

ULUSLARARASI HUKUKUN SINIRLARINDA BİR MÜDAHALE ARACI: SİBER YAPTIRIMLAR VE SİBER KARŞI ÖNLEMLER ÜZERİNE HUKUKİ BİR DEĞERLENDİRME

*An Instrument of Intervention within the Limits of International Law:
A Legal Assessment of Cyber Sanctions and Cyber Countermeasures*

Zeynep ERHAN BULUT*

Özet

Bu çalışma, uluslararası hukuk bağlamında giderek artan siber güvenlik tehditleri karşısında ortaya çıkan “siber yaptırımlar” ve “siber karşı önlemler” kavramlarını hukuki açıdan incelemeyi amaçlamaktadır. Birleşmiş Milletler Güvenlik Konseyi tarafından uygulanan kolektif yaptırımlar ile devletlerin tek taraflı olarak uyguladığı karşı önlemler arasındaki farklar, normatif dayanaklar ve meşruiyet sorunu temelinde analiz edilmiştir. Çalışmada ilk olarak Birleşmiş Milletler Şartı’nın VII. Bölümü çerçevesinde siber yaptırımların hukuki geçerliliği ve uygulanabilirliği değerlendirilmiştir. İkinci bölümde ise devletlerin tek taraflı olarak uyguladığı siber karşı önlemler, “Devlet Sorumluluğu” çerçevesinde ele alınmış; atfedilebilirlik, orantılılık ve geçicilik gibi uluslararası hukuk ilkeleri ışığında hukuki sınırları irdelenmiştir. Son olarak, Amerika Birleşik Devletleri, Birleşik Krallık ve Avrupa Birliği gibi aktörlerin siber yaptırım uygulamaları örneklerle değerlendirilmiş; Türkiye’nin bu konudaki yaklaşımı da karşılaştırmalı olarak ele alınmıştır. Elde edilen bulgular, siber yaptırımların hem kolektif hem de tek taraflı biçimlerinin, teknik gelişmelerin hızına paralel olarak uluslararası hukukta yeni düzenlemelere ihtiyaç duyulduğunu ortaya koymaktadır.

Anahtar Kelimeler: Siber yaptırım, siber karşı önlem, Güvenlik Konseyi, devlet sorumluluğu, insan hakları

Abstract

This study examines the concepts of cyber sanctions and cyber countermeasures from a legal perspective, in response to the growing cyber security threats in the context of international law. It analyses the differences, normative bases, and legitimacy issues between collective sanctions imposed by the United Nations Security Council and unilateral countermeasures implemented by individual states. The first section evaluates the legal validity and applicability of cyber sanctions within the framework of Chapter VII of the UN Charter. The second section addresses unilateral cyber countermeasures taken by states, analysed under the framework of State Responsibility. It examines their legal limits considering international law principles such as attributability, proportionality, and temporariness. Finally, the study evaluates the cyber sanction practices of

➤ Bu makale Etik Kurul iznine tabi değildir/This article is not subject to Ethics Committee permission.

➤ Makale Geliş Tarihi/Article Received Date: 2.06.2025

➤ Yayın Kurulu Kabul Tarihi/Editorial Board Acceptance Date: 30.10.2025

* Dr. Öğr. Üyesi, Çankırı Karatekin Üniversitesi Hukuk Fakültesi, Milletlerarası Hukuk Ana Bilim Dalı, Çankırı/Türkiye, zeynep@karatekin.edu.tr, <https://orcid.org/0000-0002-5766-126X>



actors such as the United States, the United Kingdom, and the European Union, and provides a comparative analysis of Turkey's approach. The findings indicate that both collective and unilateral cyber sanctions highlight the need for new regulatory measures in international law in line with the rapid pace of technological developments.

Keywords: Cyber sanction, cyber countermeasure, Security Council, state responsibility, human rights

GİRİŞ

Birleşmiş Milletler (BM) Güvenlik Konseyi tarafından, BM Şartı'nın VII. Bölümü çerçevesinde uygulanan geleneksel yaptırımlar, genellikle hedef alınan devlet ya da aktörün uluslararası yükümlülüklerine uymasını sağlamak amacıyla kullanılmaktadır. Ancak bu yaptırımlar, çoğu zaman sivil nüfusa ciddi zararlar vermesi ve beklenen siyasi sonuçları doğurmaması nedeniyle eleştirilmektedir¹. Bu bağlamda uluslararası hukuk literatüründe siber yaptırımlar; hem geleneksel yaptırımlara tamamlayıcı bir araç olarak hem de siber uzayın giderek daha fazla çatışma alanı haline geldiği çağdaş uluslararası ilişkilerde başlı başına bir yaptırım modeli olarak tartışılmaya başlanmıştır².

Aşağıda detaylıca tartışılacağı üzere BM Güvenlik Konseyi'nin siber yaptırımlar uygulama yetkisi hem teknik hem de hukuki olarak mümkün gözükmemektedir. Fakat BM henüz siber yaptırımları sistematik olarak tanımlamamıştır. Bu nedenle BM Güvenlik Konseyi tarafından alınabilecek siber yaptırımların hukuki çerçevesi çizilmeli ve uygulanabilecek yaptırımlar konusunda BM'ye getirilen normatif sınırlamalar -insan hakları hukuku ve insancıl hukuk- dikkate alınmalıdır. Zira bu sınırlamalar BM Güvenlik Konseyi'nin hareket alanını şekillendirmektedir.

BM kararı olmaksızın otonom şekilde tek taraflı yaptırım uygulayan diğer birimler ise devletlerdir. Nitekim devletler halihazırda tek taraflı siber karşı önlemler almaktadır. Aşağıda da tartışılacağı üzere, devletlerin uyguladığı bu tür karşı önlemlerin bağlayıcı bir normatif düzenlemeye tabi olmaması, uluslararası hukuk açısından meşruiyet sorunlarına yol açmaktadır. Zira koşulları karşılanmaksızın uygulanan tek taraflı yaptırım niteliğindeki siber karşı önlemler, hedef devletin egemenliğini ihlal edebilir³. Bununla birlikte düşük maliyetleri ve mevcut

¹ Dursun Peksen, 'Better or Worse? The Effect of Economic Sanctions on Human Rights' (2009) 46(1) *Journal of Peace Research* 59, 59-77.; Lee Jones, *Societies Under Siege: Exploring How International Economic Sanctions (do not) Work* (Oxford University Press 2015).; Thomas G. Weiss, 'Sanctions as a Foreign Policy Tool: Weighing Humanitarian Impulses' (1999) 36(5) *Journal of Peace Research* 499, 499-509. Francisco Rodríguez, 'The Human Consequences of Economic Sanctions' (2024) 51(4) *Journal of Economic Studies* 942, 942-963.

² Siber uzay, bir yandan sanal gerçeklik ortamlarında insanların içine girip etkileşim kurabildiği üç boyutlu dünyaları, diğer yandan ise bilgisayar ağları, internet, yazılımlar ve veri depolama teknolojilerinden oluşan işlevsel iletişim alanını ifade eden dijital bir mekândır. Rebecca Bryant, 'What Kind of Space is Cyberspace' Minerva-An Internet (2001) 5 *Journal of Philosophy* 138, 139-140.

³ Thanapat Chatinakrob, 'Interplay of International Law and Cyberspace: State Sovereignty Violation,

normatif belirsizlikler nedeniyle devletler, bu tür önlemleri bir dış politika aracı olarak giderek daha fazla tercih etmektedir. Özellikle güçlü devletler tarafından benimsenen bu yeni yaptırım biçimi karşısında, yalnızca teknik kapasite değil, aynı zamanda açık tanımlar, hukuki çerçeveler ve normatif denge mekanizmalarının da oluşturulması gerekmektedir. Zira siber uzayın artan jeopolitik rolü göz önünde bulundurulduğunda, uluslararası hukuk bu alanı daha ciddiyetle ele almak zorundadır.

Günümüzde siber uzayın öneminin giderek arttığını ve bu alanın doğasında barındırdığı güvenlik tehditlerinin daha belirgin hale geldiği ifade edilebilir. Çünkü siber uzayın kendisi başlı başına devletler arası düşmanca faaliyetlerin gerçekleştiği bir çatışma alanına dönüşmüştür⁴. Nitekim geleneksel bağlamda alınan BM Güvenlik Konseyi yaptırım kararları ve tek taraflı devlet yaptırımları, bilgi ve iletişim teknolojilerinin gelişiminden etkilenmiş; bu doğrultuda, söz konusu tedbirlerin biçim ve nitelikleri değişime uğramıştır. Bu bağlamda yenilik, söz konusu eylemlerin siber uzayda gerçekleşmesi ve bilgisayar ağlarına yönelik saldırı yöntemlerinin ciddi bir etkinlik ile kullanılmasıdır.

Bu çerçevede, bu çalışmada öncelikle yaptırım kavramı ele alınacaktır. Devamında ise ilk olarak, kolektif yaptırımların teorik altyapısı incelenecek; ardından BM Güvenlik Konseyi uygulamaları ve Yaptırımları İzleme Komitelerinin siber yaptırım tavsiye kararları üzerinden kapsamlı bir değerlendirme yapılacak ve uygulamalara yönelik eleştiriler sunulacaktır. Çalışmanın ikinci bölümünde, tek taraflı yaptırım niteliğindeki karşı önlemlerin hukuki çerçevesi çizilecek ve bu önlemlerin uygulanabilmesi için gerekli koşullar detaylı bir şekilde incelenecektir. Bu koşullar doğrultusunda, karşı önlemlerin siber alandaki uygulama örnekleri üzerinden analizler yapılacaktır. Bu bölümün odak noktası, devletlerin silahlı saldırı teşkil etmeyen kötü niyetli siber faaliyetlere karşı hangi koşullar altında karşı önlem uygulayabileceklerini incelemektir. Bu noktada, dikkat edilmesi gereken önemli bir husus, siber olmayan faaliyetlere karşı da siber karşı önlemlerin kullanılabilmesidir. Son bölümde ise, siber yaptırımlar konusunda çeşitli ülke örnekleri incelenecek ve Türkiye'nin tutumu üzerine bir değerlendirme yapılacaktır.

I. ULUSLARARASI HUKUKTA YAPTIRIM KAVRAMI

Uluslararası hukuk literatüründe ağırlıklı olarak BM Güvenlik Konseyi'nin aldığı önlemler “yaptırım” olarak adlandırılmaktadır. Uluslararası Hukuk Komisyonu da modern uluslararası hukukta “yaptırım” (sanction) kavramının, (i) ciddi sonuçlar doğuran bir uluslararası yükümlülük ihlali sonrasında, (ii) ulusla-

Extraterritorial Effects, and the Paradigm of Cyber Sovereignty’ (2024) 23(1) *Chinese Journal of International Law* 25, 25-72.

⁴ Detaylı bilgi için bkz. Derek S. Reviron (ed), *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Georgetown University Press 2012).



rarası toplumun tamamını ilgilendiren durumlarda ve (iii) özellikle BM'nin BM Şart'ından kaynaklanan yetkileri çerçevesinde uluslararası barış ve güvenliği sağlamak amacıyla alabileceği bazı önlemleri ifade etmek üzere kullanıldığına dikkat çekmektedir⁵. Prof. Abi-Saab da yaptırımı, uluslararası hukuka aykırı bir fiile karşı yetkili bir toplumsal organ tarafından uygulanan zorlayıcı bir tepki olarak tanımlamaktadır⁶. Crawford, “yetkili toplumsal organ” ifadesinden kendi adına hareket eden tek bir devletin ya da küçük bir devlet grubunun anlaşılması gerektiğini vurgulamaktadır⁷. Nitekim Crawford, bu tanımdaki “yetkili toplumsal organ”ın, BM Güvenlik Konseyi gibi uluslararası toplumun çıkarları adına kolektif hareket etme yetkisine sahip bir kurum olabileceğini ifade etmektedir⁸. Bu bağlamda “yetkili toplumsal organ” tekil devletlerin değil, uluslararası normlara göre hareket eden meşru kolektif yapıların kararlarının geçerliliğini esas alır⁹. Schmitt de BM Güvenlik Konseyi tarafından BM Şartı'nın VII. Bölümü uyarınca uygulanan gönüllü ya da zorunlu yaptırımların karşı önlem olarak değerlendiremeyeceğini ifade etmektedir¹⁰.

Ancak uluslararası hukuk literatüründe hem devletlerin tek taraflı önlemleri hem de BM Güvenlik Konseyi'nin kolektif önlemleri için “yaptırım” kavramının kullanıldığı görülmektedir. Bu durum, kavramın içeriği ve kapsamı bakımından ciddi bir terminolojik belirsizliğe yol açmaktadır. Zira BM Şartı'nın VII. Bölümü, “yaptırım” (sanction) terimini değil, yalnızca “önlem” (measure) kavramını kullanmaktadır. Devletlerin uluslararası hukuka aykırı fiillerinden doğan sorumluluğu düzenleyen ve yumuşak hukuk¹¹ niteliğinde olan “Devletlerin Uluslararası Hukuka Aykırı Fiillerinden Dolayı Sorumluluğu Hakkında Taslak Maddeler”, bu tür tek taraflı uygulamalar için “karşı önlem” (countermeasure) terimini be-

⁵ Yearbook International Law Commission, 1979 Vol 2, Part 2, Report of the Commission to the General Assembly on the Work of Its Thirty-first Session, 121 <https://legal.un.org/ilc/publications/yearbooks/english/ilc_1979_v2_p2.pdf> E.T.14.02.2025.

⁶ James Crawford, ‘The Relationship Between Sanctions and Countermeasures’ in Mariano Garcia Rubio and Hassiba Hadj-Sahraoui (eds), *United Nations Sanctions and International Law* (Graduate Institute of International and Development Studies Vol 1, Kluwer Law International 2001) 57.

⁷ ibid. 57.

⁸ ibid. 57.

⁹ James Crawford and Freya Baetens, ‘The Creation of States in International Law’ in D Lyons (ed), *Leading Works in International Law* (Routledge 2023) 37–53.

¹⁰ Michael N. Schmitt, ‘Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law’ (2013) 54 *Virginia Journal of International Law* 697, 702.

