IJPS, 2024: 6(2):184-201
International Journal of Politics and Security, 2024: 6(2):184-201

Uluslararası Hukukun Zorlu Sınavı: Siber Uzay ve Uluslararası Hukuk Arasındaki İlişki

Erdi Şafak[1]

Özet

Siber uzayın günümüzde sosyal, ekonomik, politik ve askeri açıdan artan önemi, devletlerin bu alana yönelik düzenlemeler yapmasını zorunlu kılmaktadır. Ancak siber uzayın yapısı düşünüldüğünde devletlerin bu alana yönelik düzenlemelerin yapılması ile ilgili tutumları konusunda ciddi farklılıklar mevcuttur. Daha da önemlisi birçok devlet bu alan ile ilgili düzenleme yapmak konusunda adım atmamaktadır. Bu çalışma, betimleyici ve normatif bir bakış açısıyla, devletlerin siber uzayda ulusal yasalar yerine uluslararası hukuk kuralları çerçevesinde bazı düzenlemelerin yapılması konusunda nasıl davrandıklarına dair başlangıç niteliğinde bir değerlendirme sunmaktadır. Çalışmada ayrıca, siber uzayın kurallarının belirlenmesindeki zorluğuna rağmen devletlerin bu alan ile ilgili düzenlemeler konusunda adım atmamasının uluslararası hukuk açısından önemi ele alınacaktır. Son olarak siber uzay ile ilgili uluslararası hukuk kurallarını inşa etmek için devletlerin kapasiteleri ve kısıtlamaları hakkında bir tartışma oluşturulmaya çalışılmıştır.

Anahtar Kelimeler: *Uluslararası Hukuk, Siber Uzay, Birlemiş Milletler, Uluslararası Aktörler*

The Difficult Exam of International Law: The Relationship Between Cyberspace and International Law

Abstract

The increasing importance of cyberspace in today's social, economic, political, and military terms necessitates states to regulate this area. However, when considering the structure of cyberspace, there are serious differences in the attitudes of states regarding the regulation of this area. More importantly, many states do not take steps to regulate this area. This study provides an initial assessment of how states act regarding the regulation of some regulations in cyberspace within the framework of international law rules instead of national laws, from a descriptive and normative perspective. The study will also address the importance of states' failure to take steps regarding the regulation of this area, despite the difficulty of determining the rules of cyberspace, in terms of international law. Finally, an attempt is made to create a discussion on the capacities and limitations of states to establish international law rules regarding cyberspace

Keywords: *International Law, Cyberspace, United Nations, International Actors*

[1] Doç.Dr. Yakın Doğu Üniversitesi, erdi.safak@neu.edu.tr, Lefkoşa, Kuzey Kıbrıs Türk Cumhuriyeti,, ORCID ID: 0000-0003-4000-2468, Makale Geliş Tarihi: 09.08.2024, Makale Kabul Tarihi: 07.10.2024

1. Giriş

Günümüzde teknolojinin gelişmesine paralel olarak "siber uzay" olarak ifade edilen ortam daha fazla önem kazanmış ve internete giderek daha fazla bağımlı hale gelen insanlığın yaşamı, alışkanlıkları ve hatta politik durumları siber uzayın etkisi altına girmiştir. Siber uzay en genel tanımıyla dijital ağlar, internet ve bilgisayar sistemleri aracılığıyla etkileşimlerin gerçekleştiği somut olmayan alan olarak tanımlanabilir. E-posta göndermek, alışveriş yapmak, web sitelerini ziyaret etmek ve sosyal medyayı kullanmak da dahil olmak üzere bu alandaki tüm dijital etkileşimler siber uzayın birer parçasını oluşturmaktadır.

Siber uzayın potansiyel riskleri ve getirileri konusunda yeteri kadar bilgisi olmayan veya siber uzaya ilgisiz olan devletlerin sayısı günümüzde giderek azalmaktadır. Ancak yine de bu alan ile ilgili çalışmalar henüz istenilen seviyede değildir. Gerek ulusal hukuk gerekse uluslararası hukuk bağlamında bazı devletler siber uzay ile ilgili düzenlemeler yapma amacıyla adım atma konusunda isteksiz davrandıkları görülmektedir. Başka bir deyişle, bu durum siber uzay ile ilgili düzenlemeler konusunda bazı devletlerin isteksiz kaldığı şeklinde yorumlanmaktadır. Bu durum, günümüzde devletlerin siber uzayda ve siber uzaya ilişkin sözlü ve fiziksel eylemlerinin yaygınlığıyla tezat oluşturmaktadır. Siber uzayın yapısı her ne kadar bu alana ilişkin kuralların belirlenmesini zorlaştırıyor olsa da Amerika Birleşik Devletleri (ABD) gibi bazı devletlerin siber uzay ile ilgili uluslararası hukuk kurallarının siber uzaya nasıl uygulanacağına ilişkin tek taraflı açıklamaları konuya öncülük etmektedir. Ancak yine de konu ile ilgili çalışmalarda devletler arasında yaşanan uyuşmazlıkların nedeni uluslararası hukuk açısından sorgulanması gereken bir konudur. Zira devlet destekli siber operasyonların sayısının giderek artması karşısında devletlerin siber uzay uluslararası hukuk kurallarının belirlenmesi ile ilgili yaşanan uyuşmazlıklar, uluslararası hukuka göre tepki verilmesini gerektiren koşulları oluşturmayı önemli kılmaktadır.

Bu çalışmada siber uzay kurallarının belirlenmesinde devletlerin konuya yeterli ilgiyi göstermemesi ve siber uzay ile ilgili uluslararası hukukun söyleyecek çok az şeyi olmasına rağmen, bu konuda yaşanan uyuşmazlıkların hukuki açıdan önem kazanıp kazanmayacağı ele alınmıştır. Son olarak siber uzayın ilgili yasal kuralları hakkında açıklık, ilgili devlet

davranışları hakkında şeffaflık, siber uzayda gerçekleşen eylemlerle ilgili iddiaları veya davranışları anlama becerisi ve değişen koşulların hızla değişmesine duyarlılık gibi çözmesi gereken önemli konular da incelenecektir.

