerden daha spesifik olan normlar ise aktörleri belirli davranış beklentileri ile ilişkilendirerek bu aktörlerin aktif hesap verebilirliğini teşvik eder. Bir grubun üyelerinin davranışlarını yöneten gayri resmi kuralları ifade eden normlar, resmi bir kuruluşun bir mevzuatın şartlarını uygulama yetkisi ile yürürlüğe koyduğu bağlayıcı ve genellikle yaptırımlarla desteklenen yasalardan farklıdır. Buradan hareketle, uluslararası normlar, uluslararası toplumda "belirli bir kimlik sahibi aktörün uyması beklenilen davranış standartlarını" ifade eden ve aktörlerin davranışları hakkında kolektif bir beklenti oluşturarak siyasi sorumluluklarını netleştiren ve yükümlülükler oluşturan politika araçlarıdır.[30] Uluslararası normlar, ikili anlaşmalar yoluyla veya devlet grupları veya diğer aktörler tarafından geliştirilebileceği gibi tek taraflı olarak ilan edilebilir ya da devlet ya da diğer uluslararası aktörlerin uygulamalarına bağlı olarak gelişir. Uluslararası normlar, uygulama ve aktarma, içselleştirme, sosyal öğrenme, anayasallaştırma ve yasallaştırma süreçleri ile etkin hale gelir.[31] Normların yasal kabulü, antlaşma hukuku, teamül hukuku, ulusal ilkeler ve Uluslararası Adalet Divanı kararları gibi uluslararası hukuktaki kaynak ve uygulamalara bağlı olarak gelişse de uluslararası siyasette normlar, usul ve referans çerçeveleri sunan daha geniş bir sosyal bağlamın bir parçası olarak değerlendirilir.[32] Uluslararası normların nasıl ve nerede kabul edildiği ve hangi aktörlerin nerede ve ne sıklıkla uluslararası etkileşimlerde bulunduğu söz konusu normların etkinliğini etkilemektedir.[33] Aktörlerin normların sosyal olarak yapılandırılmış anlamlarını inşa etme süreçlerine katılmaları söz konusu normların kabulünü olumlu olarak etkilemektedir. Açık ve kapalı müzakerelere izin veren uluslararası kuruluşlar bünyesinde normlar sosyal tanınma ve ikna süreçleri ile yaygınlaşabilir. Nitekim normların sosyal tanınırlığı, devletlerin normlara uyumunda resmi geçerlilikten daha çok etkili olmaktadır.[34] Kara mayınlarına karşı kampanya, kimyasal silah yasağı, balinaların korunması, ırkçılıkla mücadele, soykırımın önlenmesi için müdahale, insan haklarının geliştirilmesi gibi birçok uluslararası normun devlet davranışını etkilediği ve kimi zaman değiştirdiği bir dizi araştırma tarafından ortaya konmuştur.[35]

[29] Cass R. Sunstein, 'Social Norms and Social Roles' (1996) 96 (4) *Columbia Law Review* 914.

[30] Finnemore ve Sikkink (n 4) 891.

[31] Antje Wiener ve Uwe Puetter, 'The Quality of Norms is What Actors Make of It' (2009) 5 (1) *Journal of International Law and International Relations* 1-16.

[32] ibid 5

[33] ibid.

[34] Martha Finnemore ve Stephen J. Toope, 'Constructing Norms for Global Cybersecurity' (2016) 110 (3) *The American Journal of International Law* 425- 479.

[35] Finnemore and Sikkink (n 3); Amitav Acharya, "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism", (2004) 58 (2) *International Organization* 239–75; Thomas Risse, Stephen C. Ropp ve Kathryn Sikkink, (der.), *The Power of Human Rights: International Norms and Domestic Change (*Cambridge University Press, 1999).

Marta Finnemore ve Kathryn Sikkink'in geniş kabul gören "normların yaşam döngüsü" modeline göre, uluslararası normlar, üç aşamalı bir süreçten geçerek kurumsallaşmaktadır. Normların ortaya çıktığı ilk aşamada, "norm liderleri" veya "norm girişimcileri" önemli rol oynamaktadırlar. Norm girişimcileri, örgütsel birtakım platformlardan yararlanarak ve sosyalleşme, itibar referansları, teknik yardım ve eğitim, kapasite oluşturma, adlandırma ve utandırma gibi farklı araçlar kullanarak söz konusu normun benimsenmesi için çalışırlar. Bu örgütsel platformların gerekli bilgi, uzmanlık ve kaynaklara sahip olması, normun kabulünü sağlayacak etkiyi oluşturabilmek adına kritik öneme sahiptir. Eğer norm girişimcileri, belirli bir sayıda devleti normu kabul etmeye ikna ederlerse, söz konusu yeni norm, yaşam döngüsünde kritik bir aşamayı geçerek yaygınlaşmaya başlayacaktır. Normların dönüm noktasını aşarak yaygınlaştığı bu ikinci safhada, devletler, uluslararası toplumun bir üyesi olma, siyasi kimliklerini ispat etme, meşruiyet kazanma ve itibar görme dürtüleri ile bu yeni normları benimseyeceklerdir. Böylece, bir devlet tarafından benimsenen uluslararası normlar, o devletin uluslararası kimliği ve ait olduğu devlet grubunu belirlemede etkin bir rol oynayacaktır. En son safha olan üçüncü safhada ise sosyalleşme, öğrenme, müzakere ve ikna, sosyal baskı gibi süreçlerle geniş ölçüde içselleştirilen normlar evrenselleşecek ve uluslararası geçerlilik kazanacaktır. Daha önce de belirtildiği gibi, normlar yasalara veya yasal olarak bağlayıcı önlemlere zaman içerisinde dönüşebilir. Diğer yandan, uluslararası normlar, yasal statü kazanmadan da özellikle hukukun üstünlüğü ilkesinin güçlü olduğu rejimlerde aktörlerin davranış, tercih ve beklentilerini yapılandıran davranış standartları olarak gelişebilir. Tersine, yaygın olarak paylaşılmayan ve kabul edilmeyen normlar yasalaşsa dahi etkisiz olabilir.

Uluslararası toplumun gündeminde siber alanı düzenlemeye yönelik birçok uluslararası norm, kural, yasa ve ilke yer almaktadır.[36] Joseph Nye, küresel siber alan yönetişiminin kapsamına giren yedi farklı alandan bahseder: 1- alan adı adresi (DNS) ve teknik standartlar, 2- suç, 3- savaş / sabotaj, 4-casusluk, 5-çevrimci gizlilik, 6-içerik kontrol, 7-insan hakları.[37] Bu alanlarla ilgili olarak siber saldırılarda çekirdek internet altyapısının kamu malı olarak korunması, sivillerin hasar almasının önlenmesi, seçim sistemlerinin korunması, siber suçların önlenmesi gibi birçok farklı norm önerileri sunulmuştur.[38] Bu makale, daha önce de belirtildiği gibi BM'nin Birinci Komitesi'nde ele alınan ve devletlerin siber teknolojileri kullanımları konusundaki davranış standartlarını belirten siber normlara odaklanacaktır. Bu bağlamda,

[36] Martha Finnemore ve Duncan B. Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110 (3) *The American Journal of International Law* 425- 479; Jürgen Feick ve Raymund Werle, "Regulation of Cyberspace", icinde Robert Baldwin, Martin Cave, ve Martin Lodge (der.), *The Oxford Handbook of Regulation* (Oxford University Press, 2010) s. 523-547; Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press, 2010).

[37] Joseph S. Nye, The Regime Complex for Managing Global Cyber Activities, *Global Commission on Internet Governance Paper Series*, 2014, 9-11.

[38] The Global Commission on the Stability of Cyberspace, *Norm Package Singapore*, Kasım 2018, https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf Erişim Tarihi 3 Ocak 2020; Geneva Internet Platform (GIP) Digital Watch, UN GGE and OEWG, 2019, https://dig.watch/processes/un-gge Erişim Tarihi 3 Ocak 2020.

aşağıdaki bölüm farklı siber güvenlik anlayışına sahip olan Rusya ve ABD'yi iki önemli norm girişimcisi olarak ele alarak BM Birinci Komitesi'nde uluslararası siber güvenlik alanında yapılan çalışmaları ve tartışmaları analiz edecek ve 2019 yılından beri devam eden BM Hükümet Uzmanları Grubu ve Açık-Uçlu Çalışma Grubu'ndaki müzakerelerde karşılaşılanabilecek zorlukları tartışacaktır.

Norm Girişimcileri ve Norm Çekişmeleri: Enformasyon Güvenliği mi Siber Güvenlik mi?