¹¹ Yumuşak hukuk, bağlayıcılığı olmayan ve taraflara zorunlu yükümlülükler getirmeyen bir hukuk türüdür. Özünde kurallardan çok genel normlar ve ilkelerden oluşur, bu nedenle bağlayıcı uyumsuzluk çözüm yollarıyla kolayca uygulanamaz ya da yaptırıma bağlanamaz. Yumuşak hukuk metinleri, taraflar açısından zorunluluk değil, yönlendirici nitelik taşır; devletlere veya aktörlere belli bir davranış standardı önerir. Bu yönüyle, çoğu zaman uluslararası hukuk yapım sürecinde ilk adım olarak değerlendirilir ve ileride bağlayıcı kurallara dönüşebilecek bir zemin oluşturabilir. Nagihan Cihangir, ‘The Role of Soft Law and the Interplay Between Soft Law and Hard Law in the Context of International Human Rights’ (2017) 8(14) *Law & Justice Review* 201, 204.

nimsemiştir. Bu kavramların birbirlerinin yerine ikame edilerek kullanılması, kavramsal düzlemde birçok tartışmaya yol açmaktadır. Zira “yaptırım” kavramı ile “karşı önlem” kavramlarının hukuki dayanakları ve uygulanma koşulları tamamen farklı özelliklere sahiptir. Bu kavramsal karışıklığı önlemek amacıyla, bu çalışmada “kolektif yaptırım” ve “tek taraflı devlet yaptırımı” şeklinde bir ayırım benimsenmiştir. Buna göre, “kolektif yaptırım” ifadesi, BM Güvenlik Konseyi kararına dayanarak uygulanan ve uluslararası hukukta yüksek düzeyde meşruiyet taşıyan yaptırımları ifade ederken, “tek taraflı devlet yaptırımları” ise esasen “karşı önlem” niteliğindeki bireysel devlet uygulamalarını tanımlamak için kullanılacaktır¹².

Bu bağlamda çalışmanın ana temasını oluşturan siber yaptırım kavramına geçmeden önce çok taraflı kolektif (multilateral) ve tek taraflı (unilateral) yaptırımlar arasındaki kavramsal farklılığın değerlendirilmesi gerekmektedir. Zira tek taraflı olarak uygulanan devlet yaptırımları ile BM Şartı’nın VII. Bölümü çerçevesinde BM Güvenlik Konseyi kararı üzerine uygulanan çok taraflı kolektif yaptırımlar birbirinden farklıdır. Tek taraflı yaptırım ifadesi, bir devletin tek başına ya da bir grup devletin *ad hoc* bir koalisyon yaratarak aldığı önlemleri ifade etmektedir. Bu tür önlemlerin temel özelliği bu devlet veya devletlerin meşru bir öz yardım (*self-help*) kavramı doğrultusunda BM’nin herhangi bir müdahalesi olmaksızın- BM’nin kararı olmaksızın ve BM adına hareket etmeksizin – uyguladığı yaptırımlardır¹³.

Tek taraflı yaptırımların, bağlayıcı nitelikte bir uluslararası hukuk kaynağına dayandığını söylemek henüz mümkün değildir. Bununla birlikte bu tür yaptırımların dayandığı hukuki gerekçenin, “devletlerin sorumluluğu” mekanizması olduğu kabul edilmektedir. Zira devletlerin uluslararası hukuka aykırı eylemleri nedeniyle sorumlu tutulabilecekleri, uluslararası hukukta genel kabul görmüş bir ilkedir¹⁴. Devlet sorumluluğuna ilişkin temel hukuki çerçeve ise, “Devletlerin Uluslararası

¹² Tek taraflı yaptırım ibaresi birçok uluslararası hukukçu tarafından kullanılmaktadır. Iryna Bogdanova and Maria Vasquez Callo-Muller, ‘Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value’ (2021) 54 *Vanderbilt Journal of Transnational Law* 911. Tom Ruys, ‘Sanctions, Retortions and Countermeasures: Concepts and International Legal Framework’ in (eds) *Research Handbook on UN Sanctions and International Law* (Edward Elgar Publishing 2017) 19–51. Alexandra Hofer, ‘The Developed/Developing Divide on Unilateral Coercive Measures: Legitimate Enforcement or Illegitimate Intervention?’ (2017) 16 *Chinese Journal of International Law* 175. Vera Rusinova and Ekaterina Martynova, ‘Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses’ (2024) 57 *Israel Law Review* 135.

¹³ *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, ICJ Reports 1997, 7. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, Merits, Judgment, ICJ Reports 1986, 127, para 249. Ayrıca bkz. Malcolm D. Evans, *International Law* (2nd edn, Oxford University Press) Part V, 469.

¹⁴ Uluslararası Adalet Divanı (UAD), bu ilkeyi birçok kez teyit etmiştir. Bkz. *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)* (Judgment) [1997] ICJ Rep 7, paras 82–83. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, 127, para 249.



sı Hukuka Aykırı Fiillerinden Dolayı Sorumluluğu Hakkında Taslak Maddeler” ile çizilmiştir. Ancak bu taslak maddeler, henüz bağlayıcı bir uluslararası hukuk normu niteliği kazanmamış olup sert/katı hukuk (hard law) değil yumuşak hukuk (soft law) niteliğindedir. Yine yumuşak hukuk niteliğinde olan Birinci Tallinn El Kitabının 6. Kuralında da “*bir devlet, kendisine atfedilebilen ve uluslararası bir yükümlülüğün ihlalini oluşturan bir siber operasyon nedeniyle uluslararası hukuki sorumluluk taşır*”¹⁵ denmektedir. Bu nedenle günümüz itibarıyla devlet sorumluluğu hukukunun siber faaliyetleri de kapsadığı kabul edilmelidir¹⁶.

Çok taraflı yaptırımlar ise BM Güvenlik Konseyi’nin kolektif güvenlik sistemi çerçevesinde baskı uygulamak amacıyla aldığı kararlara dayalı önlemlerdir¹⁷. Uluslararası barış ve güvenliğin sağlanması temel sorumluluğu olan BM Güvenlik Konseyi, BM Şartı’nın 39. maddesi çerçevesinde “barışın tehdidi, bozulması ve saldırı eylemi” durumunda önlem alma yetkisi ile donatılmıştır. BM Güvenlik Konseyi tarafından alınabilecek önlemler “zorlama tedbirleri” olarak ifade edilmekte olup VII. Bölüm çerçevesinde düzenlenmektedir¹⁸. Tek taraflı yaptırım kararlarından farklı olarak BM Güvenlik Konseyi kararı ile alınan yaptırım kararları tüm BM üyesi devletler üzerinde bağlayıcıdır¹⁹. Bu doğrultuda, BM tarafından alınan ve niteliği gereği çok taraflı olan yaptırım kararlarının BM üyesi tüm üye devletler açısından hukuken bağlayıcı olduğu ifade edilmelidir.

Bu çerçevede, takip eden bölümlerde siber yaptırımların iki temel boyutu olan kolektif siber yaptırımlar ile devletler tarafından tek taraflı olarak uygulanan siber karşı önlemler ayrıntılı şekilde ele alınacaktır. İncelemede, her iki yaptırım türünün hukuki dayanakları, uygulanabilirlik koşulları ve uluslararası hukuk açısından doğurduğu meşruiyet sorunları değerlendirilecektir. Böylece siber uzayda yürütülen yaptırım uygulamalarının mevcut normatif çerçeveye ne ölçüde uyum sağladığı ortaya konulmaya çalışılacaktır.

A. KOLEKTİF SİBER YAPTIRIMLAR

Benatar ve Gombeer’in ifade ettiği üzere, geleneksel anlamda yaptırım kavramı, BM Güvenlik Konseyi tarafından “*hedef alınan devletin (veya devlet dışı aktörün) uluslararası hukuka uymasını sağlamak ve/veya davranışını ve politi-*

¹⁵ Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).

¹⁶ Daha detaylı bilgi için bkz. Schmitt, ‘Below the Threshold Cyber Operations’ (n 10) 700.

¹⁷ Hans Köchler, ‘Sanctions and International Law’ (2019) 14(3) *International Organisations Research Journal* 27, 28.

¹⁸ Daha detaylı bilgi için bkz. Erdem Denk, *Uluslararası Örgütler Hukuku: Birleşmiş Milletler Sistemi* (Siyasal Kitabevi 2015) 264–270.

¹⁹ BM Şartı Madde 24(1). “*Birleşmiş Milletlerin üyeleri, örgütün hızlı ve etkili hareket etmesini sağlamak için uluslararası barış ve güvenliğin korunmasında başlıca sorumluluğu Güvenlik Konseyine bırakırlar ve bu sorumluluk gereğince grevlerini yerine getirirken Güvenlik Konseyinin kendi adlarına hareket ettiğini kabul ederler*”.

kasını deęiřtirmesi yönünde baskı uygulamak amacıyla kullanılan araçlardır”²⁰. BM Şartı’nın 39. maddesine göre BM Güvenlik Konseyi, “*barışın tehdit edildiğini, bozulduğunu ya da saldırı eylemi olduğunu saptar ve uluslararası barış ve güvenliğin korunması ya da yeniden tesisi için tavsiyelerde bulunur veya 41. ve 42. maddeler uyarınca hangi önlemler alınacağını kararlařtır*”. Bu madde çerçevesinde öncelikle BM Güvenlik Konseyi’nin bir saptama yapması beklenmektedir. BM Şart’ın 41. maddesi silahlı kuvvet kullanımını içermeyen önlemlere yönelik düzenlemeleri ihtiva etmektedir. Buna göre BM Güvenlik Konseyi, ekonomik ilişkilerin ve demir yolu, deniz, hava, posta, telgraf, radyo ve dięer iletişim araçlarının tamamen veya kısmen kesilmesi ve diplomatik ilişkilerin kesilmesi kararı alabilir. 42. madde ise BM Güvenlik Konseyi’nin silahlı kuvvet kullanımını içeren zorlama tedbirler almasını mümkün kılmaktadır. Denk’in de ifade ettięi üzere BM Güvenlik Konseyi hangi tedbiri alacağı hususunda tam bir takdir yetkisine sahiptir²¹. Bu bağlamda BM Güvenlik Konseyi 39. madde çerçevesinde yalnızca saptama da yapabilir, 41. ve 42. maddedeki tedbirleri de uygulayabilir²². Anılan maddeler arasında hiyerarşik bir öncelik söz konusu deęildir. Bu teorik bağlamda ele alınması gereken temel mesele, BM Güvenlik Konseyi tarafından alınabilecek siber yaptırım kararlarının, BM Şartı’nın VII. Bölümü çerçevesinde nasıl bir hukuki deęerlendirmeye tabi tutulabileceğidir.

BM üyesi devletler, uluslararası barış ve güvenliğin korunması konusunda asli yetkiyi BM Güvenlik Konseyine vermektedir. Her ne kadar “siber uzayın” egemenlik alanı bağlamında statüsüne yönelik tartışmalar devam etse de siber saldırıların devletler arasındaki ilişkileri olumsuz etkileyebileceęi büyük ölçüde kabul görmektedir²³. Bu bağlamda BM Güvenlik Konseyi’nin sorumluluğunun “siber uzayda da uluslararası barış ve güvenlięi korumayı” kapsadığı konusunda şüphe yoktur²⁴. Bu kabule dayanarak, BM Güvenlik Konseyi, BM Şartı’nın 39. maddesi kapsamında barışa tehdit, barışın ihlali ya da saldırı eylemi durumunu belirlemesi hâlinde, uluslararası barış ve güvenlięi sağlamak ya da yeniden kurmak amacıyla gerekli gördüğü her türlü önlemi alabilir veya bu tür önlemlerin uygulanmasına izin verebilir²⁵.

²⁰ Marco Benatar and Kristof Gombeer, ‘Cyber Sanctions: Exploring a Blind Spot in the Current Legal Debate’ (ESIL 2011 4th Research Forum, 2011) 2.

²¹ Denk (n 18) 268-269.

²² ibid. 270.

²³ Hisham Eslam and Garima Tiwari, ‘Cyberspace: Reimagining Cybersecurity and Its Impact on State Sovereignty’ in Mohamed Chawki and Ajith Abraham (eds), *Cybercrime Unveiled: Technologies for Analysing Legal Complexity* (Springer 2025) 93-112.

²⁴ Nils Melzer, *Cyberwarfare and International Law* (United Nations Institute for Disarmament Research 2011).

²⁵ ibid.



BM Şartı'nın VII. Bölümü çerçevesinde alınabilecek önlemler bakımından BM Güvenlik Konseyi'nin geniş bir takdir yetkisi olduğunu ifade etmiştik. Bu bağlamda alınacak önlemler 40. madde kapsamında tavsiye niteliğinde olabileceği gibi, ilgili taraflara geçici tedbirlere uymaları çağrısında bulunmak şeklinde de uygulanabilir. BM Güvenlik Konseyi 41. madde çerçevesinde kuvvet kullanımına varmayan “telgraf, radyo ve diğer iletişim araçlarının tamamen veya kısmen kesilmesine” de karar verebilir. Bu noktada dikkat çekilmesi gereken husus, barışı tehdit eden eylemin siber uzayda ortaya çıkıp çıkmadığının önem arz etmemesidir. Zira barışı tehdit eden bir eylem siber uzayda gerçekleşmese dahi, BM Şartı'nın 41. maddesi, BM Güvenlik Konseyi'ne siber yaptırım kararı alabilmesi için açık bir yasal zemin sunmaktadır. Başka bir ifade ile siber saldırılar gibi yeni tehditlere karşı uygulanabilecek yaptırımlar, bu maddeden türetilen bir dayanakla uluslararası hukukun içinde yer alabilir²⁶. Zira madde metninde geçen önlemler arasında “iletişim araçlarının tamamen veya kısmen kesilmesi” düzenlemesi de bulunmaktadır²⁷. Günümüzde bilgisayar teknolojisi ve bu teknolojinin sunduğu çok yönlü uygulamalar, çağdaş dönemin temel iletişim araçlarını teşkil etmektedir²⁸. Zira 41. maddede sayılan önlem listesi tahdidi değildir. Bu durum Eski Yugoslavya Uluslararası Ceza Mahkemesi tarafından görülen *Tadić* davasında da teyit edilmiştir. Mahkemenin kararına göre, 41. maddede öngörülen önlemler yalnızca örnekleme mahiyetinde olup diğer tedbir türlerini dışlamamaktadır²⁹. Bu maddenin tek koşulu, alınacak önlemlerin “kuvvet kullanımını” içermemesidir³⁰. Bu bağlamda 41. maddenin içeriği negatif bir tanımlamaya dayanmaktadır. Yani madde metni hangi önlemlerin alınabileceğini sıralamak ve sınırlamaktan ziyade, hangi tür önlemlerin alınamayacağını düzenlemektedir. Alınabilecek önlemlerin tahdidi olmamasının en önemli göstergelerinden biri, özellikle Soğuk Savaş sonrasında 41. maddede sayılan önlemlerin dışında da alınan yaptırım kararlarıdır. Soğuk Savaş'ın ardından, özellikle devlet dışı aktörlerin uluslararası ilişkilerde daha etkin rol oynamaya başlamasıyla birlikte, listelenen önlemlerin yalnızca devletleri hedef aldığı ve uluslararası ilişkilerin dönüşen yapısı karşısında yetersiz kaldığı fark edilmiştir³¹. Bu nedenle ekonomik, siyasi ve diplomatik yaptırımlar gibi klasik yöntemlere ek olarak, kişisel malvarlıklarının dondurulması, seyahat özgürlüğünün kısıtlanması ve hatta sınır aşan hareketliliğin engellenmesine yönelik yeni araçlara başvurulmaya başlanmıştır³².