2. Siber Uzay Tanımı

Siber uzay, elektronik verileri depolamak ve kullanmak için çeşitli ağlar üzerindeki elektronik ve iletişim cihazlarından oluşan sanal ve dinamik bir ortam olarak tanımlanmaktadır[2]. Siber uzayın yapısı insan beyninin yapısına benzemektedir. Bir insan beyni, sinyal göndermek için kullanılan milyonlarca nörondan oluşmaktadır. Aynı şekilde siber uzay da iletişim kurmak için çok sayıda ağ bağlantısından oluşur. Siber uzayın var olmasının temel amacı bilgi paylaşımı ve dünya çapında iletişim kurmaktır. Ancak artık siber uzay başlangıçtaki amacının ötesinde hizmet vermekte ve günlük yaşamımızda önemli bir rol oynamaktadır. Siber uzay ağ cihazları, kişisel bilgisayarları ve sunucuları, süper bilgisayarları, sensörleri ve dönüştürücüleri vb. içermektedir.[3]

Genel anlamda, çoğu uygulayıcı siber uzayın çalışma konseptini elektronik bilgilerin depolandığı, kullanıldığı ve iletişimin gerçekleştiği ağlarla birbirine bağlanan bilgi işlem cihazlarının toplamı olarak tanımlamaktadır.[4] Siber uzayın doğasını anlamanın bir başka yolu da onun amacını ifade etmektir. Bu amaç, bilginin işlenmesi, kullanılması, insanlar arasındaki iletişimin kolaylaştırılması, arttırılması ve insanlar ile bilgi arasındaki etkileşim olarak tanımlanabilir. Hem bilgi hem de insanlar siber uzayın gücünün merkezinde yer almaktadır.[5]

Siber uzayın fiziksel katmanı, siber uzayın, yani onun inşa edildiği fiziksel aygıtların temelidir. Siber uzay, birbirine bağlı bilgi işlem aygıtlarından oluşan bir alan olarak da tanımlanabilir.[6] Siber uzayın temelleri, bilgisayarlar - sunucular, internet ve diğer türdeki ağlar ile iletişim kanallarıdır. İletişim, kablolar veya fiberler üzerinden, radyo iletimi yoluyla veya bilgi işlem ve depolama cihazlarının bir yerden bir yere fiziksel olarak taşınması yoluyla

[2] David Clark, Characterizing, Cyberspace: Past, Present and Future (MIT, CSAIL, 2010), 2-6.
[3] Duncan B. Hollis ve Barrie Sander, International Law and Cyberspace: What Does State Silence Say? (Temple University Beasley School of Law Legal Studies Research Paper No. 2022-22), 1-3.
[4] Jonathan Zittrain, The Future of the Internet And How to Stop It (London: Yale University Press, 2008), 7-10.
[5] Katie Hafner ve Matthew Lyon, Where Wizards Stay Up Late - The Origins of the Internet (New York: A Touchstone Book, 1998) 7-9.
[6] Hollis ve Sander, International Law and Cyberspace, 1-3.

gerçekleşebilmektedir[7].

Bilgi sistemleri ve internet tarafından yönlendirilen siber uzay, insanların birbirleriyle bağlantı kurması, etkileşim kurması ve işbirliği yapması için yeni araçlar sağlayarak çevremizi olağanüstü şekillerde dönüştürmektedir. Bilgi ve iletişim teknolojisinin bileşenlerinin sürekli evrimi, temel dijital bileşenlerdeki ilerlemeler ve buna karşılık gelen maliyet düşüşleri, internetin dünya çapında giderek daha kolay erişilebilir ve kullanılabilir hale geldiğini göstermektedir. Sonuç olarak, siber uzay, yenilikler, girişimler, sosyal ağlar ve suç için yeni bir odak noktası haline gelmiştir[8].

3. Devletlerin Siber Saldırılar ile İlgili Tutumları

Devletler siber uzay ortamına ilgi duymaya başladıkça, bu alanın siyasi, askeri ve istihbarat amaçları için nasıl kullanabileceğiyle de daha fazla ilgilenmeye başlamışlardır. Bu durum, devletlere siber uzayda küresel ölçekte daha hızlı ve nispeten daha ucuz bir şekilde faaliyet göstermenin bir yolunu sunmuştur. Devletler siber uzayda gerçekleştirdikleri faaliyetlerini hem gizlice hem de örtülü olarak yapabilmektedirler.[9] Devletler, siber uzayda çeşitli saldırgan 'siber operasyonlar' gerçekleştirebilirler. Bu saldırılara şu örnekler verilebilir: (i) bilgisayar sistemlerinin, ağlarının veya destekledikleri altyapının kullanılabilirliğini veya bütünlüğünü bozan veya devre dışı bırakan siber saldırılar, (ii) siber casusluk normalde gizli olan verilere yetkisiz erişim sağlayan bilgi operasyonları ve (iii) hedef kitlenin tutum veya davranışlarını yazarların çıkarlarıyla uyumlu olacak şekilde değiştirmek veya güçlendirmek için dijital kaynakları bilişsel amaçlarla kullanan bilgi operasyonlarıdır. Bu operasyonların birçoğunun 'vekilleri' içermesi, çevrimiçi etkinliği bir devletin yönetimi veya kontrolü altında sınırlandırma çabalarını daha da karmaşık hale getirmektedir.[10]

Siber operasyonlar, siber uzayın yapısı gereği, çoğu zaman önceden tespit edilemeden ya da gözlemlenemeden gerçekleşir ve gözlemlense bile herhangi bir kişiye atfedilemeyebilir. Özellikle devlet destekli siber operasyonların gizli ve örtülü doğası, siber uzayla ilgili yapılan

[7] Zittrain, The Future of the Internet And How to Stop It, 7-10.
[8] Uche Mbanaso ve Emmanuel S. Dandaura, "The Cyberspace: Redefining A New World", OSR Journal of Computer Engineering, Volume 17, Issue 3, (2015), 18.
[9] Hollis ve Sander, International Law and Cyberspace, 1-3.
[10] Laura DeNardis, The Global War for Internet Governance (London: Yale University Press, 2014), 12.