Rusya, enformasyon güvenliğinin[39] uluslararası güvenlik bağlamında ele alınmasında norm girişimcisi olarak önemli rol oynamıştır.[40] Uluslararası enformasyon güvenliği konusunda ABD ile sürdürdüğü ikili müzakerenin başarısızlıkla sonuçlanmasının ardından Rusya, BM Genel Kuruluna uluslararası güvenlik bağlamında enformasyon ve iletişim teknolojilerindeki gelişmelere ilişkin bir önerge sunmuştur.[41] BM Genel Kurulu önergeyi 53/70 sayılı kararı ile kabul ederek enformasyon güvenliğinde bilimsel ve teknolojik gelişmelerin olduğunu, ancak potansiyel kötü amaçlı kullanımının da olabileceğinin altını çizmiş ve BM Üye Devletlerinin enformasyon güvenliği konusunda görüşlerini isteyen yıllık önergeleri kabul etmeye başlamıştır.[42] 2001 yılından itibaren Rusya, enformasyon güvenliği alanında mevcut ve potansiyel küresel tehditleri azaltmak için alınacak önlemler konusunda genel kabul görmüş uluslararası standartlar veya araçlar mevcut olmadığından bu konu üzerine çalışacak bir özel bir hükümet uzmanları grubu kurulmasını önermiştir.[43] BM Genel Kurulu 58/32 Sayılı Kararı ile Rusya'nın önergesini kabul ederek Genel Sekreter'den devletlerin enformasyon ve iletişim teknolojilerinin kullanımından kaynaklanan mevcut ve potansiyel tehditleri değerlendirmek ve bunlara karşı ortak önlemlerin belirlenmesi için bir hükümet uzmanları grubunun 2004 yılında kurulmasını ve sonuç raporunu Genel Kurul'a sunmasını istemiştir.[44] 2004 yılından günümüze kadar altı farklı hükümet uzmanları grubu oluşturulmuş ve bu gruplar 2010, 2013 ve 2015'te siber alanda devlet davranışlarını düzenlemeye yönelik birtakım normlar üzerine uzlaşmaya varmışlardır. BM HUG raporları ve ilgili BM Genel Kurul kararları mevcut

[39] Başlangıçta "verilerin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması" olarak tanımlanan enformasyon güvenliği kavramı, Rusya ve Çin gibi devletlerin enformasyonun içeriğinin de siyasal rejimlerinin istikrarı için tehdit olarak algılanmalarından dolayı genişletilerek bu devletler tarafından "bireyin, toplumun, devletin ve bu aktörlerin çıkarlarının enformasyon alanındaki tehditlerden, yıkıcı ve diğer olumsuz etkilerden korunması" olarak tanımlanmıştır: Shanghai Cooperation Organization, Agreement on Cooperation in the Field of International Information Security, 16 Haziran 2009, https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/SCO-090616-IISAgreement.pdf Erişim Tarihi 15 Ocak 2020

[40] Danielle Flonk, 'Content Control Contestations: Russia and China as Entrepreneurs of Illiberal Internet Norms' (2019) Paper for the Authoritarian Politics and International Relations Workshop, Berlin, January.

[41] UN General Assembly, Revised Draft Resolution, Russian Federation**,** A/C.1/53/L.17/Rev.1, 2 Kasım 1998.

[42] UN General Assembly Resolution 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/53/70, 4 Ocak 1999.

[43] UN General Assembly Resolution 56/19, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/56/19, 7 Ocak 2002.

[44] UN General Assembly Resolution 58/32, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/58/32, 8 Aralık 2003.

uluslararası hukukun siber uzayda geçerli olduğunu belirtmiş, devletlerin kendi ülkelerindeki enformasyon ve iletişim teknolojisi üzerinde egemenlik yetkilerinin olduğu ve devletlerin bu alanda uluslararası yanlış eylemler içine girmemesi ve bu tür eylemler için vekiller kullanmaması gerektiğini vurgulamıştır.

Bu normların etkinliğinin artması ve uluslararası hukukun siber alanda uygulanabilmesi, uluslararası toplumdaki bu normların uygulanmasına yönelik görüş ayrılıklarının azalmasına bağlıdır. Son on beş yıl içinde elliden fazla devletin Birinci Komite ve BM HUG bünyesinde katkıda bulunduğu uluslararası siber güvenlik veya enformasyon güvenliği tartışmaları, ABD ve Rusya'nın başını çektiği iki grubun çekişmesine sahne olmuştur. Bu iki grup devlet arasında norm çekişmesinin temeli siber güvenliğin veya enformasyon güvenliğinin tanımı ve kapsamı, siber güvenliğe yönelik tehdit algıları, devletlerin siber güvenliğini sağlamadaki yetki ve görevleri ve bu normların uygulanmasına dayanmaktadır. Rusya liderliğindeki Çin, İran, Mısır gibi siber egemenler olarak adlandırılabilecek birinci grup ülke, ulusal hükümetleri uluslararası siber politikaları tanımlamak ve uygulamak için yegâne aktörler olarak görmektedir. Ulusal siber alanda sınırsız devlet egemenliğini ve içerik üzerindeki katı devlet kontrollerini savunan bu ülkeler, devletlerin "enformasyon alanlarını" koruma hakkını vurgulamaktadır.[45] Rusya tarafından oldukça geniş ve muğlak şekilde tanımlanan enformasyon alanı kavramı "bireysel ve sosyal bilinç, enformasyon ve iletişim altyapısı ve enformasyonun kendisi de dahil olmak üzere enformasyonun yaratılması, dönüştürülmesi veya kullanılmasını içeren faaliyetlerin yürütüldüğü alanı" ifade etmektedir.[46] Enformasyon güvenliğini "enformasyon alanında ulusal çıkarların korunması"[47] olarak tanımlayan Rusya'nın enformasyon güvenliği doktrini hem enformasyon ve iletişim altyapısına hem de enformasyonun kendisine yönelik tehditlerin ortadan kaldırılmasını içermektedir.[48] Enformasyon içeriğinin gözetimini de kapsayan daha geniş ve bütünleşik bir "enformasyon güvenliği" stratejisi izleyen Rusya, sivil ve askeri enformasyon teknolojilerinin dünya çapındaki gelişiminin uluslararası yasal düzenlemelere ihtiyaç duyduğunu vurgulamaktadır. Nitekim, 1999 yılındaki ilk BM kararından bu yana, Rusya'nın siber alana ilişkin öncelikli dış politikası devletlerin siber silah geliştirmesini veya siber alan aracılığı ile diğer devletlerin içişlerine karışmasını yasaklayacak çok- taraflı bir siber silah kontrol antlaşmasının benimsenmesi yönünde olmuştur.[49]

---

45 Hannes Ebert ve Tim Maurer, 'Contested Cyberspace and Rising Powers' (2013) *34 (6) Third World Quarterly* 1054–1074; Julien Nocetti, 'Contest and Conquest: Russia and Global Internet Governance' (2015) 91 *International Affairs* 111-130.

46 Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space, 2012, https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle Erişim Tarihi 20 Kasım 2019.

47 The Information Security Doctrine of the Russian Federation, 2000, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf Erişim Tarihi 20 Kasım 2019

48 ibid.

49 United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General A/54/213, 10 Ağustos 1999, 9.

Rusya, Şangay İşbirliği Örgütü (The Shanghai Cooperation Organisation- SCO) çerçevesinde ve Çin'in desteğiyle bölgesel düzeyde enformasyon kontrolü normlarını desteklemektedir. SCO üyelerinin 2009 yılında imzaladığı Uluslararası Enformasyon Güvenliği Alanında İşbirliği Anlaşması "diğer devletlerin siyasi, ekonomik ve sosyal sistemini zayıflatmak için enformasyonun kullanılması", "enformasyon alanında egemenlik veya ulusal kontrol" ve "enformasyon yoluyla yetkisiz sınır-aşan etki" gibi Rusya tarafından belirlenen kavram ve tehditleri içermektedir.[50] Anlaşma, enformasyon güvenliğini oldukça geniş şekilde ve yine Rusya'nın ulusal kavramsallaştırmasına benzer bir şekilde "bireyin, toplumun, devletin ve bu aktörlerin çıkarlarının enformasyon alanındaki tehditlerden, yıkıcı ve diğer olumsuz etkilerden korunması" olarak tanımlamaktadır. Bu anlaşmaya dayanarak SCO'nun altı üyesinden dördü 2011 yılında BM Genel Kurulu'na "Uluslararası Enformasyon Güvenliği Davranış Kuralları" adlı bir sözleşme sunmuştur.[51] Sözleşme, başka bir hükümetin politik, ekonomik ve sosyal sistemine zarar vermeyi amaçlayan enformasyon alanındaki eylemleri ve toplumu istikrarsızlaştırma amacıyla aleyhte yürütülen psikolojik kampanyaları enformasyon alanındaki en büyük tehditlerden biri olarak görmektedir.[52] Uluslararası insan hakları hukuku kapsamında ele alınan çevrimiçi gizlilik ve serbest bilgi akışı gibi ilkeleri ihlal ettiği için sivil toplum ve batılı devletlerin eleştirilerine maruz kalan Sözleşme kısıtlı olarak revize edilerek, SCO'nun altı üye devleti tarafından 2015 yılında tekrar BM Genel Kuruluna sunulmuştur.[53]

ABD ve Avrupa ülkelerinin başını çektiği, çok-paydaşlılar olarak adlandırılabilecek olan devlet grubu, serbest bilgi akışı ve kullanıcıların etkinliği üzerinde asgari devlet kontrollerinin olduğu kamu ve özel sektör arasında dağıtılmış bir güvenlik ağı tarafından çok-paydaşlı olarak yönetilen açık ve özgür bir siber alanı savunmaktadır. Enformasyon güvenliği kavramının enformasyonun içeriğini de tehdit olarak içermesi yüzünden karşı çıkan bu devletler, siber-fiziksel altyapı ve ağların güvenliğine odaklanan bir siber güvenlik kavramını tercih etmekte ve BM'de uluslararası güvenlikle ilgili yürütülen müzakerelerde ulusal ve küresel siber ağların ve siber alandaki verilerin güvenilirliğini, kullanılabilirliğini ve bütünlüğünün güvence altına alınması ve kritik altyapılara zarar gelmesinin önlenmesi konularında iş birliğinin öneminin altını çizmektedirler.[54] ABD'nin başını çektiği bu devletler enformasyon güvenliği ve/veya siber güvenliğin kapsamı ve odağı hakkında uluslararası ortak bir anlayış olmadığı ve siber teknolojiler çok hızlı geliştiği için birtakım sivil ve /

[50] Shanghai Cooperation Organization, *Agreement on Cooperation*

[51] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359.

[52] ibid., Madde 4.

[53] Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/273.