²⁶ Benatar and Gombeer (n 20) 11.

²⁷ ibid. 11.

²⁸ ibid. 11.

²⁹ *Prosecutor v Duško Tadić aka “Dule” (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction)* (ICTY, 2 October 1995) para 35.

³⁰ ibid. para 35.

³¹ Denk (n 18) 274.

³² ibid. 274.

42. madde çerçevesinde ise BM Güvenlik Konseyi hava, deniz veya kara kuvvetleriyle kuvvet kullanmaya yönelik her türlü eylemi gerçekleştirebilir. Bu noktada tartışma konusu yaratan olgu ise barışa yönelik tehdidin siber uzayda ortaya çıkması halidir. Melzer, BM Şartı'nın 42. maddenin lafzi yorumundan kuvvet kullanımının yalnızca “hava, deniz ve kara kuvvetleriyle” sınırlıymış gibi gözüktüğünü ifade etmektedir³³. Devamında ise BM Şartı'nın 42. maddenin temel amacının BM Güvenlik Konseyi'nin zorlayıcı tedbirlere başvurma yetkisini sınırlamak değil; aksine, gerektiğinde dönemin önde gelen askerî güçlerinin sahip olduğu tüm silahlı kapasiteyi kapsayacak şekilde bu yetki alanını genişletmek olduğunu ifade etmektedir³⁴. Bu çerçevede, 42. maddeye amaçsal (teleolojik) bir yorumla yaklaşıldığında, BM Güvenlik Konseyi'nin siber uzayda silahlı kuvvet kullanımına yönelik yetkilendirme yapamayacağı yönündeki bir değerlendirme, hükmün ruhuyla ve uluslararası barış ve güvenliğin dinamik nitelikleriyle bağdaşmayacaktır³⁵.

Denk ile benzer şekilde Melzer de BM Güvenlik Konseyi'nin siyasi bir kavram olarak nitelendirdiği “barışa tehdit” kavramı bakımından oldukça geniş bir takdir yetkisine sahip olduğunu ifade etmektedir³⁶. Zira hukuki değerlendirme açısından “barışa tehdit” halinin tespiti, ne mutlaka uluslararası hukuka aykırı bir eylemin gerçekleşmiş olmasını ne de BM Şartı çerçevesinde kuvvet tehdidi, kuvvet kullanımı ya da silahlı bir saldırının vuku bulmuş olmasını zorunlu kılar³⁷. Başka bir ifadeyle barışa tehdit durumu, somut bir ihlalin varlığından bağımsız olarak değerlendirilebilir ve bu durumun tespiti, hukuki olduğu kadar siyasi takdir unsurlarını da içeren bir süreçtir³⁸. Bu bağlamda siber operasyonların da barışı tehdit edip etmediği konusundaki BM Güvenlik Konseyi'nin takdir yetkisi aynı esnekliğe sahiptir. Bu takdir yetkisi çerçevesinde alınabilecek önlemlerin sınırı ise öncelikle BM Şartı'nın amaç ve ilkeleri sonrasında ise uluslararası hukuk ilkelemesine uygunluktur³⁹. Bu ilkeler, BM Şartı'nın 1. maddesinin 3. fıkrası çerçevesinde belirlenebilir. Buna göre BM Güvenlik Konseyi “temel insan hakları hukuku” ve “uluslararası insancıl hukuka” saygı gösterme yükümlülüğü altındadır⁴⁰.

Söz konusu amaç ve ilkeler ilerleyen yıllarda kabul edilen insan hakları sözleşmeleri vasıtasıyla somutlaştırılmış ve uygulamaya geçirilmiştir. Bu çerçevede, BM'nin dolayısıyla BM Güvenlik Konseyi'nin, bu normatif çerçeveyi koruma

³³ Melzer (n 24).

³⁴ ibid.

³⁵ ibid.

³⁶ ibid.

³⁷ ibid.

³⁸ ibid.

³⁹ ibid.

⁴⁰ BM Şartı, m.1(3).



yükümlülüğü hukuken kabul edilen bir sorumluluk alanı olarak değerlendirilmiştir⁴¹. İkinci en temel ve genel sınırlamanın uluslararası hukukun emredici normlarından (*jus cogens*) kaynaklandığını söylemek mümkündür. Sonuç olarak bu hukuki sınırlar çerçevesinde BM'nin siber yaptırım kararı alması mümkündür. Ancak, özellikle internet bağlantılı yaptırımların “insan hakları” ihlali sınırlamasına takılma olasılığının oldukça yüksek olduğunu vurgulamak önemlidir.

BM İnsan Hakları Konseyi, 27 Haziran 2016 tarihli kararında internetin “ifade özgürlüğü” kapsamında bir insan hakkı olarak tanınması gerektiği yönünde bir karar almıştır. Bu kararda, internetin ifade özgürlüğü, bilgiye erişim ve katılım hakları gibi temel insan haklarıyla bağlantılı olduğu vurgulanmıştır⁴². İnternetin henüz yaygın olmadığı dönemlerde bile BM Güvenlik Konseyi, iletişimin kesilmesine yönelik yaptırım kararlarının insan hakları üzerindeki etkilerine dikkat çekmiştir. Örneğin BM Güvenlik Konseyi tarafından 1968 yılında Güney Rodezya'ya karşı alınan yaptırım kararlarının kapsamı oldukça geniş tutulmuş fakat ırkçı ayrımcılık (apartheid) tarzı rejimin posta, telgraf ve radyo iletişimini kesilmesine yönelik herhangi yaptırım kararı almamıştır⁴³. Bu durumun temel gerekçesi ise bu tür kesintilerin iletişim özgürlüğü ve temel insani ihtiyaçlar açısından fazla sert olacağı yönündeki kanaattir⁴⁴.

Yine 1993 yılında Boşnak Sırlara yönelik olarak kabul edilen yaptırım kararları da bu bağlamda önemlidir. Zira BM Güvenlik Konseyi'nin 820 sayılı Kararı, birçok yaptırım kararı almasına rağmen özellikle telekomünikasyon alanındaki bazı yaptırımları doğrudan istisna olarak düzenlemiştir. Karara göre “*Federal Yugoslavya Cumhuriyeti'nde (Sırbistan ve Karadağ) yürütülen herhangi bir iş için hizmet sunumunu, finansal ve finansal olmayan hizmetler dahil olmak üzere, yasaklamayı kararlaştırır. Ancak, bu yasağın istisnaları, iletişim, posta hizmetleri, hukuki hizmetler (1992 tarihli 757 sayılı Karar ile uyumlu) ve 724 sayılı karar ile kurulmuş Komite tarafından her bir vaka için onaylanan, insani veya diğer istisnai amaçlar için gerekli olabilecek hizmetler olacaktır*”⁴⁵. Ancak BM Güvenlik Konseyi, 21 Nisan 1995 tarihli ve 988 sayılı Kararı ile özellikle telekomünikasyon bağlantılarının kesilmesi konusunda teşvik edici nitelikte bir karar almıştır⁴⁶. Bu karar göre “*1994 yılı Ağustos ayında uygulamaya koydukları, Bosna-Hersek Cumhuriyeti'nin Bosnalı Sırp güçlerinin kontrolü altındaki bölgeleri ile Yugoslavya Federal Cumhuriyeti (Sırbistan ve Karadağ) arasın-*

⁴¹ Benatar and Gombeer (n 20) 16.

⁴² United Nations Human Rights Council, ‘The Promotion, Protection and Enjoyment of Human Rights on the Internet’ UN Doc A/HRC/32/L.20 (27 June 2016).

⁴³ United Nations Security Council, ‘Resolution 253 (1968)’ (29 May 1968) UN Doc S/RES/253. United Nations Security Council, ‘Resolution 277 (1970)’ (18 March 1970) UN Doc S/RES/277.

⁴⁴ Benatar and Gombeer (n 20) 11–12.

⁴⁵ United Nations Security Council, ‘Resolution 253 (1968)’ (29 May 1968) UN Doc S/RES/253.

⁴⁶ Benatar and Gombeer (n 20) 11–12.

daki uluslararası telekomünikasyon bağlantılarının kesilmesi kararını yeniden yürürlüğe koymaları konusunda Yugoslavya Federal Cumhuriyeti (Sırbistan ve Karadağ) yetkililerini teşvik eder”⁴⁷.

Benatar ve Gombeer siber yaptırımlara yönelik en çarpıcı örneğin UNITA (Angola’nın Tam Bağımsızlığı için Milli Birlik)⁴⁸ harekâtına yönelik olduğunu ifade etmektedir⁴⁹. Kanaatimizce, BM Güvenlik Konseyi, siber yaptırımlar konusunda temkinli bir tutum sergilemektedir. Zira incelediğimiz üç örnekte de doğrudan BM Güvenlik Konseyi kararları üzerinden değil, kurulan yaptırım komitelerinin tavsiyeleri üzerinden siber yaptırımlara dikkat çekilmektedir. UNITA örneğinde, siber yaptırımlara ilişkin ilk yönlendirmeler, doğrudan BM Güvenlik Konseyi tarafından değil, UNITA’ya yönelik yaptırımların uygulanmasını izlemekle görevli Yaptırımlar İzleme Komitesi’nin 2001 tarihli raporunda yer alan tavsiye kararları ile gündeme gelmiştir. BM Güvenlik Konseyi’nin 864 sayılı Kararı doğrultusunda kurulan BM Güvenlik Konseyi Angola Yaptırımlar Komitesi’nin⁵⁰ 2001 tarihli raporuna göre UNITA, siber teknolojiyi propaganda aracı olarak etkin şekilde kullanmakta; özellikle internet siteleri ve e-posta yoluyla yasa dışı faaliyetlerini duyurarak dijital alanda görünürliğini artırmaktadır⁵¹. Zira UNITA kwacha.org ve kwacha.com gibi siteler üzerinden, barış ya da diyalog çağrısı yapmak yerine, gerilla eylemlerine dair bilgiler paylaşılmakta; bu içerikler sık sık güncellenerek siber ortamda psikolojik savaş unsuru haline getirilmektedir. Komite’nin raporuna göre “UNITA’nın internete verdiği önem küçümsenemez. Bu teknoloji, grubun kendini ayakta tutmak ve Birleşmiş Milletler Güvenlik Konseyi yaptırımlarının devamına karşı mücadele etmek için en güçlü araçlarından biri olduğu açıkça görülmektedir”⁵².

Yaptırımları izleme komitelerinin tavsiyelerinde de görüldüğü üzere BM Güvenlik Konseyi’nin bilgi ve iletişim teknolojileri bağlamında yeni nesil önlemler alma yetkisi, alabileceği önlemlerin tahdidi olmaması nedeniyle mümkündür. Bu doğrultuda, BM Güvenlik Konseyi tarafından çeşitli yenilikçi siber önlemler hayata geçirilebilir. Örneğin, belirli bir devletin kamu kurumlarına veya siber saldırılardan sorumlu yapılarına yönelik internet trafiğinin engellenmesi yoluyla bir siber

⁴⁷ United Nations Security Council, ‘Resolution 988 (1995)’ (21 April 1995) UN Doc S/RES/988, para 10.

⁴⁸ UNITA’nın amacı ve faaliyetleri için bkz. Mürsel Bayram, ‘Angola İç Savaşının Ana Aktörleri ve Uluslararası Ramifikasyonları’ (2016) 6(15) *Ordu Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Araştırmaları Dergisi* 365–383.

⁴⁹ Benatar and Gombeer (n 20) 11–12.

⁵⁰ United Nations Security Council, ‘Resolution 864 (1993)’ (15 September 1993) UN Doc S/RES/864.

⁵¹ United Nations Security Council, *Letter dated 12 October 2001 from the Chairman of the Security Council Committee established pursuant to resolution 864 (1993) concerning the situation in Angola addressed to the President of the Security Council* (12 October 2001) UN Doc S/2001/966.

⁵² *ibid.* 15.



abluka uygulanabilir⁵³. Benzer şekilde, devlet destekli propaganda faaliyetleri yürüten ya da siber saldırılar gerçekleştiren web sitelerinin uluslararası erişiminin kısıtlanması suretiyle alan adı (domain) engellemeleri yapılabilir⁵⁴. Ayrıca, ilgili devlete ait ya da onunla bağlantılı İnternet Protokolü (IP) adres bloklarının küresel iletişim altyapısından dışlanması şeklinde IP yasakları da bir başka önlem olarak gündeme gelebilir⁵⁵. Bu tür yaptırımlar, siber saldırıların yayılma kapasitesini önemli ölçüde sınırlayabilir. Yine BM Güvenlik Konseyi'nin siber saldırılarda kullanılan finansman kanallarının kesilmesi amacıyla kripto cüzdanlara erişimin engellenmesi, yani kripto varlıklara yönelik kısıtlamalar uygulaması da mümkündür. Bu tür önlemler, siber tehdit aktörlerinin finansal hareket kabiliyetini azaltarak saldırıların önlenmesine veya caydırılmasına katkı sağlayabilir.

Bu örnekler bağlamında tartışılacak en güncel olaylardan biri BM Güvenlik Konseyi'nin 2006 yılında 1718 sayılı Karar ile Kuzey Kore Demokratik Halk Cumhuriyeti'ne yönelik aldığı yaptırım kararlarıdır. Alınan yaptırım kararlarının hedefi Kuzey Kore Demokratik Halk Cumhuriyeti'nin nükleer denemeler yapmasını veya balistik füze fırlatmasını engellemektir⁵⁶. Bu amaç doğrultusunda nükleer ve balistik füze programlarına dahil olan bireylere yönelik silah ambarları, mal varlıklarının dondurulması ve seyahat yasakları bulunmaktadır⁵⁷. Ayrıca önemle belirtmek gerekir ki yaptırımlar Kuzey Kore'ye nükleer, balistik füze ve diğer kitle imha silahları programlarıyla ilgili malzeme tedarikini, satışını veya transferini yasaklamaktadır⁵⁸. 1718 sayılı Karar doğrudan siber yaptırımları da kapsamaktadır.