düzenlemelere ilişkin devletlerin isteksiz kalmasını anlaşır kılmaktadır. Bu noktada derin ve sığ gizli siber operasyonları birbirinden ayırmak önemlidir. Derin gizli operasyonlar, varlığı henüz kamuya açıklanmayan bir devlete atfedilebilecek eylemleri kapsamaktadır. Sığ gizli operasyonlar ise varlığı kamuya açık hale gelen (örneğin, sızıntılar, kısmi ifşaatlar veya diğer aktörlerin tespiti yoluyla) ancak içeriği belirsiz kalan bir devlete atfedilebilen eylemleri kapsamaktadır.[11] Ayrıca gizli olmayan, gizli olan ve yarı gizli siber operasyonlar arasında da bir ayrım yapılabilir. Gizli olmayan operasyonlar, eylemde bulunan devlet tarafından resmi olarak kabul edilen bir devlete atfedilebilen eylemlerdir. Gizli operasyonlar, bir Devlete atfedilebilen ve eylemde bulunan devlet tarafından resmi olarak kabul edilmeyen eylemler olarak tanımlanmaktadır. Yarı gizli operasyonlar ise bir devlete atfedilebilen, kısmen kabul edilen, gerçekleştikten sonra bir noktada kabul edilen veya eylemde bulunan devletin resmi onayı olmadan rapor edilen ve varsayımsal olarak gerekçelendirilen eylemlerdir.[12]

Siber uzayda bugüne gerçekleştirilen siber saldırılarda, saldırıya uğrayan devletler genellikle duruma tepkisiz kalmıştır. Örneğin 2010 yılında İran'da nükleer santrallere gerçekleştirilen Stuxnet siber saldırısında İran'ın herhangi bir tepkisi olmamıştır. İran'ın bu tepkisizliği, dış nedenlerden ziyade iç işletme sorunlarından kaynaklandığı varsayılmakta ve İran olayı 'büyük bir siber saldırı' olarak nitelendirerek, ABD ile İsrail'i kötü niyetli bilgisayar solucanını yaymakla suçlamıştır. Ancak İran Stuxnet saldırısının uluslararası hukuka aykırı bir eylem olduğuna dair iddiası uluslararası kamuoyunda herhangi bir karşılık bulmamıştır.[13]

Siber uzayda gerçekleştirilen saldırılar ile ilgili devletler, olayın uluslararası hukuk kapsamındaki niteliği konusunda farklı düşünceler taşıyarak, genel olarak siber saldırı gerçekleştiren devletlerin davranışlarını kınamakla yetinmişlerdir. Örneğin ABD Dışişleri Bakanı John Kerry, 2014'te Sony Pictures Entertainment'a yönelik siber saldırının Kuzey Kore'nin "uluslararası normlara açıkça saygısızlığını" gösterdiğini öne sürerken, olayı kınamakla yetinmiş, uluslararası hukukun bu konuda adım atması konusu gündeme

[11] Milton L. Mueller, Networks and States: The Global Politics of Internet Governance (Massachusetts Institute of Technology 2010), 60-61.
[12] David P. Fidler, "Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection", Articles by Maurer Faculty, (2015): 2452.
[13] Fidler, Whither the Web?, 8.

getirilmemiştir.[14] 2016 ABD başkanlık seçimleri döneminde gerçekleştirilen siber saldırı iddialarına ilişkin olarak ABD, saldırının Kuzey Kore tarafından gerçekleştirildiğini iddia etmiş ve ABD başta olmak üzere Birleşik Krallık, Avustralya, Kanada, Japonya ve Yeni Zelanda, yapılan siber saldırıyı kınamakla yetinmişlerdir. Söz konusu devletler siber saldırı ile ilgili olarak uluslararası hukuk kurallarının konuya ilişkin düzenlemelerine ihtiyaçtan hiç bahsetmemişlerdir.[15]

İstisnai olarak, devletler, düşmanca siber operasyonların başka bir devlete atfedilmesi neticesinde bunun uluslararası hukuku ihlal ettiği iddialarını (uluslararası hukukun hangi belirli kurallarının ihlal edildiği konusunu net bir şekilde belirtmeden) da ifade etmişlerdir. Örneğin Ekim 2018'de Birleşik Krallık ve ABD, Rus askeri istihbarat teşkilatı tarafından siyasi kurumlara, işletmelere, medya kuruluşlarına ve uluslararası bir spor ajansına karşı yürütülen bir dizi siber operasyonu ifşa etmiş ve bu durumu kınamışlardır.[16] Birleşik Krallık Dışişleri Bakanlığı saldırıyı kınamanın ötesinde, Rusya'nın bu davranışının, uluslararası hukuk kurallarının ihlali anlamına geldiğini belirtmiştir. Hollanda ise saldırıyı "uluslararası hukukun üstünlüğünün baltalandığı" şeklinde değerlendirirken[17], Kanada Rusya'nın kötü niyetli siber faaliyetlerinin "uluslararası hukuku hiçe saydığını ve kurallara dayalı uluslararası düzeni baltaladığı" yönünde açıklamada bulunmuştur.[18] Rusya'nın Birleşik Krallık'a gerçekleştirmiş olduğu iddia edilen siber saldırılar ile ilgili suçlamalar iddia edilen operasyonlarının uluslararası hukuku ihlal edip etmediği veya uluslararası hukukun hangi kurallarını ihlal ettiği yönünde tartışmaları da beraberinde getirmiştir.