[54] Eneken Tikk-Ringas, "*Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012",* (ICT4Peace Publishing, 2012).

veya askeri teknolojilerin geliştirilmesini veya kullanılmasını kısıtlayacak bağlayıcı yasal bir düzenlemeden önce siber alana ilişkin kapsayıcı ilkelerin tüm yönleriyle oluşturulması gerektiğini savunmaktadırlar.[55] Rusya'nın enformasyon güvenliği alanında yasal olarak bağlayıcı bir silah kontrolü antlaşması için sunduğu öneriye karşı uluslararası toplumun "gönüllü normlar" geliştirmesi fikrini ortaya atan ABD Dışişleri Bakanlığı, özellikle 2010 yılından sonra aktif bir şekilde barış zamanında siber alanda devlet davranışını düzenleyecek bir takım bağlayıcı olmayan rızaya dayalı uluslararası normların geliştirilmesi konusunda norm liderliğini üstlenmiştir.[56] ABD ve müttefikleri uluslararası hukukun siber alan için geçerli olduğunu savunmakta ve BM Şartı, mevcut silahlı çatışma antlaşmaları ve insanilik, gereklilik, orantılılık, ayrım gözetme gibi uluslararası insancıl hukukun yerleşik ilkelerinin siber teknolojilerin askeri uygulamalarına uygulanabileceğini öne sürmektedirler. Aşağıdaki bölüm, bu tartışmaların sahne olduğu BM Hükümet Uzmanları Grubunu mercek altına alarak siber alanı düzenleyen gönüllü normların ortaya çıkma sürecine odaklanacaktır.

Birleşmiş Milletler Uluslararası Güvenlik Bağlamında Enformasyon ve Telekomünikasyon Alanındaki Gelişmelerle İlgili Hükümet Uzmanları Grubu (BM HUG)

BM uluslararası güvenlik bağlamında enformasyon ve telekomünikasyon alanındaki gelişmelerle ilgili kurulan Hükümet Uzmanları Grubu (BM HUG), BM'nin Birinci Komitesi altında görev yapan bir çalışma grubudur. 1956 yılından bu yana daimî statüye sahip olan Birinci Komite, BM Genel Kurulunda bulunan altı ana komiteden biridir. Genel Kurulun sözlü kayıtları olan tek ana komitesi olan Birinci Komite, silahsızlanma ve uluslararası güvenlik konularındaki gündem maddelerini belirlemekle yetkilidir. Nükleer, kimyasal, biyolojik ve kitle imha silahlarının yayılmasını önleme, uzayın silahsızlandırılması ve uzayda silahlanma yarışının önlenmesi gibi alanlarda önemli başarılara imza atan Birinci Komite, uluslararası siber güvenlik tehditlerinin tartışıldığı en üst düzey forumdur. Birinci Komite, son yirmi yılda siber alanda devletlerin sorumlu davranışları, güven artırıcı önlemler ve kapasite geliştirme norm, kural ve ilkelerini göz önünde bulundurarak siber güvenlik konusunu geniş çapta ele almış ve bu konularda özel olarak çalışacak bir hükümet uzmanları grubun kurulmasına fırsat tanımıştır.

BM HUG 'eşit coğrafi dağılım temelinde' oluşmaktadır. Geleneksel olarak, BM Güvenlik Konseyi'nin beş daimî üyesinin tüm HUG'larda temsil edilmekte ve kalan sandalyeler bölgesel gruplara tahsis edilmektedir. İlk üç HUG, 15 üyeden oluşurken,

[55] Alex Grigsby, 'The End of Cyber Norms' (2017) 59 (6) *Survival* 109-122.

[56] Tim Maurer, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' (2019) *Hague Journal on the Rule of Law* 1-23.

2014-2015 yıllarında görev yapan dördüncü HUG'da üye sayısı 20'ye, daha sonra ise 25'e çıkarılmıştır. Grubun üye yapının oluşumunu BM Silahsızlanma İşleri Yüksek Temsilciliği Ofisi'nin önerisi üzerine Genel Sekreter belirlemektedir. Genel Sekreter, coğrafi ve politik dengenin yanı sıra aday ülkelerin diğer HUG'larda kaç kere görev aldığı, şu anda farklı bir HUG'da hizmet verip vermedikleri, konuya gösterdikleri ilgi ve merak gibi unsurları göz önüne alınarak üye seçimine karar vermektedir.[57] Ülkeler belirlendikten sonra, devletlerden HUG'a katılmak için bir uzman tayin etmeleri istenmektedir ve bu uzmanlar genellikle devlet yetkilileri olmaktadır. İlk kurulan HUG'lara katılan enformasyon güvenliği uzmanlarının bazıları diplomatik kökenli, bazılarının ise teknik kökenli olduğu göze çarpmaktadır. Teknik kökenli uzmanlar HUG'a eşlik eden yoğun diplomatik müzakerelerde bazen geride kalabildikleri için yerlerini zamanla diplomatik kökenli uzmanlara bırakmışlardır.[58] Uzmanlara kimi zaman hukuki danışmanlar eşlik etmektedir, fakat her ülke tek bir uzman tarafından temsil edilmekte, grupta delegasyonlar yer almamaktadır. Nihai Rapordaki kararlar da dahil olmak üzere gruptaki tüm kararlar oy birliği ile alınmakta ve grubun başarısında güçlü bir başkan önemli rol oynamaktadır. Gruba, 2004-2005 ve 2009-2010 yıllarında Rusya Federasyonu, 2012-2013'de Avustralya, 2014-2015 ve 2019-2021'de Brezilya, 2016-2017'de ise Almanya başkanlık yapmıştır. BM Silahsızlanma İşleri Ofisi, siber HUG'ların Sekretaryası olarak görev yapmaktadır. HUG'ların toplantıları kapalı olarak yürütülmekte olup HUG'da temsil edilmeyen diğer devletlerden, sivil toplum kuruluşlarından, özel sektör veya uluslararası kuruluşlardan gözlemciler toplantılara katılamamaktadır.

[57] The United Nations Institute for Disarmament Research, '*Report of the International Security Cyber Issues Workshop Series*' (2016) 4

[58] ibid 5.

Tablo 1

Uluslararası Güvenlik Bağlamında Enformasyon ve Telekomünikasyon Alanındaki Gelişmelerle İlgili Hükümet Uzmanları Grupları

Dönem	Üye Sayısı	Grup Başkanı	Kurucu Karar	Toplantı Yeri ve Sayısı	Rapor	Uzlaşı
2004/2005	15	Rusya	A/RES/58/32	New York (2) Cenevre (2)	A/60/202	Yok
2009/2010	15	Rusya	A/RES/60/45	New York (2) Cenevre (2	A/65/201	Var
2012/2013	15	Avustralya	A/RES/66/24	New York (2) Cenevre (2	A/68/98	Var
2014/2015	20	Brezilya	A/RES/68/243	New York (2) Cenevre (2	A/70/174	Var
2016/2017	25	Almanya	A/RES/70/237	New York (2) Cenevre (2	A/72/327	Yok
2019-2021	25	Brezilya	A/RES/73/266	New York (2) Cenevre (2		

Birinci BM HUG (2004-2005)

2004 yılında kurulan ilk on beş üyeli çalışma grubunun görüşmelerine yukarıda söz ettiğimiz iki grubun arasında uluslararası siber güvenliğin temel unsurlarına yönelik görüş farklılıkları damgasını vurmuştur. Rusya ve ABD'nin başını çektiği iki grup ülke enformasyon içeriğine mi yoksa sadece enformasyon altyapısına mı odaklanması gerektiği konusunda anlaşmaya varamamasından dolayı, nihai bir uzlaşma raporu yayınlayamamış ancak usul meselelerine değinen kısa bir rapor yayınlamıştır.[59] Rusya, Çin, Brezilya ve Beyaz Rusya gibi devletler, devletlerin kendi enformasyon güvenliğini sağlamada sınırsız hak sahibi olduğunu, sınır ötesi enformasyon içeriğinin bir ulusal güvenlik meselesi olarak kontrol edilmesi gerektiği ve enformasyon güvenliğine yönelik yeni bir uluslararası rejimin kurulması gerektiğini savunmuşlardır.[60] ABD ve Avrupa ülkeleri ise uluslararası siber güvenliğin enformasyon içeriğine değil sadece enformasyon altyapısına uygulanması gerektiğini ve var olan uluslararası hukukun siber alana uygulanabileceğini iddia etmişlerdir.[61] Uluslararası alanda mevcut uluslararası hukukun enformasyon güvenliğine yönelik farklı yorumlarının olduğunu belirten Grup Başkanı Krutskikh, 'uluslararası topluluğun temelde yeni ve hassas problemlerle karşı karşıya kaldığı bir dizi kapsamlı meseleyi dikkate almak için çok sınırlı bir zamana' sahip olduğunu vurgulayarak grubun çalışmalarına devam etmesini önermiştir.[62] Bu öneriye rağmen, Bush başkanlığındaki ABD Yönetimi'nin 2005-2008 yılları arasında 30 devletin

[59] Report of the Secretary-General 60/202, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/60/202, New York: United Nations, 5 Ağustos 2005.

[60] Eneken Tikk-Ringas (n 54) *7*

[61] The United Nations Office for Disarmament Affairs, Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security (2015) 1; Christian Henderson, *"*The United Nations and the Regulation of Cybersecurity", *içinde* Nicholas Tsagourias ve Russell Buchan, (der.), *International Law and Cyberspace. Research Handbooks in International Law*, (Edward Elgar, 2015) 474-475.

[62] United Nations General Assembly, First Committee 13th meeting, A/C.1/60/PV.1, 17 Ekim 2005, 5

ortak sponsor olduğu Rusya'nın önergesine tek başına karşı oy kullanmasından ötürü bu dönemde anlamlı bir ilerleme kaydedilememiştir.