⁵³ Abluka hukukunun siber bağlamda uygulanıp uygulanamayacağı ve uygulanacaksa hangi ölçüde uygulanabileceği sorusu Tallinn El Kitabı 2.0'da yoğun tartışmalara sebebiyet vermiştir. Abluka, savaş yöntemi olarak kullanılan ve belirli limanlara, havaalanlarına veya düşman bir devletin mülkiyetinde, işgali altında ya da kontrolü altındaki kıyı bölgelerine tüm gemi ve hava araçlarının (hem düşman hem de tarafsız; tarafsız olanlarla ilgili olarak) girişini veya çıkışını engellemeye yönelik saldırgan hareketleri kapsar. Siber abluka tartışmaları için bkz. Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017). ch 9, 504–11.

⁵⁴ Alan adı engellemeleri için bkz. Špaček S, Laštovička M, Horák M and Plesník T, 'Current Issues of Malicious Domains Blocking' in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (IEEE 2019) 551–56. Domain (alan adı), internet dünyasında bir web sitesinin kimliği ve adresi olarak işlev görür. Alan adı kullanıcıların tarayıcıya yalnızca harf, sayı ve sembollerden oluşan bu ismi yazarak ilgili siteye erişmesini sağlar. Kısaca domain, sitelerin internet üzerindeki görünür yüzü ve kullanıcıların ilgili siteyi bulmasını sağlayan dijital adres. Domain Nedir, <<https://www.turk.net/internet-hiz-altyapi-sorgulama>> E.T. 06.05.2025.

⁵⁵ IP (İnternet Protokolü) adresi, internete ya da yerel ağa bağlı her cihaza verilen benzersiz sayısal etikettir; cihazların birbirleriyle iletişim kurmasını ve veri alışverişini sağlar. What Is An IP Address? How Does It Work? <[https://www.fortinet.com/resources/cyberglossary/what-is-ip-address#:~:text=An%20Internet%20Protocol%20\(IP\)%20address,use%20the%20internet%20to%20communicate](https://www.fortinet.com/resources/cyberglossary/what-is-ip-address#:~:text=An%20Internet%20Protocol%20(IP)%20address,use%20the%20internet%20to%20communicate)> E.T.05.02.2025.

⁵⁶ United Nations Security Council, 'Resolution 1718 (2006)' (14 October 2006) UN Doc S/RES/1718 (2006).

⁵⁷ ibid.

⁵⁸ ibid.

rım ibaresini kullanmamasına rağmen 2019 Uzmanlar Paneli'nin (2019 Panel of Experts) 2019 yılı ara raporu, Kuzey Kore Demokratik Halk Cumhuriyeti'nin giderek daha karmaşık hale gelen siber saldırılarla finansal kurumlardan ve kripto para borsalarından yasa dışı fon transferleri gerçekleştirdiğini ve çalınan gelirleri aklarak finansal yaptırımlardan kaçmaya çalıştığını tespit etmiştir⁵⁹. Rapora göre kripto para borsalarına yapılan büyük ölçekli saldırılar, Kuzey Kore Demokratik Halk Cumhuriyeti'ne, geleneksel bankacılık sektörüne göre daha az denetim ve izlenebilirlik ile gelir elde etme imkânı sağlamaktadır⁶⁰. Bu siber faaliyetler, ülkenin kitle imha silahları programları için finansman sağlamaktadır ve bu faaliyetlerin toplam gelirinin 2 milyar dolara kadar ulaşabileceği tahmin edilmektedir⁶¹. 2019 Uzmanlar Paneli, bu yasa dışı siber faaliyetlerin önlenmesi amacıyla yaptırım kararlarının genişletilmesini tavsiye etmektedir. Ancak, bu örnekte de diğer örneklerde olduğu gibi siber yaptırım tavsiyesi yine yaptırım komitesinden gelmektedir.

Sonuç olarak BM Güvenlik Konseyi'nin doğrudan siber yaptırım kararı aldığını söylemek henüz mümkün değildir. Ancak, BM Güvenlik Konseyi bazı kararlarında siber faaliyetleri dolaylı olarak ele almakta ve özellikle terörizmin finansmanı ve kritik altyapılara yönelik tehditler bağlamında bilgi ve iletişim teknolojilerinin kötüye kullanımını kınamaktadır. Örneğin, BM Güvenlik Konseyi 12 Şubat 2015 tarihli 2199 Sayılı kararında “*Küreselleşen bir toplumda teröristlerin ve destekçilerinin, özellikle internet olmak üzere, yeni bilgi ve iletişim teknolojilerini terör eylemlerini kolaylaştırmak amacıyla artan biçimde kullanmalarından; ayrıca bu teknolojileri terör eylemlerini teşvik etmek, üye toplamak, finansman sağlamak veya planlamak için kullanmalarından*” duyulan endişeyi açıklamaktadır⁶².

Yine BM Güvenlik Konseyi 13 Şubat 2017 tarihli 2341 Sayılı kararında da doğrudan “siber saldırı” kavramını kullanmamakta ancak devletlerin kritik alt yapılarının terör saldırılarına karşı korunması gerekliliğine dikkat çekmektedir⁶³. Kararda, “*Her devletin, kendi kritik altyapısının neyi kapsadığını ve bu altyapıyı terör saldırılarına karşı nasıl etkin bir şekilde koruyacağını belirleme yetkisine sahip olduğunu kabul ederek, kritik altyapının güvenilirliğinin ve dayanıklılığının sağlanmasının ve terör saldırılarına karşı korunmasının, ilgili devletlerin ulusal güvenliği, kamu güvenliği, ekonomisi ile halkının refahı ve esenliği açı-*

⁵⁹ United Nations Security Council, *Letter dated 27 August 2019 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council* (30 August 2019) UN Doc S/2019/691.

⁶⁰ ibid.

⁶¹ ibid.

⁶² United Nations Security Council, ‘Resolution 2199 (2015)’ (12 February 2015) UN Doc S/RES/2199 (2015).

⁶³ United Nations Security Council, ‘Resolution 2341 (2017)’ (13 February 2017) UN Doc S/RES/2341 (2017).



sından giderek artan önemini kabul eder” ifadesine yer verilmektedir⁶⁴. Dijitalleşmenin ulaştığı düzey göz önünde bulundurulduğunda, günümüz koşullarında bilgi ve iletişim teknolojilerine yönelik saldırıların da kritik altyapı kapsamında değerlendirilmesi bir zorunluluk hâline gelmiştir. Bu bağlamda siber saldırılar kritik altyapılara yönelik tehditler arasında değerlendirilmelidir. Schmitt’in de ifade ettiği üzere ülkesel egemenlik, devletin topraklarında bulunan siber altyapıyı (bu altyapının kamuya ait olup olmamasından bağımsız olarak) koruma altına alır⁶⁵. Dolayısıyla başka bir devletin topraklarında bulunan siber altyapıya yönelik düşmanca siber operasyonlar, özellikle fiziksel zarar veya yaralanmaya neden olduklarında, ilgili devletin egemenliğinin ihlali anlamına gelir⁶⁶. Nitekim Birinci Tallinn El Kitabına göre zararın meydana gelmesi, bir siber operasyonun devlet sorumluluğu hukuku uyarınca uluslararası hukuka aykırı bir fiil olarak nitelendirilmesi için ön koşul değildir⁶⁷. Bu bağlamda bir devletin egemenliği altındaki bir platformda bulunan siber altyapıya müdahale edilmesi, platformun fiziksel olarak nerede bulunduğuna bakılmaksızın ilgili devletin egemenliğinin ihlali sayılabilir⁶⁸.

Sonuç olarak BM’nin siber alana yönelik çalışmalarında da yalnızca genel tanımlar yapıldığı, sorunların tespitine odaklanıldığı ve üye devletler arasında koordinasyonun sağlanmasına yönelik teşvikin ön planda tutulduğu görülmektedir⁶⁹. Ancak, BM’nin siber alana yönelik olarak hem bağlayıcı normatif düzenlemeler hem de bağlayıcı yaptırım kararları aldığı yönünde bir değerlendirme yapmak şu aşamada mümkün değildir. Kanaatimizce bunun başlıca nedeni, siber yaptırımların potansiyel olarak insan hakları ihlallerine yol açabilmesidir. Bu nedenle siber yaptırımların etkinliği ve meşruiyeti, insan haklarına saygı gösterilmesi bağlamında dikkatlice değerlendirilmelidir⁷⁰.

B. TEK TARAFLI SİBER YAPTIRIMLAR

Tek taraflı yaptırımların insan haklarından yararlanılmasına olumsuz etkileri üzerine çalışan BM Özel Raportörü Idriss Jazairy, tek taraflı yaptırımları “*Devletler veya devlet grupları tarafından, başka bir devleti egemen yetkilerini kullanma konusunda boyun eğmeye zorlamak ve bu yolla belirli bir politika değişikliği*

⁶⁴ ibid.

⁶⁵ Schmitt, ‘Below the Threshold Cyber Operations’ (n 10) 704.

⁶⁶ ibid. 704-705.

⁶⁷ Schmitt (ed), *Tallinn Manual on the International Law* (n 15) 30.

⁶⁸ Schmitt (ed), *Tallinn Manual on the International Law* (n 15) Kural 4.

⁶⁹ İbrahim Akdağ, *Birleşmiş Milletler Tarafından Gerçekleştirilen Silahsızlanma Çalışmaları ve Türkiye’nin Bu Çalışmalara Yaklaşımı* (Master’s thesis, Sosyal Bilimler Enstitüsü 2014) 523.

⁷⁰ Siber yaptırımlar bağlamında insan hakları ve insancıl hukuk ihlalleri konusu oldukça kapsamlıdır ve ayrıntılı bir inceleme gerektirir. Çalışmanın odak noktası olan hukuki çerçeveye odaklanmak amacıyla söz konusu potansiyel ihlaller bu çalışma kapsamında ele alınmamıştır.

*sağlamak amacıyla uygulanan -başta ekonomik ve siyasi nitelikte olanlar olmak üzere- çeşitli önlemler*⁷¹ şeklinde tanımlanmıştır. Tek taraflı siber yaptırımlar ise genellikle varlıkların dondurulması, yaptırım uygulanan kişi ve/veya kuruluşlarla ekonomik ilişkilerin kısıtlanması ve seyahat yasaklarını içerir⁷². Rusinova ve Martynova yaptırımların esas itibarıyla ekonomik veya finansal nitelikte olduğunu ifade etmektedir⁷³. Ancak tek taraflı yaptırımların ekonomik nitelikleri, yaptırımların arkasındaki siyasi motivasyonun göz ardı edilebileceği anlamına gelmemektedir⁷⁴. Bu nedenle yaptırımların sadece ekonomik bir olgu olarak değerlendirilmesi mümkün değildir.

Tek taraflı siber yaptırımlar *“siber saldırıları gerçekleştiren veya kolaylaştıran bireylere, tüzel kişilere ve devlet organlarına karşı uygulanan kısıtlayıcı -geçici-ekonomik önlemler”* olarak tanımlanmaktadır⁷⁵. Bu bağlamda siber yaptırımlar; mülk ve mülkiyet haklarının dondurulması, seyahat yasakları ve hedeflenen kişi veya kuruluşlara yapılan ve onlardan alınan bağışların tamamen yasaklanması şeklinde tezahür ettiği söylenebilir⁷⁶. Tek taraflı siber yaptırımlar bireylere, tüzel kişilere, devlet organlarına ve aynı zamanda siber saldırıların faili olduğu iddia edilen kişilere destek veya yardım sağlayan herkese yönelik uygulanabilmektedir⁷⁷. Ayrıca bireysel uygulanan yaptırımların özellikle hükümetle çalışan ya da hükümetle güçlü bağları olan özel aktörlere de uygulanmasının temel amacı, devlet yetkililerinin karar alma süreçlerini etkilemektir⁷⁸.

Ancak siber yaptırımlar da dahil olmak üzere tek taraflı yaptırımların bağlayıcı nitelikte bir hukuki zemininin bulunmaması, siber yaptırımların uygulama alanlarının ve hedef alınan kişilerin kontrolsüz bir şekilde genişletilmesine yol açabilmektedir. Zira çok taraflı yaptırımların aksine tek taraflı yaptırımlar BM kararı veya onayına tabi değildir. Başka bir ifade ile tek taraflı yaptırımlar herhangi bir bölgesel ya da uluslararası örgütün önceden onayına gerek duyulmaksızın devletlerin kendi iç hukuklarına dayanarak yürürlüğe konulmaktadır⁷⁹. Bu durumun tek taraflı yaptırımlar bakımından bir meşruiyet sorunu yarattığı ifade edilebilir.

⁷¹ Birleşmiş Milletler İnsan Hakları Konseyi, *Report of the Special Rapporteur on the Negative Impact of Unilateral Coercive Measures on the Enjoyment of Human Rights*, Idriss Jazairy, UN Doc A/HRC/30/45 (10 August 2015) para 13.

⁷² Bogdanova and Callo-Muller, ‘Unilateral Cyber Sanctions’ (n 12) 914.

⁷³ Rusinova and Martynova (n 12) 139.

⁷⁴ ibid. 139.

⁷⁵ Bogdanova and Callo-Muller, ‘Unilateral Cyber Sanctions’ (n 12) 912.

⁷⁶ ibid. 926.

⁷⁷ ibid. 913-914.

⁷⁸ Rusinova and Martynova (n 12) 139.

⁷⁹ Örneğin “ABD’nin Hasımlarıyla Yaptırımlar Yoluyla Mücadele Etme Yasası” (Countering America’s Adversaries Through Sanctions Act- CAATSA) 2 Ağustos 2017’de yürürlüğe giren federal bir yasadır. Düzenlemenin amacı ABD’nin ulusal güvenliğine tehdit oluşturduğu kabul edilen İran, Kuzey Kore ve Rusya gibi ülkelere karşı yaptırımlar uygulanmasıdır. Detaylı bilgi için bkz. Elvan



Ancak yukarıda da ifade ettiğimiz üzere tek taraflı yaptırımların uygulanması devletlerin sorumluluğu mekanizması çerçevesinde gerçekleştirilmektedir. Günümüz itibarıyla karşı önlem alınabilmesinin bazı temel koşulları bulunmaktadır⁸⁰. Bu temel koşulların yerine getirilmesi karşı önlemlerin uluslararası hukuk çerçevesinde meşru sayılmasına olanak sağlayacaktır. Zira Uluslararası Adalet Divanı'nın *Gabčíkovo-Nagymaros Project* kararında da teyit ettiği üzere, bir devletin başka bir devletin uluslararası hukuka aykırı fiiline karşılık olarak aldığı karşı önlemler, başlı başına hukuka aykırı fiiller olarak değerlendirilmez; belirli koşullara uyulduğu sürece, meşru bir *self-help* aracı olarak kabul edilebilir⁸¹. Sonraki bölümde bu koşullar siber karşı önlemler çerçevesinde incelenecektir.