Kısacası siber uzayda siber saldırılardan mağdur olan devletler, ya da üçüncü devletler

[14] U.S. Department of State, Condemning Cyber-Attacks by North Korea, Press Release 2014, https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm. (18.09.2024).
[15] Thomas P. Bossert, "It's Official: North Korea Is Behind WannaCry",2017, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537, (18.09.2024).
[16] UK National Cyber Security Centre, Reckless Campaign of Cyber-attacks by Russian Military Intelligence Service Exposed, Press Release, 2018, https://www.gchq.gov.uk/news/reckless-campaign-of-cyber-attacks-by-russian-military-intelligence-service-exposed, (19.09.2024).
[17] Ministry of Defence of the Netherlands, Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber-operation Targeting OPCW, 2018, https://english.defensie.nl/topics/cyber-security/russian-cyber-operation, (19.09.2024).
[18] Global Affairs Canada, Canada identifies malicious cyber-activity by Russia, 2018, https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html, (19.09.2024).

saldırıları sadece kınamakla yetinmektedir. Efrony ve Shany'nin de belirttiği gibi, günümüzde siber saldırılara maruz kalan devletlerin, siber operasyonlarla karşı karşıya kaldıklarında davranışlarına yön verecek uluslararası hukuk kuralları ile ilgili çok az şey bulunmaktadır.[19] Bu bağlamda siber saldırılardan etkilenen devletlerin, siber saldırıları sadece kınaması ya da saldırılar sonrası sessiz kalması konu ile ilgili uluslararası hukuk kurallarının oluşturulup, yürürlüğe girmesini daha da zorlaştırmaktadır.

4. Siber Uzay ile İlgili Uluslararası Hukuk Kurallarını Belirleme Konusunda Yaşanan Uyuşmazlıkların Nedenleri

Siber saldırılara maruz kalan devletlerin, saldırıya uluslararası hukuk kuralları çerçevesinde cevap verilmesi hususunda isteksiz kalmaları konusunun en önemli sebebi siber operasyonların gizli ve/veya örtülü niteliği nedeniyle, bunların tepki gerektiren bir uygulama olarak nitelendirilmesinin oldukça zor olmasıdır. Uluslararası hukukta devlet uygulamalarının, devlet uygulaması olarak nitelendirilebilmesi için kamuya açık olması gerektiği yaygın olarak ileri sürülmektedir. [20] Uluslararası Hukuk Komisyonu raporlarına göre, devletlerin gerçekleştirmiş olduğu uluslararası hukuka aykırı gizli bir fiziksel eylem ortaya çıkarsa, devlet bu davranışının yasal olarak haklı olduğunu (meşru savunma) iddia etmeye çalışmadığı sürece, devletin uluslararası sorumluluğu doğacak ve davranış uluslararası hukuka aykırı bir davranış olarak nitelendirilecektir.[21] Bu durum, siber operasyonlar yürüten bir devletin, gizli bir siber operasyonu kabul etmediğinde, saldırı fiziksel bir saldırı gibi ispat edilemeyeceğinden devletin sorumluluğu konusu önemli bir sorun yaratmaktadır. Siber saldırı eyleminde bulunan devletin, davranışının uluslararası hukuka uygun bir 'uygulama' (meşru savunma) olduğunu iddia etmesi ise konuyu başka bir boyuta taşıyacaktır. Bu davranışın uluslararası hukuk açısından geçerli olabilmesi için siber saldırıya uğrayan Devletin, saldırıya yanıtını siber uzayda vermesi

[19] Efrony D. ve Shany Y. A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, American Journal of International Law, 112(4), (2018):583-657.
[20] Maurice Mendelson, "The Subjective Element in Customary International Law", The British Year Book of International Law; Oxford Vol. 66, Iss. 1, (1996): 177 – 208.
[21] International Law Association Committee on Formation of Customary (General) International Law, Statement of Principles Applicable to the formation of General Customary International Law (Report of the 69th Conference 1, ILA, London, 2000) 15.

gerekecektir.[22]

Siber saldırılara karşı devletlerin saldırıya uluslararası hukuk kuralları çerçevesinde cevap verilmesi hususunda isteksiz kalmaları konusunda bir diğer neden, birçok devletin bu alanda siber casusluk faaliyetleri yürütmek istemesi olarak düşünülebilir. Günümüzde devletler siber casusluğu kendileri aleyhine gerçekleştirilecek yasa dışı eylemlere karşı yasal bir istisna yol olarak ya da bu durumu tamamen uluslararası hukukun kapsamı dışında gören bir konu olarak değerlendirmektedirler. Örneğin ABD Savunma Bakanlığı Baş Hukuk Müşavirliği pek çok devletin yabancı ağlara yönelik kamuya açık olarak bilinen sayısız siber saldırı vakasına tam veya kısmen tepkisiz kalınması göz önüne alındığında, devletlerin egemenliğinin siber uzayda her zaman uluslararası hukukun temel kuralı olarak işlev gördüğü fikrini reddettikleri sonucunun doğduğunu belirtmiştir.[23] ABD Savunma Bakanlığının tespiti siber casusluk ile ilgili faaliyetlerin uluslararası hukuk açısından değerlendirilmesi bakımından önem teşkil etmektedir.

Siber uzay ile ilgili uluslararası hukuk kurallarını belirleme konusunda yaşanan uyuşmazlıkların temel nedenlerinden bir diğeri de devletlerin siber uzayda uygulanacak uluslararası hukuk kurallarına uyma konusunda gösterecekleri tutumdur. Devletler uluslararası belgelere yalnızca rıza göstererek, kendi özgür siyasi iradelerini kullanarak katılırlar. Şaşırtıcı olmayan bir şekilde devletler, bağımsız ve tarafsız kolluk kuvvetlerinin zorunlu yargı yetkisini tanıyan bağlayıcı antlaşmalara katılmayı sıklıkla reddederler. Uluslararası toplum, bu tür bir taahhütte bulunma isteksizliğini pragmatik bir yaklaşımı benimseyerek telafi etme eğilimindedir. Buna göre siber uzay ile ilgili uluslararası hukuk kurallarına uyulması, uluslararası belgeler tarafından kurulan uyum sistemleri, zorunlu kolluk kuvvetleri veya cezalandırıcı önlemler yerine işbirliği ve koordinasyon yoluyla doğrulamaya yoğunlaşabilecektir[24].