İkinci BM HUG (2009-2010)

İlk HUG'un uzlaşıya varamamasının ardından, Rusya'nın 'uluslararası enformasyon güvenliğinin her açıdan ele alınmasına devam edilmesi' önerisini kabul eden BM Genel Kurulu, aynı ilkeler çerçevesinde ikinci bir HUG'un 2009'da çalışmalarına başlamasına karar vermiştir.[63] Grup siber alandaki mevcut ve potansiyel tehditlerin yirmi birinci yüzyılın en ciddi zorlukları arasında olduğuna dikkat çeken ilk uzlaşı raporunu 2010'da yayınlamıştır.[64] Raporda, siber alandaki riskleri azaltmak ve kritik altyapıları korumak için uluslararası normların kabul edilmesi, güven oluşturma ve risk azaltmaya yönelik tedbirlerin geliştirilmesi ve ulusal mevzuat, politikalar ve en iyi uygulamalar hakkında enformasyon alışverişi sağlanması ve siber güvenliği artırmak için devletler, özel sektör ve sivil toplum arasındaki iş birliği ve dayanışmanın tesis edilmesi istenmiştir. Uzlaşı raporunun yayınlanmasında ABD'nin uzun zamandır devam eden muhalif pozisyonunu Obama'nın başkan seçilmesi ile tersine çevirmesi ve Rusya tarafından verilen önergeye ortak sponsor olmayı kabul etmesi önemli rol oynamıştır.[65] Obama yönetimi altında ABD, pozisyon değiştirerek uluslararası iş birliğine dayalı bir yaklaşım benimsemiş, Rusya ve Çin ile siber güvenlik konusunda ikili görüşmeler yapmaya başlamış ve nihayet Rusya'nın önergesine olumlu oy kullanarak HUG'un ilk uzlaşı raporunu yayınlamasına olanak tanımıştır.

Üçüncü BM HUG (2012-2013)

Üçüncü BM HUG grubu, Genel Kurul'un 2011 yılında kabul ettiği 66/24 sayılı kararı doğrultusunda 2012 ve 2013 yıllarında bir araya gelmiştir.[66] Grup 2013 yılında siber alan ve uluslararası hukuk arasındaki ilişkiyle ilgili olarak önceki HUG'lardan daha kapsamlı sonuçlara ulaştığı uzlaşı raporunu yayınlamıştır.[67] Rapor, uluslararası hukukun, özellikle BM Şartı'nın, siber alana uygulanabileceğini,[68] devlet egemenliği normu ve sorumluluklarının devletlerin siber alandaki faaliyetlerinde ve kendi ülkelerindeki enformasyon ve iletişim altyapısı üzerinde geçerli olduğunu kabul etmiştir.[69] Devletlerin siber alanda kasıtlı olarak yanlış eylemlerde bulunmak

63 United Nations General Assembly Resolution 60/45, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/60/45, 8 Aralık 2005.

64 Note by the Secretary-General 65/201-Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201, 30 Temmuz 2010.

65 Maurer (n 11) 23-25.

66 United Nations General Assembly Resolution 66/24, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/66/24, 2 Aralık 2011.

67 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98, 24 Haziran 2013.

68 ibid., Madde 19.

69 ibid., Madde 20.

için vekiller kullanmaması ve topraklarının devlet-dışı aktörler tarafından bu tür eylemlerde bulunmak için kullanılmamasını vurgulayarak devlet egemenliğinin haklar kadar birtakım sorumluluklar da içerdiğinin de altını çizmiştir.[70] Siber alanın güvenliğini sağlamak için yapılan çabaların, insan haklarına ve temel özgürlüklere saygı çerçevesinde yürütülmesi gerektiğini[71] ve BM'nin Üye Devletler arasında diyalogu teşvik etmede önemini vurgulamıştır.[72] Grup, siber güvenliği geliştirmek için güven artırıcı ve kapasite artırıcı önlemler konusunda bazı özel önerilerde de bulunmuştur.[73]

Dördüncü BM HUG (2014-2015)

68/243 sayılı Genel Kurul kararı ile Aralık 2013'de kurulması kararlaştırılan yirmi üyeli dördüncü HUG[74], 2014 ve 2015 yıllarında dört kez toplanmış ve Haziran 2015'te oldukça önemli bir uzlaşı raporuna imza atmışlardır.[75] Önceki raporların aksine, 2015 raporu bir yandan devletlerin egemen eşitliği, uluslararası uyuşmazlıkların barışçıl yollarla çözümlenmesi, devletlerin diğer devletlerin içişlerine müdahale etmemeleri gibi bağlayıcı uluslararası hukuk[76] ile diğer yandan gönüllü, bağlayıcı olmayan normlar[77] arasında ayrım yaparak bu ilkeleri iki ayrı bölümde değerlendirmiştir. HUG'un 2015 yılındaki uzlaşı Raporu, güvenli, istikrarlı, erişilebilir ve barışçıl küresel bir siber alanı teşvik etmek için gönüllü ve bağlayıcı olmayan sorumlu devlet davranış norm, kural ve ilkelerini on bir maddede ortaya koymuştur.[78] Bu on bir maddeden, beşi sınırlayıcı karaktere sahip normları, yedisi ise uluslararası güvenlik amacıyla iyi uygulamaları ve olumlu görevleri ifade eden ilkeleri kapsamaktadır. BM Genel Kurulu Aralık 2015'te, HUG raporunu oybirliği ile kabul etmiş ve üye devletlere siber teknolojileri kullanımlarında raporun rehberlik etmesini istemiştir. Buna göre, Raporun III. Bölümünün 13. maddesinde ifade edilen sınırlayıcı normlar şu şekildedir:

- Devletler, kendi topraklarındaki siber teknolojilerin uluslararası yanlış eylemler için kullanılmasına izin vermemelidir (Madde 13/c).
- Devletler, kritik altyapıya kasıtlı olarak zarar veren veya kritik altyapının işletilmesini engelleyen siber faaliyetler içerisine girmemeli veya desteklememelidir (Madde 13/f).

70 ibid., Madde 23.

71 ibid., Madde 21.

72 ibid., Madde 13.

73 ibid., Madde 26-33.

74 United Nations General Assembly Resolution 68/243, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/68/243, 27 Aralık 2013.

75 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 Temmuz 2015.

76 ibid, VI. Bölüm, Madde 24-29.

77 ibid, III. Bölüm.

78 ibid, III. Bölüm, Madde 13.

- Devletler, son kullanıcıların siber ürünlere olan güvenini koruyabilmek için tedarik zincirinin bütünlüğünü sağlamak konusunda makul adımlar atmalı ve kötü niyetli siber araç ve tekniklerinin çoğalmasını ve zararlı gizli işlevlerin kullanımını önlemeye çalışmalıdır (Madde 13/i).

- Devletler, başka bir Devletin yetkili acil müdahale ekiplerinin enformasyon sistemlerine zarar verecek faaliyetleri yürütmemeli veya bilerek desteklememelidir. Bir Devlet, kötü niyetli uluslararası faaliyetlerde bulunmak için yetkili acil durum müdahale ekiplerini kullanmamalıdır (Madde 13/k).

- Devletler, siber alanın güvenli bir şekilde kullanılmasını sağlarken, ifade özgürlüğü hakkı da dahil olmak üzere insan haklarına tam saygı gösterilmesini sağlamak için internette insan haklarının geliştirilmesi, korunması ve kullanılmasına ilişkin İnsan Hakları Konseyi'nin 20/8 ve 26/13 sayılı kararlarının yanı sıra dijital çağda gizlilik hakkını tanıyan 68/167 ve 69/166 sayılı Genel Kurul kararlarına uymalıdır (Madde 13/e).

Raporun yine 13. Maddesinde listelenen uluslararası siber güvenlik alanındaki iyi uygulama ve olumlu görev ilkeleri şunlardır:

- Devletler, siber teknoloji kullanımında istikrarı ve güvenliği artırmak ve zararlı olduğu kabul edilen ya da uluslararası barış ve güvenliğe tehdit oluşturabilecek siber uygulamaları önlemek için önlemler geliştirmek ve uygulamak konusunda iş birliği yapmalıdır (Madde 13/a).

- Siber olaylarda, devletler olayın daha geniş bağlamı, siber alanda isnat etme zorlukları ve sonuçların niteliği ve kapsamı da dahil olmak üzere tüm ilgili bilgileri dikkate almalıdır (Madde 13/b).

- Devletler enformasyon alışverişi, birbirlerine yardım etme, siber alanın terörizm ve suç amaçlı kullanımını kovuşturma ve bu tür diğer tehditleri ele almak için iş birliği tedbirleri geliştirmelidir (Madde 13/d).

- Devletler, küresel siber güvenlik kültürünün oluşturulması ve kritik enformasyon altyapılarının korunması ve diğer ilgili kararlar hakkında 58/199 sayılı Genel Kurul kararını dikkate alarak kritik altyapılarını siber tehditlerden korumak için uygun önlemleri almalıdır (Madde 13/g).

- Devletler, kritik altyapısı kötü niyetli siber eylemlere tabi olan başka bir devletin uygun yardım taleplerine yanıt vermelidir. Devletler ayrıca, gerekli özen prensibini dikkate alarak, kendi topraklarından başka bir devletin kritik altyapısını hedef alan kötü niyetli siber faaliyetlerini azaltmak için yapılan uygun taleplere cevap vermelidir (Madde 13/h).

- Devletler, siber güvenlik açıklarının sorumlu bir şekilde rapor edilmesini teşvik etmeli ve siber teknolojiye bağımlı altyapıya yönelik potansiyel tehditleri sınırlamak ve ortadan kaldırmak için bu tür güvenlik açıklarına ilişkin mevcut çözümlerle ilgili bilgileri paylaşmalıdır (Madde 13/j).

Rapor, "uluslararası toplumun beklentilerini yansıtan" bu normların, "sorumlu devlet davranışları için standartları belirlediğini" ve "uluslararası toplumun devletlerin faaliyetlerini ve niyetlerini değerlendirmesine izin verdiğini" ifade etmektedir.[79] Bu normlar, her ne kadar bağlayıcı olmayıp gönüllü nitelikte olsa da belirli bağlamlarda devlet aktörlerinden hangi davranışın beklendiğini belirtmesi ve devletlerin üstlenmesi gereken "olumlu" eylemleri veya kaçınmaları gereken "olumsuz" eylemleri önermesi bakımından yeteri derecede kapsayıcıdır. Genel Kurul tarafından kabul edilen on bir norm ve ilke, G7[80], G20[81], Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT)[82], ve Güneydoğu Asya Ülkeleri Birliği (ASEAN)[83] dahil olmak üzere diğer uluslararası örgütler tarafından onaylanmıştır. Paris Siber Alanda Güven ve Güvenlik Çağrısı,[84] ve Siber Alanın İstikrarına İlişkin Küresel Komisyon[85] gibi çok-paydaşlı girişimler de bu normlara atıfta bulunmakta ve desteklemektedir.