1. Siber Karşı Önlemler

Karşı önlemler, uluslararası bir yükümlülüğü ihlal eden devleti, bu ihlali durdurmaya ve/veya telafi etmeye zorlamak amacıyla başvurulun araçlardır⁸². Bu amaca ulaşmak için zarar gören devlet, sorumlu devlete karşı bir yaptırım aracı olarak yükümlülüğünü ihlal eder⁸³. Uluslararası hukuk bakımından değerlendirildiğinde devletlerin siber operasyonlara karşı aldıkları yaptırım kararları iki şekilde ortaya çıkabilir. Genel olarak “karşı önlem” şeklinde ifade edilen yaptırım türünün ilki zararlar karşılık (counter measures) diğeri ise misillemedir (retorsion)⁸⁴. Zarar-

Çekişler, ‘Uluslararası Hukukta İkincil Yaptırımlar Açısından Amerika’nın Hasımlarıyla Mücadele Yasası’ (2021) 18(69) *Uluslararası İlişkiler Dergisi* 71.

⁸⁰ Hüseyin Pazarıcı, *Uluslararası Hukuk* (Gözden geçirilmiş 21. baskı, Turhan Kitabevi 2022) 472–473.

⁸¹ *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)*, Judgment, ICJ Reports 1997, 7. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, Merits, Judgment, ICJ Reports 1986, 127, para 249. Ayrıca bkz. Evans, *International Law* (n 13) Part V, 469.

⁸² Talita Dias, *Countermeasures in International Law and Their Role in Cyberspace* (Research Paper, International Law Programme, May 2024) 18.

⁸³ İbid. 18.

⁸⁴ Misilleme herhangi bir uluslararası yükümlülükle çelişmeyen, fakat dostane olmayan bir eyleme karşılık olarak yapılan dostane olmayan bir eylem olarak tanımlanabilir. Başka bir ifade ile “*bir devletin başka bir devletin hukuka aykırı olmayan ancak çıkarlarını zedeleyen davranışına karşı uluslararası hukukun yasaklamadığı yollarla karşılık vermesi*” olarak tanımlanabilir (Pazarıcı (n 80) 470). Bu bağlamda misillemenin temel koşulu gerçekleştirilen karşı eylemin uluslararası hukuka uygun olmasıdır. Uluslararası hukuk çerçevesinde meşru bir misillemenin uygulanabilmesi için, bu tedbirin muhatap devletin tanınmış haklarını değil, yalnızca hukuken korunan menfaatlerini (çıkartlarını) hedef alması gerektiği ifade edilmelidir (Pazarıcı (n 80) 470). Uluslararası Hukuk Komisyonu (International Law Commission), *Articles on Responsibility of States for Internationally Wrongful Acts*, 2001, Madde 49-54). Misillemenin, dostane olmayan bir siber saldırıya karşılık olarak yapıldığı varsayıldığından, hedef alınan siber operasyonun uluslararası hukuku ihlal ettiğinin ayrıca tespit edilmesine gerek bulunmamaktadır. Zira ifade ettiğimiz üzere misilleme en fazla dostane olmayan eylemler olarak kabul edilir. Bu bağlamda bu tür eylemler, “hukuki değil, sadece siyasi veya ahlaki anlamda yanlış olan ya da basitçe bir nezaketsizlik niteliği taşıyan davranışlardır” (Thomas Giegerich, ‘Retorsion’, *Max Planck Encyclopedia of Public International Law* (online edn, Oxford University Press 2021– <<https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e983?prd=MPIL>> E.T. 15.01.2025). Bu tür eylemler, hedef devletin ilk eylemi ister uluslararası hukukun açık bir ihlalini teşkil etsin, ister yalnızca diplomatik teamüllere aykırı

la karşılık veya karşı önlem, zarara uğramış bir devletin, hukuka aykırı eylemi gerçekleştiren devleti, yükümlülüklerine uymaya ikna etmek amacıyla aldığı bir tedbirdir⁸⁵. Pazarcı da “zararla karşılığı bir devletin uluslararası hukuka aykırı bir fiili nedeniyle zarar gören bir başka devletin birinci devletin hukuka uygun davranmasını sağlamak amacıyla uluslararası hukuka aykırı yollarla karşılık vermesi” olarak tanımlamaktadır⁸⁶.

Uluslararası Hukuka Aykırı Fiillerden Dolayı Devletlerin Sorumluluğuna İlişkin Taslak Maddeler’in 1. maddesine göre “Bir devletin her türlü uluslararası hukuka aykırı fiili, o devletin uluslararası sorumluluğunu doğurur”. Buna göre, ilk koşul, karşı önlemlerin yalnızca uluslararası hukuka aykırı bir fiile tepki olarak uygulanabilmesidir. Taslak Maddeler’in 2. maddesine göre ise uluslararası hukuka aykırı fiilin, uluslararası hukuk bakımından ilgili devlete atfedilebilir olması gerekir. Buna göre karşı önlem yalnızca hukuka aykırı fiili gerçekleştiren ve eylem kendisine atfedilebilen devlete karşı uygulanabilecektir. Başka bir ifade ile karşı önlemin “üçüncü devletleri” etkilememesi şarttır. Taslak Maddeler’in 3. maddesi uyarınca, bir devlet fiilinin uluslararası hukuka aykırı sayılıp sayılmayacağı, uluslararası hukuk kuralları çerçevesinde belirlenir. Karşı önlemlere ilişkin üçüncü koşul ise alınan önlemin orantılılık ilkesine uygun olmasıdır. Dördüncü koşul ise karşı önlemin kuvvet kullanmayı içermemesi şarttır⁸⁷.

Uluslararası mahkemeler ve yargı organları da karşı önlemlerin tabi olduğu çeşitli koşulları belirlemiştir. Bunlar arasında uluslararası hukukun daha önce ihlal edilmiş olması, ihlalin durdurulması ve/veya telafi edilmesi için önceden bir talepte bulunulması gerekliliği, ihtilafın çözümü için protesto ve çözüm tek-lifini içeren bir bildirimde bulunulması, orantılılık, gereklilik (zorunluluk), geri alınabilirlik ve geçicilik gibi şartlar yer almaktadır⁸⁸. Bu koşullar ışığında siber

veya dostane olmayan bir nitelik taşısın, genellikle misilleme kapsamında değerlendirilir (ibid). Bu çerçevede, misilleme niteliğindeki önlemler genellikle, muhatap devletin eyleminin açık bir hukuki ihlal teşkil etmesinden ziyade, söz konusu eylemin siyasi, diplomatik veya ahlaki düzlemde uygunsuz ya da arzu edilmeyen olarak değerlendirilmesine dayalı olarak uygulanmaktadır (ibid). Bu doğrultuda, misilleme önlemleri yalnızca bağlayıcı nitelikteki uluslararası hukuk normlarının (hard law) ihlali durumunda değil; aynı zamanda bağlayıcılığı bulunmayan düzenlemelerin (soft law), centilmenlik anlaşmaları olarak bilinen gayriresmî mutabakatların, siyasi nitelikteki beyan ve taahhütlerin ya da uluslararası nezaket ve karşılıklı saygı ilkelerinin ihlaline karşılık olarak da başvurulabilecek araçlar arasında yer almaktadır (ibid). Bu bağlamda, bazı siber yaptırım türleri misilleme kapsamında değerlendirilebilir. Dolayısıyla, bu yaptırımlar yaptırım uygulayan devletin uluslararası yükümlülüklerini ihlal etmemektedir. (Bogdanova and Callo-Muller, ‘Unilateral Cyber Sanctions’ (n 12) 941.)

⁸⁵ UNGA Res 56/83, *Articles on Responsibility of States for Internationally Wrongful Acts* (12 December 2001) UN Doc A/RES/56/83 (ARSIWA) Article 49(1).

⁸⁶ Pazarcı (n 80) 472.

⁸⁷ ibid. 472-473.

⁸⁸ *Responsabilité de l’Allemagne à raison des dommages causés dans les colonies portugaises du sud de l’Afrique (Portugal v Germany)*, 1928, 2 Reports of International Arbitral Awards (RIAA) 1011 (‘Naulilaa’) 1026-7. *Gabčíkovo-Nagymaros Project (Hungary/Slovakia)*, *Judgment*, International



yaptırımların bir “karşı önlem” olarak değerlendirilip değerlendirilemeyeceğinin analiz edilmesi gerekmektedir.

a. Uluslararası Hukuku İhlal Eden Bir Eylemin Varlığı

Yukarıda da ifade ettiğimiz üzere siber yaptırımların karşı önlem olarak meşru sayılabilesinin ilk koşulu, hedef alınan devletin daha önce uluslararası hukuk normunu ihlal eden bir eyleminin bulunmasıdır. Bu bağlamda açıklığa kavuşturulması gereken husus uluslararası hukuka aykırı eylemin nasıl tespit edileceğidir. Uluslararası Adalet Divanı Statüsü’nün 38. maddesine göre uluslararası hukukun asıl kaynakları: andlaşmalar, yapılageliş (teamül) kuralları başka bir ifade ile örf ve âdet hukuku normları ve son olarak hukukun genel ilkeleridir⁸⁹. Bu bağlamda, bir uluslararası hukuk ihlalden söz edilebilmesi için, öncelikle birincil kaynakların ihlali söz konusu olmalıdır. Diğer bir deyişle, bu tür ihlaller, bir devletin ya bir andlaşma kapsamındaki yükümlülüklerini ya da uluslararası örf ve âdet hukuku kuralını ihlal etmesi suretiyle meydana gelebilir⁹⁰. Bu bağlamda bir devlete yönelik siber operasyonların, yalnızca o devletin münhasır yetki alanına giren konularda onu etkilemekle sınırlı kalmayıp zorlayıcı bir nitelik kazanması, müdahale etmeme ilkesinin ihlali anlamına gelir. Böyle bir durum, uluslararası hukuk bakımından bir haksız fiil teşkil eder⁹¹. Haksız fiil sayılmasının bir sonucu olarak karşı önlem alabilmenin ilk koşulu gerçekleşmiş olur.

Ancak günümüzde devletlerin siber alandaki davranışlarını düzenleyen “bağlayıcı” veya katı hukuk sayılan uluslararası hukuk düzenlemeleri henüz mevcut değildir⁹². Siber alana ilişkin temel başvuru metinlerinden biri Tallinn El Kitabı 2.0’dır; ancak bu eser yumuşak hukuk (soft law) niteliğinde olduğundan devletler açısından bağlayıcı değildir. Tallinn El Kitabı’nın kendisi de resmi bir belge olmadığını ve herhangi bir kurum ya da kuruluşun görüşlerini yansıtmadığını ifade etmektedir⁹³. Bu bağlamda karşı önlemin temel koşulu olan uluslararası hukukun ihlalinin varlığı sorgulanabilir mahiyettedir⁹⁴. Tallinn El Kitabı’nın 2.0’nın 14. Kuralına göre “*Bir devlet, kendisine atfedilebilen ve uluslararası hukuki bir*

Court of Justice (ICJ), ICJ Reports 1997, 7, paras 84 and 87. *Air Services Agreement of 27 March 1946 (United States v France)*, Decision of the Arbitral Tribunal, 9 UN Reports of International Arbitral Awards (RIAA) 415 (1978), paras 83, 90, 91. *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)*, Judgment, International Court of Justice (ICJ), ICJ Reports 1986, 14, para 249. World Trade Organization (WTO), *European Communities – Regime for the Importation, Sale and Distribution of Bananas*, Recourse to Arbitration by the European Communities under Article 22.6 of the DSU, Decision by the Arbitrators, WT/DS27/ARB, 9 April 1999, paras 6.3–6.5. Ayrıca bkz. Dias (n 82).

⁸⁹ Daha detaylı bilgi için bkz. Pazarcı (n 80) 39.

⁹⁰ Schmitt, “Below the Threshold Cyber Operations” (n 10) 704.

⁹¹ ibid. 705.

⁹² Bogdanova and Callo-Muller, ‘Unilateral Cyber Sanctions’ (n 12) 942.

⁹³ Schmitt (ed), *Tallinn Manual 2.0* (n 53).

⁹⁴ Bogdanova and Callo-Muller, ‘Unilateral Cyber Sanctions’ (n 12) 942.

yükümlülüğün ihlalini oluşturan siber bağlantılı bir eylem nedeniyle uluslararası sorumluluk taşır”⁹⁵. Düzenleme açık bir hüküm getirmesine rağmen bağlayıcı olmaması nedeniyle tartışmaya açıktır.

b. Karşı Önlemler ve Eylemin Devlete Atfedilebilir Olması

Karşı önlemler açısından önem taşıyan bir diğer koşul, eylemin devlete atfedilebilir olmasıdır. Siber alana yönelik bağlayıcı bir düzenlemenin bulunmamasının (gri alan) en önemli nedenlerinden biri bu belirsizliğin devletlerin çıkarlarına hizmet etmesidir⁹⁶. Çünkü siber alanda yürütülen faaliyetlerin atfedilebilirliği teknik açıdan oldukça karmaşıktır⁹⁷. Bir devletin uluslararası seviyede sorumlu tutulabilmesi için uluslararası hukuka aykırı fiilin ya bizzat devletin organları (yasama, yürütme ve yargı) tarafından gerçekleştirilmesi ya da faaliyeti yürüten kişinin devlet adına ve hesabına hareket ediyor olması gerekmektedir.

Tallinn El Kitabı 2.0’ın 15. Kuralında da atfedilebilirlik düzenleme konusu yapılmıştır. Buna göre “Bir devletin organları tarafından ya da iç hukuk uyarınca kamu gücü yetkilerini kullanmakla yetkilendirilmiş kişi veya kuruluşlar tarafından gerçekleştirilen siber operasyonlar devlete atfedilebilir”. Bu noktada dikkat çekilmesi gereken husus siber saldırıların genellikle devlet dışı aktörler veya kişiler tarafından gerçekleştiriliyor olmasıdır. Bu durum eylemin devlete atfedilebilmesini oldukça güçleştirmektedir. Zira bugüne kadar hiçbir devlet, bir başka devleti uluslararası bir siber operasyon nedeniyle “resmî” olarak sorumlu tutmamıştır⁹⁸. Devletlerin siber saldırılara ilişkin atfetme veya faili belirleme konusundaki yaklaşımları son derece ihtiyatlıdır⁹⁹.

Devlet dışı aktörler tarafından gerçekleştirilen siber saldırılar bakımından Uluslararası Adalet Divanı’nın Nikaragua kararı yol gösterici mahiyettedir. Bu karara göre, bir kişinin veya kuruluşun devlet adına ve hesabına hareket ettiğini söyleyebilmek için o kişi veya kuruluşun her faaliyetinin “tam bir bağımlılık” içinde “devletin kontrolü” altında olması gerekmektedir¹⁰⁰. Bu bağlamda Divan kontraların Amerika Birleşik Devletleri Hükûmeti ile olan ilişkisinin, bir taraftan

⁹⁵ Schmitt (ed), *Tallinn Manual 2.0* (n 53).