[22] William Thomas Worster, "The Effect of Leaked Information on the Rules of International Law", *American University International Law Review*, 28 no. 2 (2013): 443-488.
[23] Paul C. Ney, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, 2020, https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/, (19.09.2024).
[24] Dan Efrony, "Enhancing Accountability in Cyberspace Through a Three-Tiered International Governance Regime", International Law Studies, Vol. 103, (2024), 399.

Yukarıdakiler veriler ışığında, kapsamlı devletler arası siber saldırıların bağlayıcı bir uluslararası sözleşme ve kabul edilebilir bir uluslararası kolluk kuvveti mekanizması kurulmasını tetiklemede başarısız olması şaşırtıcı değildir. Bu nitelikteki araçlar ve mekanizmalar, gelişmiş siber yeteneklerle ilişkili riskleri önemli ölçüde azaltmak ve devletlerin bu yetenekleri istismar etme ve yasadışı, gizli siber operasyonlara girme cazibesini sınırlamak için elzemdir. Ancak, küresel sistemde devletler arasında işleyen bir uluslararası yasal siber güvenlik rejiminin unsurlarını oluşturma konusunda fikir birliğine varmak şu anda bir hayal gibi görünmektedir[25].

Siber saldırıya maruz kalan bir devletin, siber operasyonlara karşı tepkisiz kalması konuya uluslararası hukuk açısından önem vermediği olasılığını ortaya çıkarmaktadır. [26] Devletler günümüzde düşmanca amaçlarla gerçekleştirilen siber saldırıları açıkça yasal terimlerle kınasın veya kınamasın, bu tür eylemleri onaylanmadığının sinyalini vermeleri son derece önemlidir. Başka bir deyişle, devletler zaman içinde siber operasyonları sürekli olarak istenmeyen ancak uluslararası hukuka aykırı olmayan bir şekilde kınaması durumunda, devletler bir noktada uluslararası hukukun bu tür eylemleri yasaklamadığı veya en azından uluslararası hukukun 'gerçek bir kuralını' dönüştürmediği sonucunu ortaya çıkarabilecektir.[27]

5. Siber Operasyonlara Uygulanacak Uluslararası Hukuk Kuralı Sorunu ve Devlet Açıklamaları

Devletlerin siber uzayda siber operasyonları yürütmeye ilgi duymaya başlaması, genel olarak bu davranışı düzenleyen ilgili uluslararası yasal çerçevelerin düzenlenmesi konusunda uyuşmazlıkların yaşanmasına neden olmuştur. Ancak yaşanan bu uyuşmazlıklar siber uzayın imkanları düşünüldüğünde, devletlerin internet yönetişimi gibi siber operasyonları büyük ölçüde uluslararası hukukun kapsamı dışında, özel olmayan bir durum olarak mı görmesi gerektiği, yoksa buna açık bir itiraz olmadığı sürece önceden var olan genel uluslararası hukuku kurallarına ve ilkelerine tabi mi görmesi gerektiği gibi soruları daha fazla tartışır hale getirmiştir. Çalışmanın bu bölümünde siber uzay ile ilgili uluslararası hukuk kuralları oluşturma çabaları

[25] Efrony, “Enhancing Accountability in Cyberspace”, 400.
[26] Worster, The Effect of Leaked Information on the Rules of International Law, 445.
[27] Mendelson, The Subjective Element in Customary International Law, 180.

incelenecektir.

Siber uzayda uluslararası hukuk kurallarının uygulanmasına yönelik çalışmalara Birleşmiş Milletler Uluslararası Güvenlik Bağlamında Enformasyon ve Telekomünikasyon Alanındaki Gelişmelerle İlgili Hükümet Uzmanları Grubu (BM HUG) önemli bir katkı sağlamıştır[28]. BM HUG sırasıyla 2013 ve 2015'teki üçüncü ve dördüncü tur görüşmelerinde siber uzay ile ilgili bazı konularda fikir birliğine ulaşmayı başarmıştır[29]. Görüşmeler neticesinde fikir birliğine varılan temel konu, uluslararası hukuk kurallarının, özellikle BM Şartı'nın sibe ruzaya uygulanabilir olduğu ilkesini teyit edilmiş ve siber uzayda sorumlu devlet davranışı için bağlayıcı olmayan on bir normdan oluşan bir liste[30] üzerinde anlaşılmıştır. Liste siber uzaya ile ilgili uluslararası hukuk kurallarının oluşmasında önemli bir adım olsa da, uluslararası hukukun siber uzaya uygulanmasına yönelik önemli siyasi ve yasal engelleri çözmeyi başaramamıştır[31].

Siber uzay ile ilgili günümüzde uluslararası hukuk açısından en önemli metin Talinn Kılavuzları olmuştur. Orijinal adı "Siber Savaşa Uygulanabilir Uluslararası Hukuka İlişkin Tallinn El Kitabı" olan Tallinn Kılavuzları, uluslararası hukukun, özellikle de *jus ad bellum* ve uluslararası insancıl hukuk kurallarının siber çatışmalar ve siber savaşlara nasıl uygulandığına ilişkin akademik, bağlayıcı olmayan bir çalışma özelliği taşımaktadır. Tallinn Kılavuzları, 2009 ve 2012 yılları arasında Tallinn merkezli Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization - NATO) İşbirlikçi Siber Savunma Mükemmeliyet Merkezi'nin daveti üzerine yaklaşık yirmi uzmandan oluşan uluslararası bir grup tarafından yazılmıştır. Tallinn Kılavuzunun ilk baskısı uluslararası hukuk kurallarının siber uzaya uygulanabilirliği ile ilgili şu ifadelere yer vermektedir;

Uluslararası hukuk kurallarının siber uzaya uygulanması ile ilgili eşik soruları, mevcut yasanın siber sorunlara uygulanıp uygulanmayacağı ve uygulanıyorsa nasıl uygulanacağıdır. Konuyla ilgili görüşler, silahlı çatışma hukukunun tam olarak uygulanmasından, Uluslararası Adalet Divanı'nın bu yasanın 'kullanılan silahlara bakılmaksızın her türlü güç kullanımına'