Diğer yandan, üzerinde anlaşılan bu normlar ABD'nin başarılı siber diplomasisinin bir ürünü olarak düşünülebilir. Nitekim ABD'nin barış zamanı siber alandaki devlet davranışını düzenlemeye yönelik teşvik ettiği siber terörizm ve siber suç alanlarında iş birliği, kritik altyapıların ve ulusal siber olaylara müdahale ekiplerinin korunmasına yönelik üç norm nihai raporda yer almıştır. ABD'nin bu tür gönüllü tedbirleri geliştirme stratejisi, Rusya'nın görüşüyle bir ölçüde çelişmektedir. Rusya, uluslararası toplumun bu tarz "ahlaki yükümlülükler" konusunda ortak anlaşmaya varmasını yasal olarak bağlayıcı normlar geliştirme sürecinin ilk adım olarak görmektedir.

---

79 ibid., Madde 10.

80 G7, Principles and Actions on Cyber, 2016, https://www.mofa.go.jp/files/000160279.pdf Erişim Tarihi 8 Ocak 2020

81 G20, Leaders' Communiqué Antalya summit, November 15-16 2015, http://www.g20.utoronto.ca/2015/151116-communique.html Erişim Tarihi 8 Ocak 2020

82 OSCE, Decision No. 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies, 2016, https://www.osce.org/pc/227281?download=true (Erişim Tarihi 8 Ocak 2020).

83 ASEAN, Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in ASEAN Report of the 2nd International Security Cyber Workshop Series, Singapore, September 20-21 2017, https://unidir.org/files/publications/pdfs/preserving-and-enhancing-international-cyber-stability-regional-realities-and-approaches-in-asean-en-778.pdf Erişim Tarihi 9 Ocak 2020

84 Paris Call for Trust and Security in Cyberspace, 12 November 2018. https://www.diplomatie. gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf Erişim Tarihi 9 Ocak 2020.

85 The Global Commission on the Stability of Cyberspace, Advancing Cyberstability Final Report, Kasım 2019, https://cyberstability.org/report/#6-norms Erişim Tarihi 10 Ocak 2020

Beşinci BM HUG (2016-2017)

70/237 sayılı Genel Kurul kararı ile Aralık 2015'te kurulması kararlaştırılan beşinci HUG[86], 2016 ve 2017 yıllarında bir araya gelmiş fakat Grup, uluslararası hukukun siber alana nasıl uygulanacağı ve siber egemenliğin kapsamı konularında fikir birliği sağlayamamasından ötürü nihai uzlaşı raporunu yayınlayamamıştır. Devletlerin uluslararası yanlış eylemlere tepki verme hakkı; meşru müdafaa hakkı, uluslararası insancıl hukukun siber çatışmalara nasıl uygulanacağı, devletlerin siber saldırılara yanıt vermede ne gibi seçeneklere sahip olabileceği konularında görüş ayrılıkları ortaya çıkmıştır. [87]

Siber normların yaşam döngüsünde kısa sureli bir duraksamayı işaret eden bu tıkanma, BM Genel Kurulu'nun Birinci Komitesinin 73. Oturumunda BM'nin Rusya ve ABD'nin başını çektiği iki rakip önergeyi onaylaması ile aşılmış ve siber normlara ilişkin sürdürülen müzakereler yeni bir sürece girmiştir. "Uluslararası Güvenlik Bağlamında Enformasyon ve Telekomünikasyon Alanındaki Gelişmeler" hakkında 73/27 sayılı karar[88] ve "Uluslararası Güvenlik Bağlamında Siber Alanda Sorumlu Devlet Davranışının Geliştirilmesi" konusunda 73/266 sayılı kararla[89], BM Genel Kurulu uluslararası siber güvenlik hakkında iki paralel süreç oluşturmuştur. Siber alanda mevcut ve potansiyel tehditlerin değerlendirilmesi; kapasite geliştirme, güven artırıcı önlemler; sorumlu devlet davranışları için normlar, kurallar ve ilkeler ve uluslararası hukukun siber alana uygulanması gibi konuları ele alacak olan yeni bir BM HUG'un ve tüm devletlerin katılımına izin veren Açık Uçlu Çalışma Grubunun kurulması siber normların yaşam döngüsünde yeni bir evrenin açılmasının önünü açmıştır.

Altıncı BM HUG (2019-2021)

ABD liderliğindeki 26 ülkenin dahil olduğu grubun önerisini kabul eden 73/266 sayılı Genel Kurul kararı doğrultusunda "uluslararası güvenlik bağlamında siber alanda sorumlu devlet davranışlarının geliştirilmesi" için 2019-2021 yılları arasında görev yapacak yeni bir 25- üyeli HUG Mart 2019'da kurulmuştur. Avustralya, Brezilya, Çin, Estonya, Fransa, Almanya, Hindistan, Endonezya, Japonya, Ürdün, Kazakistan, Kenya, Morityus, Meksika, Fas, Hollanda, Norveç, Romanya, Rusya Federasyonu, Singapur, Güney Afrika, İsviçre, İngiltere, Amerika Birleşik Devletleri ve Uruguay devlet temsilcilerinin oluşturduğu altıncı hükûmet uzmanları grubunun

---

[86] United Nations General Assembly Resolution 70/237, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/70/237, 23 Aralık 2015.

[87] Grigsby (n 54) 114-115; Maurer (n 56) 7-9; GIP Digital Watch, UN GGE and OEWG; Eneken Tikk and Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy' (2017), Cyber Policy Institute 16-23, https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf Erişim Tarihi 10 Aralık 2019

[88] United Nations General Assembly Resolution 73/27, Developments in the Field of Information And Telecommunications in the Context of International Security, A/RES/73/27, 5 Aralık 2018.

[89] United Nations General Assembly Resolution 73/266, Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/RES/73/266, 22 Aralık 2018.

başkanlığına Brezilya Büyükelçisi Guilherme de Aguiar Patriota seçilmiştir. İlk toplantısını Aralık 2019'da gerçekleştiren Grup, Mart ve Ağustos 2020'de tekrar bir araya gelecek ve Mayıs 2021'de son oturumunu gerçekleştirerek nihai raporunu yayınlayacaktır. Başkan, oturumlar arasında tüm BM Üye Devletleri ile gayri resmi istişareler yapacak, ayrıca Afrika Birliği, Avrupa Birliği, Amerikan Devletleri Örgütü, Avrupa Güvenlik ve İşbirliği Teşkilatı ve Güneydoğu Asya Ulusları Birliği Bölgesel Forumu gibi bölgesel kuruluşlarla da istişareler gerçekleştirecektir.[90] ABD ve müttefikleri, BM HUG'un mevcut normatif çerçevenin uygulanmasıyla ilgili daha teknik konulara bakmayı ve özellikle de uluslararası hukukun siber alana uygulanmasına yönelik devam eden sorunların ve mevcut normların uygulanmasına ilişkin sorunların çözümlenmesini tercih etmektedir.

Tablo 2

Birleşmiş Milletler Uluslararası Güvenlik Bağlamında Enformasyon ve Telekomünikasyon Alanındaki Gelişmelerle İlgili Hükümet Uzmanları Grupları Üyeleri

	2004-2005	**2009-2010**	**2012-2013**	**2014-2015**	**2016-2017**	**2019-2021**
1	Beyaz Rusya	Beyaz Rusya	Arjantin	Beyaz Rusya	Avusturalya	Avusturalya
2	Brezilya	Brezilya	Avusturalya	Çin	Botsvana	Brezilya
3	Çin	Çin	Beyaz Rusya	Kolombiya	Brezilya	Çin
4	Fransa	Estonya	Kanada	Mısır	Kanada	Estonya
5	Almanya	Fransa	Çin	Estonya	Çin	Fransa
6	Hindistan	Almanya	Mısır	Fransa	Küba	Almanya
7	Ürdün	Hindistan	Estonya	Almanya	Mısır	Hindistan
8	Malezya	İsrail	Fransa	Gana	Estonya	Endonezya
9	Mali	İtalya	Almanya	İsrail	Finlandiya	Japan
10	Meksika	Katar	Hindistan	Japonya	Fransa	Urdun
11	Kore	Kore	Endonezya	Kenya	Almanya	Kazakistan
12	Rusya	Rusya	Japonya	Malezya	Hindistan	Kenya
13	Güney Afrika	Güney Afrika	Rusya	Meksika	Endonezya	Moritus
14	Birleşik Krallık	Birleşik Krallık	Birleşik Krallık	Pakistan	Japonya	Meksika
15	ABD	ABD	ABD	Kore Cumhuriyeti	Kazakistan	Fas
16				Avrupa Birliği	Kenya	Hollanda
17				Rusya	Meksika	Norveç
18				İspanya	Hollanda	Romanya
19				Birleşik Krallık	Kore Cumhuriyeti	Rusya
20				ABD	Rusya	Singapur
21					Senegal	Güney Afrika
22					Sırbistan	İsviçre
23					İsviçre	Birleşik Krallık
24					Birleşik Krallık	ABD
25					ABD	Uruguay

[90] The UN Open-ended Working Group, 2019, https://www.un.org/disarmament/open-ended-working-group/ Erişim Tarihi 4 Ocak 2020

Birleşmiş Milletler Uluslararası Güvenlik Bağlamında Enformasyon ve Telekomünikasyon Alanındaki Gelişmelerle İlgili Açık Uçlu Çalışma Grubu (2019-2020)

Rusya'nın başını çektiği önergenin BM Genel Kurulu tarafından onaylanmasıyla "Uluslararası Güvenlik Bağlamında Enformasyon ve Telekomünikasyon Alanındaki Gelişmeler" üzerine çalışacak BM HUG'la özdeş yetki ve kaynaklara sahip bir Açık Uçlu Çalışma Grubu (AUÇG) kurulmuştur. BM AUÇG'nin farkı tüm BM üye devletlerinin katılımına açık olması ve BM himayesinde düzenli kurumsal diyalog kurma olasılığını araştırmakla görevlendirilmesidir. Toplantılarına konu ile ilgili tüm paydaşlar (iş dünyası, sivil toplum kuruluşları ve akademi) katılabilecektir. Paydaşların başvuruları BM Silahsızlanma İşleri Ofisi tarafından yönetilecek ve "itiraz yok" esasına göre yani hükümetlerin itirazları göz önüne alınmadan onaylanacaktır. İsviçre Büyükelçisi Jürg Lauber, AUÇG Başkanı olarak seçilmiştir. AUÇG'nin gündeminde mevcut ve potansiyel tehditler; uluslararası hukuk, kurallar, normlar ve ilkeler; düzenli kurumsal diyalog; güven artırıcı önlemler; ve kapasite geliştirme olmak üzere altı önemli konu vardır.[91] Bu gündem çerçevesinde AUÇG'nin raporunu oybirliğiyle kabul etmesi gerekmektedir.