⁹⁶ Birinci sırada atfedilebilirlik yer almakla birlikte, siber saldırıların gerçekleştirilmesinin diğer gerekçeleri arasında düşük maliyet ve hukuki belirsizlik bulunmaktadır. Bu üç sebep siber operasyonları hem devletler hem de devlet dışı aktörlere çekici kılmaktadır. Detaylı bilgi için bkz. Scott J. Shackelford and Richard B. Andres, ‘State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem’ (2010) 42 *Georgetown Journal of International Law* 971.

⁹⁷ Bogdanova and Callo-Muller, ‘Unilateral Cyber Sanctions’ (n 12) 923.

⁹⁸ Rusinova and Martynova (n 12) 156.

⁹⁹ Bu konuda detaylı örnekler için bkz. Rusinova and Martynova (n 12) 156.

¹⁰⁰ Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14, para 109. Daha detaylı bilgi için bkz. Muhammed Fatih Kafadar, ‘Uluslararası Hukukta Devletlerin Sorumluluğu Bağlamında Siber Saldırıların Atfedilebilirliği Meselesi’ (2020) 2 *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi*.



bağımlılık ve diğer taraftan kontrol açısından hangi düzeyde olduğunu inceleme konusu yapmıştır¹⁰¹.

Birinci Tallinn El Kitabı'nın 5. Kuralı bir devletin kendi topraklarında veya münhasır egemenlik denetimi altındaki siber altyapının, diğer devletleri olumsuz ve hukuka aykırı şekilde etkileyen eylemler için kullanılmasına bilerek izin vermemesi gerektiğini düzenlemektedir¹⁰². Devletlerin bu yükümlülüğe uymak için 'azami çaba' göstermeleri gerekmektedir¹⁰³. Zararlı siber faaliyetlerin büyük ölçüde 'hacktivist' gibi devlet dışı aktörlerce gerçekleştirilmesi ve 'siber terörizm' olgusunun giderek daha yakın ve somut bir tehdit haline gelmesi, devletlerin egemenlik alanları içindeki siber etkinlikleri denetleme yükümlülüğünü uluslararası hukuk bakımından daha da kritik kılmaktadır¹⁰⁴.

Uluslararası Hukuka Aykırı Eylemlerden Dolayı Devletlerin Sorumluluğuna İlişkin Taslak Maddeler'in 8. maddesi de bir özel kişinin devletin talimat veya yönlendirmesi ile hareket etmesini veya devlet tarafından kontrol edilmesini atfedilebilirlik bakımından yeterli görmektedir. Bu bağlamda sonuçlandırılması gereken temel mesele siber saldırıyı gerçekleştiren kişinin veya devlet dışı aktörün devlet ile olan bağının ispatlanmasıdır. Bogdanova ve Callo-Muller'e göre bu bağın ispatlanması ciddi bir kanıt yükü gerektirir zira devletin doğrudan sorumluluğu teknik olarak tespit edilse bile yasal olarak bağ kurmak oldukça güçtür¹⁰⁵. Kafadar'ın da ifade ettiği üzere siber saldırıların devletin *de jure* veya *de facto* organlarına atfedilebilmesini zorlaştıran önemli faktörlerden biri, siber uzayın doğası gereği saldırganların kimliklerini kolayca gizleyebilmesidir¹⁰⁶. Salırganlar, başka bir devleti sorumlu göstermek amacıyla IP adreslerini veya o devletin dijital izlerini taklit edebilirler (spoofing)¹⁰⁷. Bu yaygın teknik, atfetme sürecini ciddi şekilde karmaşıklaştırmaktadır.

c. Karşı Önlemlerin Yalnızca Zarar Gören Devlet Tarafından Gerçekleştirilmesi

Karşı önlemin meşru sayılabilmesinin bir diğer koşulu ise yalnızca zarar gören devlet tarafından gerçekleştirilmesidir¹⁰⁸. Uluslararası Hukuka Aykırı Eylemlerden Dolayı Devletlerin Sorumluluğuna İlişkin Maddeler'in 42. ve 49. maddelerine

¹⁰¹ Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14, para 109. Daha detaylı bilgi için bkz. Kafadar (n 100).

¹⁰² Schmitt (ed), *Tallinn Manual on the International Law* (n 15) Rule 5.

¹⁰³ James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge University Press 2002) 178–186.

¹⁰⁴ Schmitt, 'Below the Threshold Cyber Operations' (n 10) 706.

¹⁰⁵ Bogdanova and Callo-Muller, 'Unilateral Cyber Sanctions' (n 12) 923.

¹⁰⁶ Kafadar (n 100) 1044.

¹⁰⁷ ibid. 1044.

¹⁰⁸ Elif Uzun, *Devletin Milletlerarası Hukuka Aykırı Eyleminden Sorumluluğu* (PhD thesis, Anadolu University 2007) dipnot 485.

göre, karşı önlem hakkı yalnızca “zarar gören” devlete aittir¹⁰⁹. Bu nedenle karşı önlem alma hakkının diğer devletler tarafından kullanılması mümkün değildir.

d. Karşı Önlemlerde Orantılılık İlkesi

Karşı önlemlerin meşru kabul edilebilmesinin bir diğer koşulu da karşı önlemin orantılı olmasıdır. Karşı önlemlerin uğranılan zararlar orantılı olması gerekliliği örf ve âdet hukuku kuralı olarak kabul edilmektedir¹¹⁰. Taslak Maddeler’in 51. maddesinde orantılılık koşulu açıkça düzenleme konusu yapılmaktadır¹¹¹. Dias’a göre orantılılık, karşı önlemlerin, uğranılan zararlar orantılı veya ona yaklaşık düzeyde olması gerektiği anlamına gelir¹¹². Bu durum, karşılıklılık (reciprocity) ilkesini gerektirmemekle birlikte, karşı önlemlerin ihlal edilen yükümlülükle veya onunla yakından ilişkili bir yükümlülükle bağlantılı olarak alınması, önlemin meşruiyetini güçlendirmekte ve uygulanma amacına ulaşma ihtimalini artırmaktadır¹¹³. Ayrıca bu bağlantı, önlemlerin ihlalin ağırlığıyla ölçülü bir biçimde uyumlu hale gelmesini sağlayarak orantılılık ilkesinin yerine getirilme-

¹⁰⁹ Bu düzenlemeye göre “zarar gören devlet” aşağıdaki tanımlara karşılık gelmektedir:

- (a) bir devletin eylemiyle ihlâl edilen hak iki taraflı andlaşmadan kaynaklanıyorsa, andlaşmanın diğer taraf devleti;
- (b) bir devletin eylemiyle ihlâl edilen hak milletlerarası bir divan ya da mahkeminin hükmü ya da başka bir bağlayıcı uyuşmazlık çözüm kararından kaynaklanıyorsa, uyuşmazlığa taraf olan ve bu haktan yararlanmaya hakkı olan diğer devlet ya da devletler;
- (c) bir devletin eylemiyle ihlâl edilen hak milletlerarası bir divan ya da mahkemeden başka bir milletlerarası örgütün bağlayıcı kararından kaynaklanıyorsa, ilgili milletlerarası örgütün kurucu belgesiyle uyumlu olarak, bu haktan yararlanmaya hakkı olan devlet ya da devletler;
- (d) bir devletin eylemiyle ihlâl edilen hak üçüncü bir devlet lehine düzenlenmiş bir andlaşma hükmünden kaynaklanıyorsa, bu üçüncü devlet;
- (e) bir devletin eylemiyle ihlâl edilen hak çok taraflı bir andlaşmadan ya da milletlerarası hukukun bir örf ve âdet kuralından kaynaklanıyorsa, aşağıdaki durumlardan biri söz konusu olduğu takdirde, çok taraflı andlaşmaya taraf olan ya da ilgili milletlerarası örf ve âdet hukuku kuralıyla bağlı olan herhangi bir devlet:
 - (i) hak o devletin lehine yaratılmış ya da ihdas edilmişse,
 - (ii) bir devletin eylemiyle hakkın ihlâl edilmesi zorunlu olarak çok taraflı andlaşmanın tarafı olan ya da milletlerarası örf ve âdet hukuku kuralıyla bağlı olan devletlerin haklarını kullanmalarını ve yükümlülüklerini yerine getirmelerini etkiliyor ise, ya da
 - (iii) hak insan haklarının ve temel hürriyetlerin korunması için yaratılmış ya da ihdas edilmişse.
- (f) bir devletin eylemiyle ihlâl edilen hak çok taraflı bir andlaşmadan kaynaklanıyorsa, o andlaşmada yer alan söz konusu hakkın taraf olan devletlerin kolektif çıkarlarını korumak için konduğu açıkça belirtilmesi durumunda, çok taraflı andlaşmaya taraf olan herhangi bir devlet. Elif Uzun, Devletin Milletlerarası Hukuka Aykırı Eyleminden Sorumluluğu, Kamu Hukuku Ana Bilim Dalı, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, Eskişehir 2007, dipnot 485. Ayrıca bkz. Neslihan Özkerim Güner, *İklim Değişikliği Nedeniyle Devletlerin Sorumluluğu* (1st edn, Seçkin Yayıncılık 2018).

¹¹⁰ Dias (n 82) 21.

¹¹¹ International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries* (2001) Commentary to Chapter II, para 6, and Article 51, paras 2–3.

¹¹² Dias (n 72) 21.

¹¹³ A/CN.4/507 and Add. 1–4 (2000), para 328.

sini kolaylaştırmaktadır. Böylelikle karşı önlemler, yalnızca tepkisel bir nitelik taşımaktan çıkıp uluslararası hukukun koruma ve dengeleme işlevleriyle daha sıkı bir biçimde örtüşebilmektedir.

Ancak bu uygulama mutlak bir zorunluluk değildir zira alınan karşı önlemin ihlal edilen asıl yükümlülüğünden farklı ya da onunla ilgisiz olması da mümkündür. Örneğin, bir devlet, çevresel bir yükümlülüğün ihlaline karşılık olarak ekonomik nitelikte karşı önlemler almayı tercih edebilir¹¹⁴. Benzer şekilde, siber olmayan bir ihlale karşı siber önlemler alınabileceği gibi siber bir ihlale karşı da siber olmayan karşı önlemler alınabilir¹¹⁵. Buradaki temel koşul alınan karşı önlemin orantılı olmasıdır. Dolayısıyla bir devletin siber uzaydaki hukuka aykırı faaliyetlere karşı önlem alma hakkı bulunduğu, bu önlemler hem orantılı olmalı hem de ihlale yol açan uluslararası hukuk kuralı ile zarar gören devletin başvurduğu önlemler arasında adil bir denge gözetilmelidir. Orantılılık değerlendirilirken hukuka aykırı fiilin ağırlığı ve ilgili haklar dikkate alınmalıdır. Başka bir ifade ile bir karşı önlemin orantılı olup olmadığı değerlendirme konusu yapılırken devletler, uluslararası hukuka aykırı fiilin ağırlığını ve ihlal edilen hakların önemini hem zarar gören hem de sorumlu devlet veya devletler bakımından dikkate almak zorundadır¹¹⁶.

Dias orantılılık değerlendirilirken hem nitel hem de nicel analizin gerekliliğine dikkat çekmektedir. Nicel değerlendirme, doğrudan ölçülebilir ve sayısal verilerle ifade edilebilen zararlara odaklanır¹¹⁷. Örnek vermek gerekirse bir devletin kritik altyapısına yönelik siber saldırı sonucunda 48 saatlik elektrik kesintisi yaşanmışsa, bu kesinti nedeniyle hastanelerde hizmet aksaması olmuşsa, milyon dolarlık ekonomik zarar ortaya çıkmışsa bu zararların nicel olarak ölçülebilmesi mümkündür. Nitel değerlendirme ise, doğrudan ölçülemeyen; ancak etkisi büyük olan, manevi, siyasi veya sosyal boyutu ağır basan zararlara odaklanmaktadır¹¹⁸. Bu tür değerlendirmeler, özellikle karmaşık toplumsal olayların ya da politik süreçlerin etkilerini anlamada kritik bir rol oynar¹¹⁹. Örneğin bir devletin vatandaşlarının kişisel verilerinin (sağlık bilgileri, kimlik numaraları vb.) çalınması ve yayımlanması halinde toplumda güven kaybı oluşabilir daha da önemlisi devlete karşı kurumsal güven zedelenebilir. Bu tür etkilerin maddi anlamda ölçülmesi mümkün değildir ancak ağır niteliksel zarar doğurduğu aşikardır. Günümüzde

¹¹⁴ Dias (n 82) 21.

¹¹⁵ Dias (n 82) 21. Ayrıca bkz. Schmitt (ed), *Tallinn Manual 2.0* (n 53) Kural 23.

¹¹⁶ ibid. 21.

¹¹⁷ Nihan Demirkasımoğlu, 'Nitel Araştırma Geleneğinde Nicel Göstergelerin Kullanımı ve Genellenebilirlik Üzerine Bir Değerlendirme' (2021) 42 *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 231.

¹¹⁸ ibid. 231.

¹¹⁹ Detaylı bilgi için bkz. Michael Quinn Patton, *Qualitative Research and Evaluation Methods* (Vol 3, Sage 2002).

de özellikle siber alanda yaşanan veri sızıntıları devletin itibarının zedelenmesi yönünde nitel zararlara sebep olmaktadır.

Bilgi ve iletişim teknolojilerinin yaygın ve birbirine bağlı yapısı nedeniyle siber karşı önlemlerin orantılılığını değerlendirmek oldukça güç olabilir¹²⁰. Siber alanın doğası gereği sahip olduğu iç içe geçmiş ve yüksek düzeyde bağlantılı yapı, siber karşı önlemlerin hedef alınan aktörle sınırlı kalmayıp, üçüncü devletler veya devlet dışı aktörler gibi istenmeyen taraflara da sıçrama riskini beraberinde getirmektedir¹²¹. Bu durum, siber alanın temel teknik özelliklerinden, yani ağların birbirine bağımlılığından, veri akışlarının sınır tanımayan yapısından ve saldırı ile savunma mekanizmalarının karmaşık etkileşiminden kaynaklanmaktadır¹²². Bu durum karşı önlemlerin meşru sayılabildiğinin koşullarından olan yalnızca zarara sebebiyet veren devletin hedef alınması kuralını ihlal edebilir. Bu nedenle siber uzayda orantılılığın hem nicel hem de nitel unsurlarının değerlendirilmesi çok daha fazla dikkat gerektirir¹²³.

e. Karşı Önlemlerin Geri Alınabilirlik ve Geçicilik Şartları

Diğer bir önemli koşul karşı önlemin geçici mahiyette olmasıdır. Taslak maddelerin 49(1) düzenlemesine göre “[k]arşı önlemler, bu önlemleri alan Devletin, sorumlu Devlete yönelik uluslararası yükümlülüklerinin geçici olarak yerine getirilmemesiyle sınırlıdır.” Bu önlemlerin amacı, “ihlalin gerçekleşmesinden önceki durumu -yani ‘meşruiyet durumu’nu veya eski hale iade durumunu- ihlal eden devletle zarar gören devlet arasında yeniden tesis etmektir”¹²⁴. Bu bağlamda ihlali gerçekleştiren devlet yükümlülüğüne uydığında ve ihlali sonlandırdığında karşı önlemin uygulanmasına devam edilemez. Bu nedenle karşı önlemler amaçlarına ulaşma süresi ile sınırlı olacak şekilde geçici niteliktedir.