[28] Efrony, "Enhancing Accountability in Cyberspace", 400.
[29] Efrony, "Enhancing Accountability in Cyberspace", 400 – 401.
[30] 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.
[31] Efrony, "Enhancing Accountability in Cyberspace", 400 – 401.

uygulanacağı yönündeki açıklamasına paralel olarak Uluslararası Sürekli Adalet Divanı'nın katı bir şekilde uygulanmasına kadar uzanmaktadır. Uluslararası Adaletin, uluslararası hukukta yasaklanmayan eylemlere ilişkin beyanlarına genel olarak izin verilmektedir.[32]

2013 yılında, Birleşmiş Milletler (BM) Hükümet Uzmanları Grubu'nun hazırlamış olduğu raporda, uluslararası hukukun genel uygulanabilirliğinin siber uzay için de mümkün olabileceğini belirtmiştir.[33] O tarihten bu yana bu tutum BM Genel Kurulu ve çeşitli bölgesel uluslararası örgütler tarafından da yinelenmiştir. Bununla birlikte, uluslararası hukukun genel olarak uygulanmasına ilişkin varoluşsal sorunların çözümü, yalnızca hangi uluslararası hukukun uygulanacağı konusundaki tartışmalara da kapı açmıştır. Örneğin, başta Çin olmak üzere birçok devlet, uluslararası insancıl hukuk kurallarının siber uzayda gerçekleşen davranışlara uygulanmasını kabul etmeye direnmiştir.[34] Diğer mevcut uluslararası hukuk doktrinleri ve mekanizmaları (örneğin, durum tespiti, karşı önlemler) benzer zorluklarla karşılaşmıştır.

2012 yılında ABD, uluslararası hukuk kurallarının siber uzaya nasıl uygulanabileceğine ilişkin resmi görüşlerini detaylandırmaya başlamıştır.[35] Diğer (çoğunlukla Batılı) devletler de kendi tek taraflı beyanlarını yayınlayarak bu örnekleri takip etmişlerdir. Şu anda 25'ten fazla devlet, uluslararası hukuk kurallarının siber uzaya uygulanmasına ilişkin ulusal görüşlerini kamuoyuna sunmuş ve BM Açık Uçlu Çalışma Grubu (OEWG) tüm devletlere bunu yapma çağrısında bulunmuştur.[36]

Siber uzayda uluslararası hukuk kurallarının oluşturulmasına yönelik devlet açıklamalarına bir diğer örnek "Siber Uzayda Sorumlu Devlet Davranışını Geliştirmeye İlişkin

[32] Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, (Cambridge: Cambridge University Press 2013), 15.
[33] See Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A68/156/Add.1, (Sept. 9, 2013).
[34] Julian Ku, How China's Views on the Law Jus Ad Bellum Will Shape its Legal Approach to Cyberwarfare, Aegis Paper No. 1701 (Stanford: Hoover Institution, 2017).
[35] Harold Hongju Koh, Harold Koh on International Law in Cyberspace, https://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/, (3.10.2024).
[36] Report of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135 (May 28, 2021).

Ortak Beyanname[37]'dir". ABD öncülüğünde, yirmi sekiz BM üye devletinin[38] uluslararası girişimi çerçevesinde yayınlanan Beyanname, devletlerin "Bağlayıcı Olmayan Normlar Listesi"ni ihlal etmelerinden sorumlu tutulması ve uluslararası hukuka uygun olarak şeffaf bir şekilde maliyetler uygulanması taahhüdünü içermektedir. Şubat 2020'de, yirmi sekiz ortak Devletten on beşi, Rusya'nın Rus askeri istihbarat teşkilatı tarafından yürütülen yıkıcı bir siber kampanyanın sorumluluğunu üstlenmesinde Gürcistan'ın yanında olduklarını açıklamış ve bu Devletler Rusya'yı kınayıp, Bağlayıcı Olmayan Normlar Listesine uymaya çağırmıştır[39]. 2020 yılından beri bu girişim de siber uzayda uluslararası hukuk kurallarının uygulanması konusunu yeteri kadar gündeme getirememiştir.

Devletlerin bu tür açıklamalarına rağmen, siber saldırılar ile ilgili kuralların oluşturulmasında yaşanan isteksizlik ya da konuyu sadece kınamakla yetinmesi siber uzay kuralları oluşturulması çabalarına zarar vermektedir. Bu noktada önemli bir sorun ile karşılamaktayız. Uluslararası hukuk bu isteksizlikleri nasıl değerlendirmelidir? Genel olarak uygulanabilir uluslararası hukuk kurallarının devletleri siber uzayda zaten bağladığı konusunda ısrar edenler için, bu ifadelerin hiçbir önemi olmadığı sonucu çıkarılabilir. Örneğin Dapo Akande, Antonio Coco ve Talita Dias şunu vurguluyor:

Uluslararası hukukun güç kullanma yasağı (BM Antlaşması Madde 2/4), müdahale etmeme kuralı genel uluslararası hukuk kapsamında ilgili koşullar altında her türlü devlet faaliyetine uygulanabilir. Dolayısıyla, uluslararası hukuk ve uluslararası insancıl hukuk kuralları, siber uzayda belirli devlet uygulamalarına ve diğer yeni teknolojilere uygulanabilirliğine ilişkin daha fazla kanıta ihtiyaç duyulmamaktadır.[40]

Ancak bazı uzmanlara göre siber uzayın yapısı ve burada gerçekleştirilen eylemler ile

[37] Joint Statement on Advancing Responsible State Behavior in Cyberspace, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/, (4.10.2024).

[38] 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, Slovenya, İspanya, İsveç, Birleşik Krallık ve Amerika Birleşik Devletleri.

[39] UK condemns Russia's GRU over Georgia cyber-attacks**,** https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (4.10.2024).