AUÇG çalışmalarına 3-4 Haziran 2019'da başlayarak yaklaşık 100 üye ülkenin temsilcilerini bir araya getiren bir toplantı düzenlemiştir. 9-13 Eylül 2019'da ilk maddi oturumunu ve 2-4 Aralık 2019'da akademi sivil toplum ve özel sektör temsilcilerinin katıldığı ikinci istişare toplantısını gerçekleştirmiştir. 10-14 Şubat 2020 arası ikinci istişare toplantısı ve 6-10 Temmuz 2020 tarihinde de nihai maddi oturumunu gerçekleşmesinin ardından, 15-30 Eylül 2020 tarihinde BM Genel Kurulu'nun 75. oturumunda final raporunu sunacaktır.

AUÇG, tüm üye devletlerin ilk kez BM'de uluslararası güvenlik ve siber teknolojiler ile ilgili önemli tartışmalara girmeleri için tarihi bir fırsat sunmaktadır. Eylül 2019'daki AUÇG'nin ilk oturumuna 117 delegasyonun katılması ve 70'ten fazlasının söz alması, AUÇG'nin çalışmalarına olan ilgi ve katılımın yüksekliğine ve devam eden diyalog ihtiyacının önemine işaret etmektedir. Daha geniş devlet katılımının yanı sıra özel sektör ve sivil toplum gibi devlet-dışı temsilcilerin katılımına izin veren ve daha şeffaf bir yapıya sahip olan AUÇG, sorumlu devlet davranışı normlarını ve güven arttırıcı önemlerin benimsenmesi için çok taraflı anlaşmalar yapma potansiyeline sahiptir. Nitekim ABD'nin de içinde olduğu 27 devlet[92], Eylül 2019'da BM Genel Kurulu'nda devletlerin siber alanda nasıl davranması gerektiği konusunda fikir birliğini yeniden teyit eden "Siber Alanda Sorumlu Devlet Davranışını Geliştirmek

[91] A/RES/73/27, Para.5.

[92] Bildiriye imzalayan devletler şunlardır: Avustralya, Belçika, Kanada, Kolombiya, Çek Cumhuriyeti, Danimarka, Estonya, Finlandiya, Fransa, Almanya, Macaristan, İzlanda, İtalya, Japonya, Letonya, Litvanya, Hollanda, Yeni Zelanda, Norveç, Polonya, Kore Cumhuriyeti, Romanya, Slovakya, İspanya, İsveç, İngiltere ve ABD.

için Ortak Bir Bildiri" yayınlamıştır.[93] Devlet ve devlet-dışı aktörlerin, siber alanı giderek kritik altyapıyı ve sivilleri hedefleyen, demokrasileri, uluslararası kurum ve kuruluşları ve küresel ekonomideki adil rekabeti zayıflatan bir platform olarak kullandıklarının altını çizen açıklama, gelecek nesillere ücretsiz, açık ve güvenli bir siber alan bırakabilmek için tüm sorumluluk sahibi devletleri gelişmekte olan uluslararası çerçeveyi desteklemeye ve bu çerçeveye aykırı hareket eden devletlerin hesap verebilmelerini sağlamak için birlikte çalışmaya davet etmiştir.

AUÇG nihai raporunda, siber alanda sorumlu devlet davranışı normlarının uygulamada ne anlama geldiğini ve devletler ve bölgesel kuruluşlar tarafından bu normların nasıl uygulanabileceği konusunda somut tavsiyeler üreterek bu normların daha geniş kitlelere yayılmasında kritik bir rol oynama potansiyeline sahiptir. Önceki HUG raporları ve AUÇG kurucu kararı, siber normları kabul etmiş olsa da bunların somut devlet eylemine nasıl dönüştürülebileceği konusunda sınırlı rehberlik sağlamaktadır. Bu nedenle AUÇG'nin üzerinde anlaşmaya varılmış normları yaymak ve uygulamak için pratik önlemler önermesi gerekmektedir. Örneğin, enformasyon güvenliği/siber güvenlik ve kritik altyapı gibi anahtar kavramların devletler tarafından farklı tanımlanması ve anlaşılması ve devletlerin bu normların varlığı konusunda farklı farkındalık düzeyleri ve farklı uygulayabilme kapasiteleri söz konusu normların uygulanmasında zorluklar yaratmaktadır. Farklı farkındalık ve kapasite düzeylerinden kaynaklanan bu zorluklar, devletler ve diğer uluslararası aktörlerin normlara uyumunu izlemek ve raporlamak için açık kurumsal mekanizma veya süreçlerin olmaması yüzünden daha da artmaktadır.

Normların etkili olabilmesi için yaygın olarak bilinmesi ve uygulanması gerekir ki eğer AUÇG, bu normların uygulanmasına yönelik birtakım kurumsal adımlar atmazsa, bu normlar tüm üye devletler tarafından onaylanmış olsa bile, küresel siber alanda istikrarı ve güvenliği artırmak için ortak anlayışları güçlendirme hedefine ulaşmada etkisiz kalacaktır. Normların uygulanabilmesinin bir yolu, ulusal siber güvenlik strateji belgeleri ve/veya Avrupa Birliği, AGİT ve ASEAN gibi bölgesel örgütlerin çerçeve belgelerinin devletlerin rapor verdiği uluslararası bir süreç ya da mekanizma aracılığıyla izlenmesidir. Küresel Siber Uzmanlık Forumu ve İnternet Yönetişim Forumu'nun En İyi Uygulama Forumu gibi bazı çok-paydaşlı girişimler, norm uygulaması konusundaki bu eksikliği gidermeye çalışmış ve bunların uygulanmasını değerlendirmek için araştırmalar yürütmüş olsa da kurumsal bir mekanizmanın yokluğunda norm uygulama durumunun tespit edilmesi zor ve düzensizdir.[94] Dolayısı ile normların uygulanabilirliğine geçilmesi için BM'de devam eden süreçlerin böyle bir mekanizma kurulmasına odaklanması gerekmektedir.

---

[93] Joint Statement on Advancing Responsible State Behavior in Cyberspace, 23 Eylül 2019, https://nz.usembassy.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/ Erişim Tarihi 5 Ocak 2020.

[94] Anriette Esterhuysen, Deborah Brown and Sheetal Kumar, '*Unpacking the GGE's Framework on Responsible State Behaviour: Cyber Norms'* (Association for Progressive Communications and Global Partners Digital, 2019) 2.

Uluslararası bir kurumsal mekanizmanın hayata geçirilmesi saldırgan siber operasyonların belirli bir devlete isnat edilmesi konusunda da oldukça önem taşımaktadır. Siber saldırıların kaynağının belirlenmesi teknik, yasal ve siyasi boyutlar içerdiğinden siber alan hukukunun en karmaşık ikilemlerden birini oluşturmaktadır. Bir devletin uluslararası haksız bir fiilden sorumlu tutulabilmesi veya saldırıya uğrayan devletin meşru müdafaa hakkını kullanabilmesi, ancak saldırının o devlete isnat edilebilmesi ile mümkündür. Fakat, siber alanın bazı karakteristik özellikleri, siber eylemlerin bir devlete isnat edilebilirliğini oldukça güç kılmaktadır. Siber operasyonların anonim olarak farklı ülkelerden, farklı bilgisayarlar kullanılarak gerçekleşmesi eylemlerin arkasındaki esas gücün tespitini oldukça zorlaştırmaktadır. Hem HUG raporu[95] hem de AUÇG'yi kuran karar[96], saldırının kökeninin gösterilmesinin isnat etme için yeterli olmadığını ve bu suçlamaların kanıtlanması gerektiğini işaret etmektedir. Fakat bu konu ana aktörler arasında tartışma konusu olmaya devam etmektedir. ABD ve müttefikleri şüphelilerin ortak bir kamuoyu açıklaması ile açık olarak ilişkilendirilmesi ve "utandırılması" gerektiğine inanmaktadır. Rusya ve müttefikleri ise böyle bir yaklaşımı, bir grup ülkenin üçüncü bir ülkeyi açık delil olmadan suçladığı sözde-yasal bir kavram olarak görmekte ve kanıta dayalı isnat etmeyi savunarak ret etmektedir.[97] Dolayısı ile siber saldırıların kaynağının nasıl isnat edileceğine yönelik tartışmalar önümüzdeki yıllarda HUG ve AUÇG'nin gündemini meşgul edecek gibi görünmektedir. Her ne kadar BM Genel Sekreteri siber alanda "hesap verebilirlik kültürünü teşvik etmeyi" savunsa da siber operasyonların kaynağını araştıracak tarafsız bir mekanizmanın yokluğunda devletleri hesap verilebilir kılmak oldukça zor olacaktır.