Taslak Maddelerin 49(3) düzenlemesine göre “[k]arşı önlemler, mümkün olduğu ölçüde, söz konusu yükümlülüklerin yerine getirilmesine yeniden başlanmasına imkân verecek şekilde alınmalıdır”. Başka bir ifade ile karşı önlemler geri alınabilir mahiyette olmalıdır. Bu kurala göre devletler etkileri geri döndürülebilir karşı önlemler almakla yükümlüdür. Ancak bu yükümlülüğün de mutlak olduğu söylenemez; zira BM Uluslararası Hukuk Komisyonu’nun Taslak Maddeleri, karşı

¹²⁰ Dias (n 82) 22.

¹²¹ ibid. 22.

¹²² Nitekim siber müdahalelerin sıklıkla ikincil etkiler (spillover effects) yarattığı, dolayısıyla doğrudan hedeflenmeyen aktörlerin de bu müdahalelerden etkilenebileceği kabul edilmektedir. Christian Eckert, Nadine Gatzert and Madeline Schubert, ‘Analyzing Spillover Effects from Data Breaches to the US (Cyber) Insurance Industry’ (2023) 29(6) *The European Journal of Finance* 669. Özellikle kritik altyapılar gibi yüksek derecede ağa bağlı sistemlerde gerçekleştirilen siber operasyonlar, jeopolitik gerilimlerin artmasına, üçüncü taraf sorumluluğu tartışmalarına ve uluslararası hukuk ihlali iddialarına zemin hazırlayabilir.

¹²³ Dias (n 82) 22.

¹²⁴ ibid. 18.

önlemlerin sonuçlarının mutlak anlamda geri döndürülebilir olmasını değil, yalnızca “mümkün olduğu ölçüde” geri döndürülebilir olmasını şart koşmaktadır¹²⁵.

Sonuç olarak, devletlerin uluslararası hukuku ihlal eden siber operasyonlar veya benzeri eylemler karşısında karşı önlemler alma yetkisi bulunmaktadır. Ancak bu tür önlemlerin meşruiyeti, yalnızca belirli hukuki koşulların yerine getirilmesi halinde söz konusu olacaktır. Bu koşullar arasında ihlalin açık şekilde tespit edilmesi, zarar gören devletin öncelikle diplomatik yolları tüketmiş olması ve alınan önlemin orantılılık ilkesine uygunluğu yer almaktadır. Aksi takdirde, gerçekleştirilen karşı önlemin uluslararası hukuk açısından meşru sayılması mümkün olmayacaktır.

Bununla birlikte tek taraflı yaptırımlar çoğu zaman uluslararası hukuka aykırı olmaları ve gelişmekte olan devletlerin insan hakları ile ekonomik durumları üzerinde olumsuz etkiler yaratmaları nedeniyle BM Genel Kurulu tarafından genellikle kınanmaktadır¹²⁶. Her ne kadar hukuki öğreti genel olarak ekonomik zorlama araçlarının sınırlarını uluslararası hukukun gri alanı olarak değerlendirse de bu tür kararlar ortaya çıkan bir yasağın habercisi olarak yorumlanabilir. Ancak daha yakından incelendiğinde, bu kararların uluslararası içtihat ve öğreti tarafından geliştirilen yeni bir teamül hukukunun oluşması için gerekli kriterleri karşılamadığı görülmektedir¹²⁷. Zira her ne kadar BM Genel Kurul kararları başlangıçta hukuki bir bağlayıcılığa sahip olmasa da bu kararlar tutarlı bir şekilde ve hukuki zorunluluk inancıyla gerçekleştirilen devlet uygulamalarına dönüşürse uluslararası örf ve âdet hukukunun bir parçası haline gelebilirler¹²⁸. Ancak örneklerde de görüldüğü üzere bu kararların tutarlı devlet uygulamalarına dönüştüğünü

¹²⁵ International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries* (2001) Commentary to Article 49, para 9.

¹²⁶ Hofer (n 12) 175.

¹²⁷ Özel Raportörün raporuna göre BM’nin, tek taraflı zorlayıcı önlemlerle ilgili sürekli aldığı kararlar ve tekrarlanan kınamalar bu alanda bir örf ve âdet hukuku gelişimine yol açarak bağlayıcı hale gelebilir. A/HRC/30/45, para 47. Bu durum devletlerin tek taraflı zorlayıcı önlemleri uygulamalarının uluslararası hukuk açısından giderek daha az kabul edilebilir hale gelmesine yol açabilir. Ancak bu hususta bir görüş birliği henüz mevcut değildir. Örneğin Mohamad devletlerin kendi politikalarını belirleme hakkına müdahale etmeyen bir ilkenin, tek taraflı ekonomik yaptırımları yasaklayan bir uluslararası örf ve âdet kuralı haline geldiğini ifade etmektedir (Rahmat Mohamad, ‘Unilateral Sanctions in International Law: A Quest for Legality’ in Ali Z Marossi and Marisa R Bassett (eds), *Economic Sanctions under International Law* (T.M.C. Asser Press 2015) 76’dan aktaran Galip Engin Şimşek, ‘Uluslararası Hukuk Açısından Ekonomik Yaptırımlar ve ABD’nin Tek Taraflı Yaptırımlarının Kısa Bir Değerlendirilmesi’ (2020) 78(4) İstanbul Hukuk Mecmuası 2049, 2061). Hofer ise BM Genel Kurulu bu kararlarının yeni bir örf ve âdet hukukunu kurmak için gerekli kriterleri karşılamadığını ifade etmektedir. (Hofer (n 12) 175). Bu hususta detaylı tartışma için bkz. Galip Engin Şimşek, ‘Uluslararası Hukuk Açısından Ekonomik Yaptırımlar ve ABD’nin Tek Taraflı Yaptırımlarının Kısa Bir Değerlendirilmesi’ (2020) 78(4) İstanbul Hukuk Mecmuası 2049, 2049-2078.

¹²⁸ Alan Boyle, ‘Soft Law in International Law-Making’ in Malcolm D. Evans (ed), *International Law* (Oxford University Press 2014) 118–137, 118.

söylemek şu an için mümkün gözükmemektedir. Bu nedenle bu aşamada bir örf ve âdet hukuku varlığından bahsetmek kanaatimizce mümkün değildir. Zira bu kararlar gelişmiş ve gelişmekte olan devletler arasında tek taraflı yaptırımların meşruiyeti konusunda var olan ayrışmayı da açıkça ortaya koymaktadır¹²⁹.

Sonuç olarak, günümüz uluslararası ilişkilerinde siber operasyonlar ve tek taraflı yaptırımlar gibi geleneksel olmayan baskı araçlarının artan kullanımı, klasik uluslararası hukuk ilkelerini önemli ölçüde zorlamaktadır. Devletlerin karşı önlem alma yetkisi, uluslararası hukukun tanıdığı meşru bir hak olmakla birlikte, bu yetkinin keyfi biçimde kullanılması hukuki meşruiyeti ortadan kaldırmaktadır. Karşı önlemlerin yalnızca belirli koşullar altında uygulanabilir olması, devletlerarası ilişkilerde denge ve hukuki öngörülebilirliğin korunması açısından hayati öneme sahiptir. Öte yandan, tek taraflı ekonomik yaptırımlar gibi uygulamalar, her ne kadar uluslararası hukukun gri alanında değerlendirilse de özellikle gelişmekte olan ülkeler açısından ciddi sosyo-ekonomik ve insan hakları ihlallerine yol açabilmektedir. BM Genel Kurulu'nun bu yaptırımları sürekli olarak kınaması, uluslararası toplum içinde bu uygulamaların meşruiyetine ilişkin derin bir görüş ayrılığına işaret etmektedir. Bu çerçevede, uluslararası hukukta teamül oluşturacak netlikte kurallar henüz gelişmemiş olsa da mevcut eğilimler uzun vadede daha bağlayıcı normların oluşabileceğini göstermektedir.

2. Siber Karşı Önlemler ve Devlet Uygulamaları

Siber yaptırımların uygulama alanının özellikle Amerika Birleşik Devletleri (ABD), Birleşik Krallık ve Avrupa Birliği (AB) tarafından genişletilerek uygulanması da tartışmalara sebebiyet vermektedir¹³⁰. Bunun temel nedenlerinden biri, uluslararası hukukta siber alanın henüz tam anlamıyla düzenlenmemiş ol-

¹²⁹ Hofer (n 12) 175.

¹³⁰ Özellikle ABD yalnızca saldırıyı gerçekleştirenleri değil dolaylı destek verdiği düşünülen kişi ve şirketleri de hedef almaktadır. Çokişler (n 79) 71. Örneğin AB, 2025 Ocak ayında, 2020 yılında Estonya'ya yönelik siber saldırılardan sorumlu tutulan üç Rus askeri istihbarat görevlisini yaptırım listesine eklemiştir. Bu saldırılar, Estonya'nın kritik altyapılarına zarar vermeyi amaçlayan siber operasyonlardır. Yaptırımlar, varlık dondurma ve seyahat yasağı gibi önlemleri içermektedir (European Council, Timeline - Sanctions Against Cyber-Attacks, <<https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/timeline-sanctions-cyber-attacks/>> E.T. 13.05.2025). Birleşik Krallık, 2025 Temmuz ayında, Rusya'nın askeri istihbarat servisi GRU'nun üç birimini ve 18 görevlisini yaptırım listesine dahil etmiştir. Bu birimler, Mariupol'deki bir tiyatroya yönelik bombalama planı, eski Rus ajanı Sergei Skripal'in ailesine yönelik saldırılar ve Avrupa genelinde siber saldırılarla ilişkilendirilmektedir. Yaptırımlar, varlık dondurma ve seyahat yasağı gibi önlemleri içermektedir (By Reuters, UK Discovers Russian 'Espionage Tool', Sanctions GRU Officers over Cyberattacks, <<https://www.reuters.com/world/uk/uk-discovers-russian-espionage-tool-sanctions-gru-officers-over-cyberattacks-2025-07-18/>> E.T. 12.04.2025). ABD, Birleşik Krallık ve Avustralya, 2025 Şubat ayında, Rusya merkezli Zservers adlı "bulletproof hosting" sağlayıcısını ve iki Rus operatörünü, LockBit fidye yazılımı saldırılarına destek verdikleri gerekçesiyle yaptırım listesine almıştır. LockBit, dünya çapında birçok kurumu hedef almış ve büyük mali zararlara yol açmıştır (AP, Russian Cybercrime Network Targeted for Sanctions Across US, UK And Australia, <<https://apnews.com/article/treasury-sanctions-uk-australia-russia-361e788f5482bfd787af01002af2ff4c>> E.T. 12.04.2025).



masıdır. Zira hangi eylemlerin yaptırıma konu olacağı belirsizliğini korumaktadır. Öte yandan ekonomik boyutta, küresel tedarik zincirlerinin kırılganlığı ve teknoloji bağımlılıkları, yaptırımların yalnızca hedef ülkeleri değil, üçüncü ülkeleri ve özel sektörü de doğrudan etkileyerek çok daha geniş kapsamlı sonuçlar doğurmasına neden olmaktadır¹³¹. Bu çerçevede, özellikle siber yaptırımlara ilişkin açık yasal çerçeveler oluşturmuş olan Amerika Birleşik Devletleri ve Birleşik Krallık'ın bireysel uygulamaları ile AB'nin siber yaptırımlara dair kolektif Tüzük temelinde geliştirdiği mekanizmaların yakından incelenmesi gerekmektedir. Nitekim Amerika Birleşik Devletleri, 2015 tarihli Executive Order 13694 ile devlet dışı ve devlet destekli siber tehdit aktörlerine karşı hedefli yaptırımları (targeted sanctions) mümkün kılmıştır¹³². Bu düzenleme 2016 ve 2021 yıllarında genişletilerek daha kapsamlı bir siber yaptırım rejimi oluşturulmuştur. Birleşik Krallık ise AB'nden ayrıldıktan sonra 2020 tarihli The Cyber (Sanctions) (EU Exit) Regulations 2020 ile kendi ulusal siber yaptırım düzenlemesini yürürlüğe koymuştur. AB ise 2019 tarihli Council Decision (CFSP) 2019/797 ve Council Regulation (EU) 2019/796 aracılığıyla, seçimlere müdahale, fikri mülkiyet hırsızlığı ve kritik altyapılara yönelik siber saldırılar gibi eylemleri hedef alan ilk kolektif siber yaptırım rejimini benimsemiştir.

İç hukuk düzenlemeleri çerçevesinde başvuru alan tek taraflı siber yaptırımların da uygulanması hususunda bazı koşullar öngörülmüştür. Örneğin “ABD'nin Amerika'nın Hasımlarına Yaptırımlar Yoluyla Karşı Koyma Yasası” (Countering America's Adversaries Through Sanctions Act -CAATSA) siber yaptırımların kapsamını belirlemek için belirli kriterler ortaya koymaktadır. Ancak Yasa içerisinde sık sık kullanılan “önemli kötü niyetli siber destekli faaliyetler” (significant malicious cyber-enabled activities) veya “kötü niyetli siber saldırı” (malicious cyber-hacking) kavramları belirsizliğini korumaktadır¹³³. Zira Yasa'da bu kavramlara ilişkin herhangi bir tanımlama yapılmamıştır. Bununla birlikte, Yasa'da siber saldırılara yönelik kullanılan ‘önemli’ ibaresi, yalnızca ciddi boyutlara ulaşan siber saldırılar karşısında yaptırım kararı alınabileceği mesajını vermektedir¹³⁴.