[40] Dapo Akande, Antonio Coco, and Talita de Sousa Dias, Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond, EJILTALK! 2021, https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond, (4.10.2024).

ilgili, devletlere yasal yükümlülükler atfetmeden önce devletlerin davranışlarını ya da uygulamalarını detaylandırmasını gerektirmektedir. Konu ile ilgili İsrail Başsavcı Yardımcısının görüşleri şu şekildedir;

Herhangi bir fiziksel alan için geçerli olan geleneksel bir kuralın siber alan için de geçerli olduğu otomatik olarak varsayılamaz. Devlet uygulamasının tanımlanmasındaki kilit soru, diğer alanlarda ortaya çıkan uygulamanın siber alanda öngörülen faaliyetle yakından ilişkili olup olmadığıdır. Ayrıca, diğer alanlarda uygulanan örf ve adet kurallarının ortaya çıkmasına neden olan hukuk görüşünün alana özgü olmadığının da tespit edilmesi gerekmektedir. Siber alanın benzersiz özellikleri göz önüne alındığında, bu tür bir analizin özellikle ihtiyatlı bir şekilde yapılması gerekmektedir, çünkü çoğu zaman bu alanın yapısı ile ilgili farklılıklar mevcuttur.[41]

Sonuç olarak devletlerin siber uzay ile ilgili kuralların oluşturulması açıklamalarına rağmen, uluslararası hukukun siber uzayda nasıl uygulanacağına dair somut bir veri bulunmamaktadır. Bu noktada devlet dışı aktörlerin çalışmaları konu ile ilgili alandaki boşluğu doldurmaya çalışmaktadır. Özellikle iki Tallinn El Kitabı ve Uluslararası Kızılhaç Komitesi'nin çalışmaları bunun en belirgin örnekleridir. Bu çabalarda ifade edilen tutumlar, 'ilk harekete geçenler' olarak, sessizliklerini bozmaya karar veren devletler arasında bile etkili olmaya devam etmiştir.

5. Sonuç

Siber uzay ile ilgili kuralların oluşturulması noktasında devletler arasında yaşanan uyuşmazlıklar nedeniyle uluslararası hukuk kurallarının bu alana ne zaman veya nasıl uygulanacağı sorusu mevcudiyetini sürdürmektedir. Devlet dışı aktörlerin (örneğin, Tallinn Kılavuzları veya BM raporları) siber uzay üzerindeki çalışmaları, devletlerin tepkisini gerektirip gerektirmediğini veya bunun için yasal bir iddianın gerekli olup olmadığı ise siber uzay ile ilgili ayrı bir tartışma konusu oluşturmaktadır.

Siber uzayın yapısı incelendiğinde bu alanla ilgili olarak kuralların oluşturulmasında devletler arasında yaşanan uyuşmazlıklar bazı gerekçelere dayanarak mantıklı gelebilir.

[41] Hollis ve Sander, International Law and Cyberspace, 3-5.

Devletler ve diğer paydaşlar siber uzay ile ilgili çalışmalarda yaşanan uyuşmazlıklar konusunu henüz açıkça kabul etmemiş olsalar bile, devlet siber operasyonları ve devletlerin siber uzaya ilişkin uluslararası hukuk kuralları beyanları incelendiğinde, henüz bu alan ile ilgili yeterli çalışmaların yapılmadığı görülmektedir.

Uluslararası hukuk ve siber uzay üzerine yapılan çalışmalar ele alınırken devletlerin konuya ilişkin çalışmalarında yaşanan uyuşmazlıklar, konu ile ilgili yasal düzenlemelerin oluşturulmasını zorlaştırmaktadır. Uluslararası hukuk bağlamında siber uzayın varlığı ve anlamı hakkındaki netlik sorunları ele aldığında, devletlerin bu alanda yapılacak düzenlemeler konusunda işbirliğine ihtiyaç duyulmaktadır. Devletlerin siber uzaydaki davranışları daha şeffaf hale gelse bile, her bir devletin teknolojiyi anlama kapasitesi, nasıl çalıştığı ve siber uzay kurallarının oluşturulmasındaki yaşanan uyuşmazlıklar, işbirliği konusunu ertelemeyecektir. Devletlerin büyük çoğunluğunun teknik bir konu olarak siber uzay konusunda yeterli anlayışa sahip olmaması nedeniyle, siber uzay şu anda kapasite sorularıyla doludur ve bu durum bazı devletleri teknolojiden anlayan aktörlerin davranış ve konuşmalarının gerisinde veya dışında bırakmaktadır. Ayrıca açıklık, şeffaflık, yetenek ve/veya duyarlılığın siber uzayda devletler arasında yaşanan uyuşmazlıkları açıklamaya yardımcı olup olmadığını değerlendirmek için işbirliğinden öte daha fazla araştırmaya da ihtiyaç bulunmaktadır.

Devletlerin siber operasyonlarına ve devletin uluslararası hukuka ilişkin beyanlarına ilişkin yaklaşımlar, siber uzay kurallarının oluşturulmasına ilişkin ek perspektiflerin faydasını göstermektedir. Çalışma sonucunda iki husus önem kazanmıştır. Bu hususlardan ilki siber uzayda gerçekleştirilen bazı davranış veya iddialara tepki verilmesi gerektiği konusunda yaşanan uyuşmazlıkların azaldığı ancak uluslararası hukuk kurallarının oluşturulması ile ilgili yaşanan uyuşmazlıkların devam ettiğidir. İkinci husus ise siber uzay ile ilgili uluslararası hukuku ilgilendiren kuralların veya düzenlemelerin yokluğu, bu alanı kullanmak isteyenleri tetiklemekte veya işlerini kolaylaştırmaktadır.

Sonuç olarak devletlerin uluslararası hukuk kurallarına uymaları konusunda yaşanan uyuşmazlıklar, uluslararası hukukun siber uzayda inşası üzerinde kendisini daha fazla hissettirmektedir. Giderek artan sayıda Devlet, bu kurallar veya normlarla ilgili tartışmalı yasal

konular hakkındaki görüşlerini kısmen açıklığa kavuşturmuş olsa da, siber uzayda normatif netlik ve şeffaflığa ulaşmak uzak bir hedef olmaya devam etmektedir.