Sonuç

Siber alan giderek artan şekilde oldukça sofistike ve geniş boyutta ve çoğu zaman devlet-desteği ile yürütülen siber operasyonlara maruz kalmaktadır. Burada gündeme gelen önemli bir soru, saldırgan siber yeteneklerde bu artışı sağlayan temel güç rekabetlerinin siber alanda çatışmayı önlemek için yürütülen diplomatik çabalara nasıl etki edeceğidir. Geçtiğimiz son on yılda, birçok devlet ulusal siber kabiliyetlerini geliştirmeye başlamış, siber güvenlik stratejilerini tanımlamış ve askeri yapıları içinde siber alanda savaşabilecek siber savunma komutanlıkları tesis etmeye başlamışlardır. Siber diplomasi ve uluslararası hukukun siber alana uygulanması her ne kadar siber alanın militerleşmesini geriden takip etse de son on yılda, uluslararası toplum, siber alanda "uluslararası kurallara dayalı düzen" inşa edebilmek adına, uluslararası hukukun siber alanda geçerliliği, barış zamanlarında devletlerin sorumlu devlet

[95] A/70/174, Madde 28f.

[96] A/RES/73/27, Madde 1.2.

[97] Geneva Internet Platform Digital Watch, How Should Attribution of Cyber Attacks be Conducted, 2019, https://dig.watch/processes/un-gge Erişim Tarihi 10 Aralık 2019

davranışı normlarını benimsemesi, siber çatışmaları azaltmanın bir yolu olarak güven artırıcı önlemlerin geliştirilmesi ve devletlerin kendilerini yıkıcı veya dengesizleştirici siber faaliyetlerden daha iyi koruyabilmelerini sağlamak için kapasite geliştirilmesi gibi dört unsurdan oluşan uluslararası bir çerçeve üzerinde antlaşmaya varmıştır. BM Genel Kurulunun tüm üyeleri, 2010, 2013 ve 2015 yıllarında birbirini izleyen üç BM Devlet Uzmanları raporunda yer alan bu çerçeveyi defalarca teyit etmiştir. BM HUG'nin 2015 yılında da herkes için 'açık, güvenli, istikrarlı, erişilebilir ve barışçıl bir siber alan sağlayabilmek için tavsiye ettiği normlar birçok çok- taraflı ve çok-paydaşlı uluslararası ve bölgesel platformlar tarafından desteklenmiştir.

Her ne kadar uluslararası hukukun siber alana nasıl uygulanacağı ve siber egemenliğin kapsamı yönündeki görüş ayrılıkları, HUG'un 2017'deki son toplantısında konsensüse ulaşmasını engelleyerek, siber normların yaşam döngüsünde kısa bir duraksamayı işaret etse de BM'nin 2018'de Rusya ve ABD'nin başını çektiği iki rakip önergeyi onaylaması ile yeni bir sürece girmiştir. Tüm devletlerin ve paydaşların katılımına izin veren AUÇG, siber alanda sorumlu devlet davranışı normlarının uygulamada ne ifade ettiği ve nasıl uygulanabileceği konusunda somut tavsiyeler üreterek bu normların daha geniş kitlelere yayılmasında kritik bir rol oynama potansiyeline sahiptir. Nitekim AUÇG bünyesinde yürütülen diplomatik müzakereler siber alanda hangi davranışların uygun olarak kabul edildiği konusunda devletler-arası bir anlaşmanın ortaya çıkmasına katkıda bulunabilir. Daha önce de belirtildiği gibi devletlerin normlara uyumu söz konusu olduğunda normların ortak tanınırlığı resmi geçerlilikten daha çok önem taşımaktadır. Normların etkinliğinin söz konusu normların nasıl ve nerede kabul edildiğine hangi aktörlerin nerede ve ne sıklıkla uluslararası etkileşimlere girdiğine bağlı olarak değiştiği göz önüne alındığında geniş çok-paydaşlı yapısı ile AUÇG bu normların sosyal tanınırlığının ve meşruiyetinin artmasına sebep olarak etkinliklerini arttırma potansiyeline sahip olduğu söylenebilir. Literatür, normların kabulünün, aktörlerin söz konusu normların sosyal olarak yapılandırılmış anlamlarını inşa etme sürecinin parçası olmalarına bağlı olduğunu ortaya koymaktadır. Dolayısı ile AUÇG'da sürdürülen müzakereler daha fazla sayıda devletin siber normların kavramsallaştırılması ve nasıl uygulanacağı konusunda katılımına izin vererek sürecin parçası olmalarını sağlayacaktır. Yalnızca devletlerin bu normların çıkarlarına olduğuna dair bir inanç, onları normları uygulamak, deneyimlerini paylaşmak ve birbirlerini sorumlu tutmak için gerekli kaynakları tahsis etmeye itecektir.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Peer-review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.

Bibliyografya/Bibliography

Acharya A, 'How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism' (2004) 58 (2) *International Organization* 239–75.

ASEAN, 'Preserving and Enhancing International Cyber Stability: Regional Realities and Approaches in *ASEAN Report of the 2nd International Security Cyber Workshop Series'*, (2017) September 20-21 2017, < https://unidir.org/files/publications/pdfs/preserving-and-enhancing-international-cyber-stability-regional-realities-and-approaches-in-asean-en-778.pdf > Erişim Tarihi 9 Ocak 2020

Chesney R ve Citron D, 'Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics' (January / February 2019) *Foreign Affairs* 147–155.

Choucri N ve Clark D D, 'Who Controls Cyberspace?' (2013) 69 (5) *Bulletin of the Atomic Scientists* 21–31.

Choucri N ve Clark D D, *International Relations in the Cyber Age: The Co-Evolution Dilemma (*The MIT Press, 2019).

Clark D 'Characterizing Cyberspace: Past, Present and Future' (2010) *MIT/CSAIL Working Paper*, < https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf >

Çelik Ş, 'Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme' (2013) 15 (1) *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 137-175.

Darıcılı A B, 'Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi', (2017) 1 (1) *Ulisa: Uluslararası Çalışmalar Dergisi*, 1-24.

Deibert R J ve Crete-Nishihata M, 'Global Governance and the Spread of Cyberspace Controls' (2012) 18 *Global Governance* 339-361.

Deibert R J ve Rohozinski R, 'Risking Security: Policies and Paradoxes of Cyberspace Security' (2010) 4 (1) *International Political Sociology* 15–32.

Deibert R J, Rohoinski R ve Crete-Nishihata M, 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War' (2012) 43 (1) *Security Dialogue* 3–24.

Deibert R, The Geopolitics of Cyberspace after Snowden (2015) 114 (768) *Current History* 9-15.

Dutton W H ve Peltu M, 'The Emerging Internet Governance Mosaic: Connecting the Pieces' (2017) 12 *Information Polity* 63–81.

Duygulu Ş, *Dönüşen Savaşların Değişen Araçları* (SETA, 2019).

Ebert H ve Maurer T 'Contested Cyberspace and Rising Powers' (2013) *34 (6) Third World Quarterly* 1054–1074.

Eneken Tikk and Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy' (2017), Cyber Policy Institute 16-23, < https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf > Erişim Tarihi 10 Aralık 2019

Esterhuysen A, Brown D ve Kumar S, 'Unpacking the GGE's Framework on Responsible State Behaviour: Cyber Norms' (2009) Association for Progressive Communications and Global Partners Digital, < https://www.apc.org/sites/default/files/UnpackingGGGCyberNorms.pdf > Erişim Tarihi 18 Ocak 2020

Farwell J P ve Rohozinski R, 'Stuxnet and the Future of Cyber War' (2011) 53 (1) *Survival* 23-40, DOI: 10.1080/00396338.2011.555586

Feick J ve Werle R, 'Regulation of Cyberspace' icinde Robert Baldwin, Martin Cave, ve Martin Lodge (der.), *The Oxford Handbook of Regulation* (Oxford University Press, 2010) 523-547.

Ferrara E, Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election (2017) 22 (8) *First Monday*, https://doi.org/10.5210/fm.v22i8.8005

Finnemore M ve Hollis D B, 'Constructing Norms for Global Cybersecurity' (2016) 110 (3) *The American Journal of International Law* 425- 479.

Finnemore M ve Sikkink K, 'International Norm Dynamics and Political Change' (1998) 52 (4) International *Organization* 894-905.

Finnemore M ve Toope S J, 'Alternatives to "Legalization": Richer Views of Law and Politics' (2001) 55 (3) International *Organization* 743-758.

Flonk D, 'Content Control Contestations: Russia and China as Entrepreneurs of Illiberal Internet Norms' (2019) *Paper for the Authoritarian Politics and International Relations Workshop in Berlin, January.*

G20, 'Leaders' Communiqué Antalya Summit' (2015) November 15-16 < http://www.g20.utoronto.ca/2015/151116-communique.html > Erişim Tarihi 8 Ocak 2020

G7, 'Principles and Actions on Cyber' (2016) < https://www.mofa.go.jp/files/000160279.pdf > Erişim Tarihi 8 Ocak 2020

*Geneva Internet Platform (GIP) Digital Watch, '*UN GGE and OEWG' (2019) < https://dig.watch/processes/un-gge > Erişim Tarihi 3 Ocak 2020

Gibson W, *Neuromancer (*Ace Science Fiction Books, 1984).

Grigsby A, 'The End of Cyber Norms' 2017 59 (6) *Survival* 109-122, DOI: 10.1080/00396338.2017.1399730

Güntay V, 'Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği' (2017) 6 (2) *Güvenlik Bilimleri Dergisi* 81-108.

Hathaway M E ve Klimburg A, 'Preliminary Considerations: On National Cyber Security' , içinde: A Klimburg (der) *National Cyber Security Framework Manual*, (NATO CCD COE Publication, 2012) 1-43.

Henderson C, '*The United Nations and the Regulation of Cybersecurity', 'çinde* Nicholas Tsagourias ve Russell Buchan, (der.), *International Law and Cyberspace. Research Handbooks in International Law*, (Edward Elgar, 2015) 474-475.

Herzog S, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses' (2011) 4 (2) *Journal of Strategic Security* 49-60.

Howard P N ve Kollany B, 'Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum' (2016) *ArXiv, abs/1606.06356*, < https://arxiv.org/abs/1606.06356>

Inkster N, 'Information Warfare and the US Presidential Election' (2016) 58 (5) *Survival* 23-32, DOI: 10.1080/00396338.2016.1231527

Jenkins R, 'Is Stuxnet Physical? Does It Matter?' (2013) 12 (1) *Journal of Military Ethics* 68-79, DOI: 10.1080/15027570.2013.782640

Joint Statement on Advancing Responsible State Behavior in Cyberspace, (2019) 23 Eylül 2, < https://nz.usembassy.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/ > Erişim Tarihi 5 Ocak 2020

Korzak E, 'The Quest for Cyber Norms' (2016) 72 (5) *Bulletin of the Atomic Scientists* 348-350 DOI: 10.1080/00963402.2016.1216683

Lindsay J R, 'Stuxnet and the Limits of Cyber Warfare' (2013) 22 (3) *Security Studies* 365-404, DOI: 10.1080/09636412.2013.816122

Maurer T, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' (2019) Hague Journal on the Rule of Law 1-23.

Maurer T, 'Cyber Norm Emergence at the United Nations, – An Analysis of the UN's Activities Regarding Cyber-security' (2011) *Belfer Center Discussion Paper* #2011-11, < https://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf >

McCombie S, Uhlmann A J ve Morrison S, 'The US 2016 Presidential Election & Russia's Troll Farms' (2020) 35 (1) *Intelligence and National Security* 95-114, DOI: 10.1080/02684527.2019.1673940

Mueller M L, *Networks and States: The Global Politics of Internet Governance* (MIT Press, 2010).

NATO, 'Warsaw Summit Communiqué: Issued by the Head of States and Governments participating in the meeting of the North Atlantic Council in Warsaw on 8-9 July 2016, < https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en > Erişim Tarihi 5 Ocak 2020.

NATO CCDCOE UN GGE Report, 'Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law' (2015) 31 Ağustos, < https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/ > Erişim Tarihi 3 Ocak 2020

Nocetti J, 'Contest and Conquest: Russia and Global Internet Governance' (2015) 91 *International Affairs* 111-130, doi:10.1111/1468-2346.12189

Nye J S, 'The Regime Complex for Managing Global Cyber Activities' (2014). *Global Commission on Internet Governance Paper Series* < https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities > Erişim Tarihi 3 Kasım 2019

OSCE Decision No. 1202, 'OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies' (2016) < https://www.osce.org/pc/227281?download=true > Erişim Tarihi 8 Ocak 2020.

Pakharenko G, 'Cyber Operations at Maidan: A First-Hand Account' içinde K. Geers (der) *Cyber War in Perspective: Russian Aggression against Ukraine*, (NATO CCD COE Publications, 2015) 59-66 < https://ccdceo.org/uploads/2018/10/Ch07_CyberWarinPerspective_Pakharenko.pdf >

Paris Call for Trust and Security in Cyberspace (2018) 12 November < https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf > Erişim Tarihi 9 Ocak 2020

Risse T, Ropp S C ve Sikkink K(der.) *The Power of Human Rights: International Norms and Domestic Change (*Cambridge University Press, 1999).

Russian Federation, '*Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*' (2012), < https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle > Erişim Tarihi 20 Kasım 2019

Russian Federation, '*Information Security Doctrine of the Russian Federation*' (2000) < https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf > Erişim Tarihi 20 Kasım 2019.

Safshekan O, 'Iran and the Global Politics of Internet Governance' (2017) 2 (2) *Journal of Cyber Policy* 266-284 DOI: 10.1080/23738871.2017.1360375

Sander B, 'Democracy under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections' (2019) 18 (1) *Chinese Journal of International Law* 1–56.

Schmitt M N, *Tallinn Manual on the International Law Applicable to Cyber Warfare.* (Cambridge University Press, 2013).

Shanghai Cooperation Organization, '*Agreement on Cooperation in the Field of International Information Security' (2009)* 16 Haziran < https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/SCO-090616-IISAgreement.pdf > Erişim Tarihi 15 Ocak 2020.

Sullivan J E ve Kamensky D. 'How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid' (2017) 30 (3) *The Electricity Journal* 30-35, https://doi.org/10.1016/j.tej.2017.02.006.

Sunstein C R, 'Social Norms and Social Roles' (1996) 96 (4) *Columbia Law Review* 903-968.

The Global Commission on the Stability of Cyberspace, '*Advancing Cyberstability Final Report'* (2019) Kasım < https://cyberstability.org/report/#6-norms > Erişim Tarihi 10 Ocak 2020.

The Global Commission on the Stability of Cyberspace, '*Norm Package Singapore',* (2018) Kasım < https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf > Erişim Tarihi 5 Ocak 2020

Tikk-Ringas E, 'Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012' (*ICT4Peace* Publishing, 2012) < https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf > Erişim Tarihi 3 Ocak 2020

Türkay, S 'Siber Savaş Hukuku ve Uygulanma Sorunsalı' (2013) 71 (1) *Journal of Istanbul University Law Faculty* 1177-1227.

U. N. General Assembly Report of the Secretary-General 60/202 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (5 August 2005), A/60/202, < https://undocs.org/en/A/60/202>

U.N. General Assembly First Committee 13th meeting Sixtieth session (17 October 2005), A/C.1/60/PV.13

U.N. General Assembly Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, < https://digitallibrary.un.org/record/710973>

U.N. General Assembly Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/273, < http://www.un.org/Docs/journal/asp/ws.asp?m=A/69/723 >

U.N. General Assembly Note by the Secretary-General 65/201, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (30 July 2010), A/65/201 < https://www.unidir.org/files/medias/pdfs/information-security-2010-doc-2-a-65-201-eng-0-582.pdf >

U.N. General Assembly Report of the First Committee, Developments in the Field Of Information and Telecommunications in The Context Of International Security, (13 November 2013), A/68/406 < https://undocs.org/A/68/406 >

U.N. General Assembly Report of the Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security (10 August 1999), A/54/213 < https://undocs.org/A/54/213>

U.N. General Assembly Resolution 53/70-Developments in the Field of Information and Telecommunications in the Context of International Security, (4 January 1999), A/RES/53/70 < https://undocs.org/A/RES/53/70 >

U.N. General Assembly Resolution 56/19, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/56/19, < https://undocs.org/A/RES/56/19 >

U.N. General Assembly Resolution 58/32, Developments In The Field Of Information And Telecommunications In The Context Of International Security, (8 December 2003), A/RES/58/32, < https://undocs.org/A/RES/58/32 >

U.N. General Assembly Resolution 60/45 "Developments in the Field of Information and Telecommunications in the Context of International Security" [on the report of the First Committee (A/60/452)], (8 December 2005), A/RES/60/45, < https://undocs.org/A/RES/60/45 >

U.N. General Assembly Resolution 66/24 (2 December 2011), A/RES/66/24 < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/460/26/PDF/N1146026.pdf?OpenElement >

U.N. General Assembly Resolution 68/243 [*On the Report of the First Committee (A/68/406)*], (27 December 2013) , A/RES/68/243 , < https://undocs.org/A/RES/68/243 >

U.N. General Assembly Resolution 70/237 [on the report of the First Committee (A/70/455)] 30 December 2015, A/RES/70/237

U.N. General Assembly Resolution 73/266 [on the report of the First Committee (A/73/505)] Advancing responsible State Behavior in Cyberspace in the Context of International Security, (2 January 2019), A/RES/73/266, < https://undocs.org/A/RES/73/266 >

U.N. General Assembly Resolution 73/27. [on the Report of the First Committee (A/73/505)] Developments in the Field of Information And Telecommunications In The Context Of International Security, (11 December 2018), A/RES/73/27 , < https://undocs.org/A/RES/73/27 >

U.N. General Assembly Revised Draft Resolution, Russian Federation, A/C.1/53/L.17/Rev.1, 2 Kasım 1998, < https://digitallibrary.un.org/record/263069 >

U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (24 June 2013), A/68/98, < https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf >

U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, (22 July 2015), A/70/174, < https://undocs.org/A/70/174 >

U.N. Institute for Disarmament Research, Report of the International Security Cyber Issues Workshop Series (2016) < *https://unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf* > Erişim Tarihi 3 Ocak 2020

U.N. Office for Disarmament Affairs, Fact Sheet: Developments in the Field of Information and Telecommunications in the Context of International Security (2015) < https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf >

U.N. Open-Ended Working Group (2019) < https://www.un.org/disarmament/open-ended-working-group/ > Erisim Tarihi 4 Ocak 2020

United Kingdom National Security Strategy 2016-2021 < https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 >

United Kingdom Parliament Digital, Culture, Media and Sport Committee, Disinformation and 'Fake News': Final Report, Eighth Report of Session 2017–19, HC 1791, (House of Commons, 2019) < https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf >

United States Government, *US Army Joint Publication JP 3-12 Cyberspace Operations,* (CreateSpace Independent Publishing Platform, June 2018) < https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf >

United States International Strategy for Cyberspace (2011) < https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf >

United States National Security Council, *Cyberspace Policy Review: Securing America's Digital Future*, (Cosimo Incorporated, 2010).

United States National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23),2008, < https://fas.org/irp/offdocs/nspd/nspd-54.pdf >

Unwala A ve Ghori S, 'Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict' (2015) 1 (1) *Military Cyber Affairs* DOI: http://dx.doi.org/10.5038/2378-0789.1.1.1001

Uren T, Hogeveen, B ve Hanson F, 'Defining Offensive Cyber Capabilities' (2018) *Australian Strategic Policy Institute*, < https://www.aspi.org.au/report/defining-offensive-cyber-capabilities > Erişim Tarihi: 17 Subat 2020

Wiener A ve Puetter U, 'The Quality of Norms is What Actors Make of It' (2009) 5 (1) *Journal of International Law and International Relations* 1-16.

Yayla M, '*Hukuki Bir Terim Olarak —Siber Savaş' (2013) 104* TBB Dergisi 177-202.