Extended Summary

Due to disagreements between states regarding the establishment of rules regarding cyberspace, the question of when or how international law rules will be applied to this area continues to exist. Whether the work of non-state actors (for example, the Tallinn Guides or UN reports) on cyberspace requires a reaction from states or whether a legal claim is necessary for this constitutes a separate discussion topic regarding cyberspace.

When the structure of cyberspace is examined, disagreements between states regarding the establishment of rules regarding this area may seem logical based on some justifications. Even if states and other stakeholders have not yet openly accepted the issue of disagreements regarding studies regarding cyberspace, when state cyber operations and the declarations of states regarding international law rules regarding cyberspace are examined, it is seen that sufficient studies have not yet been conducted regarding this area.

When considering studies on international law and cyberspace, disagreements experienced in the studies of states on the subject make it difficult to establish legal regulations on the subject. When addressing the issues of clarity regarding the existence and meaning of cyberspace in the context of international law, there is a need for cooperation between states on regulations to be made in this area. Even if states' behaviors in cyberspace become more transparent, the capacity of each state to understand technology, how it works, and disagreements experienced in establishing cyberspace rules will not postpone the issue of cooperation. Since the vast majority of states do not have sufficient understanding of cyberspace as a technical issue, cyberspace is currently full of capacity questions, leaving some states behind or outside the behaviors and speeches of technologically savvy actors. In addition, more research is needed beyond cooperation to evaluate whether openness, transparency, capability, and/or sensitivity help explain disagreements between states in cyberspace.

Approaches to states' cyber operations and state declarations regarding international law demonstrate the benefits of additional perspectives on establishing cyberspace rules. As a result

of the study, two issues have gained importance. The first of these issues is that the disagreements experienced on the need to react to certain behaviors or claims made in cyberspace have decreased, but the disagreements experienced on the establishment of international law rules continue. The second issue is that the absence of rules or regulations regarding international law related to cyberspace triggers or facilitates the work of those who want to use this area.

As a result, the disagreements experienced on the compliance of states with international law rules make themselves felt more on the establishment of international law in cyberspace. Considering the advancement of technology and the advantages of cyberspace, the need for studies conducted on the establishment, functioning or effectiveness of international laws related to cyberspace is increasing day by day.

Kaynakça

Akande, D., Coco, A., & Dias, .T. D. (2021), Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond, EJILTALK! 2021, https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond, (4.10.2024).

Bossert, Thomas P., It's Official: North Korea Is Behind WannaCry, Wall Street Journal, 2017, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537. (18.09.2024).

Clark, David, Characterizing Cyberspace: Past, Present and Future (MIT,CSAIL, 2010), 2-6.

Denardis Laura, The Global War For Internet Governance, Yale University Press, 2014.

Efrony, Dan, "Enhancing Accountability in Cyberspace Through a Three-Tiered International Governance Regime", International Law Studies, Vol. 103, (2024), 399.

Fidler, David, ""Whither the Web?: International Law, Cybersecurity, and Critical Infrastructure Protection", Articles by Maurer Faculty, (2015): 2452.

Global Affairs Canada, Canada identifies malicious cyber-activity by Russia, 2018, https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html, (19.09.2024).

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.

Hollis Duncan B. & Sander, Baries, International Law and Cyberspace: What Does State Silence Say? (Temple University Beasley School of Law Legal Studies Research Paper No. 2022-22), 1-3.

Hollis, Duncan, B. & Raustiala, K. (2023), The Global Governance of the Internet, in M. Barnett & D. Snidal (Eds.), The Oxford Handbook Of Internatıonal Institutions. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4197418.

International Law Association Committee on Formation of Customary (General) International Law, Statement of Principles Applicable to the formation of General Customary International Law (Report of the 69th Conference 1, ILA, London, 2000)

Joint Statement on Advancing Responsible State Behavior in Cyberspace, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/, (4.10.2024).

Ku, Julian How China's Views on the Law Jus Ad Bellum Will Shape its Legal Approach to Cyberwarfare, Aegis Paper No. 1701 (Stanford: Hoover Institution, 2017).

Koh, Harold Hongju, Harold Koh on International Law in Cyberspace, https://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/. (3.10.2014).

Lyon Matthew ve Hafner Katie, Where Wizards Stay Up Late - The Origins of the Internet New York: A Touchstone Book, 1998

Mbanaso, Uche & Dandaura, Emmanuel S., "The Cyberspace: Redefining A New World", OSR Journal of Computer Engineering, Volume 17, Issue 3, (2015), 18.

Mendelson Maurice, "The Subjective Element in Customary International Law", The British Year Book of International Law; Oxford Vol. 66, Iss. 1, (1996): 177 – 208.

Ministry of Defence of the Netherlands, Netherlands Defence Intelligence and Security Service disrupts Russian cyber-operation targeting OPCW, 2018, https://english.defensie.nl/topics/cyber-security/russian-cyber-operation, (19.09.2024).

Mueller, Milton L., Networks and States: The Global Politics of Internet Governance Massachusetts Institute of Technology, 2010.

Ney, Paul C., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, 2020, https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/, (19.09.2024).

Report of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135 (May 28, 2021),

Revision of the International Telecommunication Regulations, 17 ASIL INSIGHT (Feb. 7, 2013).

Schmitt Michael N. Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press 2013.

UK National Cyber Security Centre, Reckless campaign of cyber-attacks by Russian military intelligence service exposed, Press Release, 2018,https://www.gchq.gov.uk/news/reckless-campaign-of-cyber-attacks-by-russian-military-intelligence-service-exposed, (19.09.2024).

UK condemns Russia's GRU over Georgia cyber-attacks**,** https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (4.10.2024).

U.S. Department of State, Condemning Cyber-Attacks by North Korea, Press Release (Dec. 18,2014), https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm. (18.09.2024).

Worster William Thomas, "The Effect of Leaked Information on the Rules of International Law", American University International Law Review, 28 no. 2 (2013): 443-488.

Zittrain, Jonathan, The Future of the Internet And How to Stop It, London: Yale University Press, 2008.