Birleşik Krallık, siber tehditlere karşı ulusal güvenliğini korumak amacıyla iç hukukta çeşitli yaptırım mekanizmaları oluşturmuştur. Bu kapsamda 2018 tarihli “Yaptırımlar ve Kara Para Aklamayla Mücadele Yasası” (Sanctions and Anti-Money Laundering Act 2018 -SAML) önemli bir düzenleme olarak kabul

¹³¹ Fabio Ghironi, Daisoon Kim, and Galip Kemal Ozhan, ‘International Economic Sanctions and Third-Country Effects’ (2024) 72(2) *IMF Economic Review* 611, 611-652.

¹³² Executive Order, ‘Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber Enabled Activities’ (1 April 2015) <<https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>> E.T. 28.05.2024.

¹³³ Countering America's Adversaries Through Sanctions Act, Pub L No 115-44, 131 Stat 886 (2 August 2017) <<https://congress.gov/115/plaws/publ44/PLAW-115publ44.pdf>> E.T. 13.05.2025.

¹³⁴ Daha detaylı bilgi için bkz. Çekişler (n 79) 71.

edilmektedir. Söz konusu Yasa, Birleşik Krallık'ın AB'den ayrılmasının ardından kendi bağımsız yaptırım rejimini geliştirmesine imkân tanımış ve siber saldırılar da dahil olmak üzere ulusal güvenliği tehdit eden eylemlere karşı uygulanabilecek yaptırımların yasal çerçevesini belirlemiştir¹³⁵. “Yaptırımlar ve Kara Para Aklamayla Mücadele Yasası”nı tamamlayıcı nitelikte çıkarılan 2020 tarihli “Siber (Yaptırımlar) (Avrupa Birliği'nden Çıkış) Düzenlemeleri” (The Cyber (Sanctions) (EU Exit) Regulations 2020) özellikle devlet destekli siber saldırılar gibi faaliyetlerde bulunan kişi, kuruluş ve devletlere karşı bireysel ya da sektörel düzeyde yaptırımların uygulanmasını mümkün kılmıştır. Bu düzenleme, seçimlere müdahale, kritik altyapılara yönelik siber saldırılar ve fikri mülkiyetin yasa dışı yollarla elde edilmesi gibi durumları hedef almaktadır¹³⁶. Her iki düzenlemede de “siber yaptırım” (cyber sanctions) kavramına yer verilmeyle birlikte, bu kavrama dair pozitif hukuk kapsamında açık ve kapsamlı bir tanım bulunmamaktadır. Bu durum, siber yaptırımların kapsamının belirlenmesi bakımından yoruma açık bir alan yaratmakta ve hukuki belirlilik ile öngörülebilirlik ilkeleri açısından tartışmalara neden olabilmektedir.

AB de siber saldırılar konusunda oldukça kapsamlı düzenlemeler yapmıştır. AB'nin siber saldırılara karşı kısıtlayıcı tedbirlerin birincisi 17 Mayıs 2019 tarihli 2019/797 Sayılı Konsey Kararı - “Avrupa Birliği veya Üye Devletlerini Tehdit Eden Siber Saldırlara Karşı Kısıtlayıcı Tedbirler” diğeri ise yine 17 Mayıs 2019 tarihli 2019/796 sayılı Avrupa Birliği Konsey Tüzüğü- “Avrupa Birliği veya Üye Devletlerini Tehdit Eden Siber Saldırlara Karşı Kısıtlayıcı Tedbirlerdir¹³⁷. AB tarafından alınan kararların daha net düzenlemeler ihtiva ettiğini söylemek mümkündür. Örneğin Tüzüğün 1. maddesinin 3. bendine göre “siber saldırılar aşağıdakilerden herhangi birini içeren eylemler olarak tanımlanır: *“bilgi sistemlerine erişim, bilgi sistemine müdahale, verilere müdahale, verilerin ele geçirilmesi..”*. 1. maddenin 7. bendinde ise tüm kavramların tanımı yapılmaktadır. Tüzüğün 2. maddesi, Amerika Birleşik Devletleri'nin, “Amerika'nın Hasımlarına Yaptırımlar Yoluyla Karşı Koyma Yasası”na kıyasla siber saldırıların hangi koşullarda “önemli” kabul edileceğini belirleyen spesifik kriterlere yer vermektedir. Bu madde, siber saldırının etkisinin değerlendirilmesinde kullanılan kapsam, ölçek, ekonomik kayıp, veri ihlalleri gibi ölçütleri sistematik bir biçimde düzenleyerek, “önemli etki” kavramını objektif ve somut faktörler çerçevesinde tanımlamaktadır. Böylece, Tüzük, “Amerika'nın Hasımlarına Yaptırımlar Yoluyla Karşı

¹³⁵ UK Government, *Sanctions and Anti-Money Laundering Act 2018* (2018) <<https://www.legislation.gov.uk/ukpga/2018/13/contents>> E.T.01.02.2025.

¹³⁶ UK Statutory Instruments, *The Cyber (Sanctions) (EU Exit) Regulations 2020, No 597* (2020) <<https://www.legislation.gov.uk/uksi/2020/597/contents/made>> E.T.01.02.2025.

¹³⁷ European Union, Decision (CFSP) 2019/797 — restrictive measures against cyber-attacks threatening the EU or its Member States (2019); Regulation (EU) 2019/796 — restrictive measures against cyber-attacks threatening the EU or its Member States (2019) <<https://eur-lex.europa.eu/EN/legal-content/summary/eu-restrictive-measures-against-cyber-attacks.html>> E.T.03.03.2025.



Koyma Yasası'nın daha genel ve geniş yoruma açık yaklaşımından farklı olarak, müdahalelerin hukuki dayanağını güçlendiren ve uygulamada öngörülebilirlik sağlayan bir normatif çerçeve oluşturmaktadır.

Tek taraflı yaptırımlara ilişkin kavramsal belirsizlik, kimin hedef alınabileceği ve hangi fiillerin yaptırıma tabi olacağı konusunda uygulamada öngörülemezlik yaratmaktadır. Bu nedenle de birçok eleştiriye sebebiyet vermektedir. Zira tek taraflı yaptırımlardaki belirsizlik uluslararası hukukta meşruiyet sorunlarına yol açmaktadır. Örneğin 2014 yılında Asya-Afrika Hukuk Danışma Örgütü (AALCO), “*üçüncü taraflara yönelik tek taraflı yaptırımların Birleşmiş Milletler Şartı'na aykırı olduğu ve uluslararası hukukun genel ilkeleriyle çeliştiği*” yönündeki derin endişesini dile getirmiştir¹³⁸. 19 Nisan 2016'da Çin, Rusya ve Hindistan dışişleri bakanları benzer bir açıklama yaparak, özellikle “uluslararası hukuka dayanmayan tek taraflı zorlayıcı önlemlerin” devletlerin egemen eşitliği, iç işlerine karışmama ve iş birliği ilkeleriyle bağdaşmadığını belirtmişlerdir¹³⁹. 25 Haziran 2016'da Çin Halk Cumhuriyeti ve Rusya Federasyonu, *Uluslararası Hukukun Teşviki Hakkında Ortak Bildiri* yayımlayarak, “uluslararası hukuka dayanmayan tek taraflı zorlayıcı önlemlerin, diğer adıyla “tek taraflı yaptırımların” çifte standartların bir örneği olduğunu ve “bazı devletlerin iradelerini diğer devletlere dayatmasının” bir tezahürü olduğunu ifade etmişlerdir¹⁴⁰. Bu tür uygulamaların, “uluslararası hukukun genel olarak tanınan ilke ve kurallarına” aykırı olduğu belirtilmiştir¹⁴¹. Söz konusu önlemlerin, BM Güvenlik Konseyi tarafından uygulanan yaptırımların amaç ve hedeflerini baltalayabileceği ve bu yaptırımların bütünlüğünü ve etkinliğini zayıflatabileceği vurgulanmıştır¹⁴². Hofer'in de ifade ettiği üzere özellikle tek taraflı ekonomik yaptırımlar sıklıkla BM Genel Kurulu kararlarında dile getirilmekte; gelişmekte olan devletler, tek taraflı yaptırımların yasallığını sorgulamakta ve bu önlemlerin uluslararası hukuk ilkelerine aykırı bir zorlama eylemi teşkil ettiğini savunmaktadır¹⁴³. Ancak tek taraflı yaptırımların yasak olduğuna dair bir uluslararası hukuk kaynağı bulunmamaktadır, bu nedenle 1993 yılında BM Genel Sekreteri tarafından yayımlanan bir raporda “[z]orlayıcı ekonomik önlemlerin ne zaman uygunsuz olduğu konusunda uluslararası hukuk-

¹³⁸ AALCO, *Extraterritorial Application of National Legislation: Sanctions Imposed against Third Parties* (2014) 22 <<http://www.aalco.int/53rdsession/extraterritorial%202014.pdf>> E.T. 07.03.2025

¹³⁹ Joint Communique of the 14th Meeting of the Foreign Ministers of the Russian Federation, the Republic of India and the People's Republic of China (19 April 2016) para 6 <http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t1356652.shtml> E.T. 05.07.2024.

¹⁴⁰ The Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law (25 June 2016) para 6 <http://www.mid.ru/en/foreign_policy/news//asset_publisher/cKNonkJE02Bw/content/id/2331698> 01.02.2024.

¹⁴¹ ibid. para 6

¹⁴² ibid. para 6.

¹⁴³ Hofer (n 12) 175.

ta açık bir fikir birliği” bulunmadığı ifade edilmiştir¹⁴⁴. Yine Tzanakopoulos da günümüz uluslararası hukukunda hukuka aykırı ekonomik zorlama eylemlerinin neredeyse hiç var olmadığını ileri sürmüştür¹⁴⁵.

“Devletlerin Ekonomik Hak ve Yükümlülükleri Şartı”nın (Charter of Economic Rights and Duties of States (UN General Assembly Resolution 3281 (XXIX), 1974) 32. maddesi devletlerin tek taraflı uyguladıkları ekonomik yaptırımlara sınır çizmektedir. Bu düzenlemeye göre “Hiçbir devlet, başka bir devleti egemenlik haklarını kullanmada boyun eğmeye zorlamak amacıyla ekonomik, siyasi ya da başka türden önlemleri kullanamaz veya bu tür önlemlerin kullanılmasını teşvik edemez”¹⁴⁶. Elagab 32. maddeye ilişkin yorumunda devletlerin ret oyu vermesine rağmen 8 devletin çekimser kaldığına dikkat çekerek bu hükmün oybirliğiyle kabul edilmediğini ifade etmiştir¹⁴⁷. Elagab BM Genel Kurulu’nun 2131 (XX) sayılı Kararına, “Devletlerin İçişlerine Müdahalenin Kabul Edilemezliği ve Bağımsızlıkları ile Egemenliklerinin Korunmasına Dair Bildiri”¹⁴⁸ değinerek anılan kararın ekonomik zorlamayı açık ve kesin bir şekilde yasaklamadığını belirtmektedir¹⁴⁹. Bu bağlamda Elagab “Devletlerin Ekonomik Hak ve Yükümlülükleri Şartı”ın bağlayıcı bir belge olmadığını ve 32. maddenin ekonomik zorlamayı hukuken yasaklayan bir hüküm olarak değil, bir “ideal”i ifade eden bir beyan olarak okunması gerektiğini ileri sürmüştür¹⁵⁰.

Uluslararası Adalet Divanı’nın Nikaragua’da ve Nikaragua’ya Karşı Askerî ve Paramiliter Faaliyetler (Nikaragua v. Amerika Birleşik Devletleri) davasında verdiği karar, 32. madde hükmü ile paralellik göstermektedir. Bu karara göre, müdahale yasağı veya müdahale etmeme ilkesi “tüm devletlerin veya devlet gruplarının başka devletlerin iç ya da dış işlerine doğrudan ya da dolaylı biçimde müdahalede bulunmasını yasaklamaktadır. Bu nedenle, yasaklanmış bir müdahale, her devletin egemenlik ilkesi uyarınca serbestçe karar verme yetkisine

¹⁴⁴ Note by the Secretary-General, *Economic measures as a means of political and economic coercion against developing countries*, UN Doc A/48/535 (25 October 1993) point 2(a).

¹⁴⁵ Antonios Tzanakopoulos, ‘The Right to Be Free From Economic Coercion’ (2015) 4 *Cambridge Journal of International and Comparative Law* 633, 633.

¹⁴⁶ UNGA Res 3281 (XXIX), Charter of Economic Rights and Duties of States (adopted 12 December 1974) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/2778/download?E.T.04.06.2025>> E.T. 23.06.2025.

¹⁴⁷ Omer Yousif Elagab, *The legality of Non-forcible Counter-measures in International Law* (PhD Thesis, University of Oxford 1986) 384.

¹⁴⁸ UNGA Res 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, UN Doc A/RES/20/2131 (21 December 1965) <<https://www.ilsa.org/Jessup/Jessup15/Declaration%20on%20the%20Inadmissibility%20of%20Intervention%20in%20the%20Domestic%20Affairs%20of%20States%20and%20the%20Protection%20of%20Their%20Independence%20and%20Sovereignty.pdf>> E.T. 01.03.2025.

¹⁴⁹ Elagab (n 147) 384.

¹⁵⁰ ibid. 384. Ayrıca bkz. Hofer (n 12) 184–185.



sahip olduğu konulara ilişkin olmalıdır. Bu konular arasında bir devletin politik, ekonomik, sosyal ve kültürel sistemini belirleme ya da dış politikasını oluşturma hakkı yer almaktadır”¹⁵¹. Ancak Şimşek’in belirttiği gibi, Adalet Divanı aynı kararında; doğrudan veya dolaylı askeri güç kullanımını içeren eylemleri, iç işlerine müdahale yasağına aykırı zorlayıcı müdahale olarak değerlendirmişken, diğer devletlere yapılan ekonomik yardımların kesilmesi ve ticaret ambargosu gibi uygulamaları iç işlerine müdahale olarak nitelendirmemiştir¹⁵². Ancak, yukarıda da ifade ettiğimiz gibi ekonomik karşı önlemlerin uluslararası hukuka aykırı olduğu iddiası da bulunmaktadır. Kanaatimizce özellikle tek taraflı ekonomik yaptırımların “karşı önlem” olarak alınmasını meşru kılacak koşullar dâhilinde değerlendirilmesi yerinde olacaktır. Zira her ne kadar ekonomik baskılar ve müdahaleler, bir devletin egemen karar alma süreçlerine zorlayıcı biçimde müdahale ettiğinde iç işlerine müdahale yasağını ihlal edebilecek nitelikte olsa da her devletin ticaret yapma ya da yapmama konusunda sahip olduğu serbesti de göz ardı edilmemelidir. Zira tek taraflı ekonomik yaptırımların baskı aracı olarak kullanılmasını doğrudan yasaklayan bağlayıcı nitelikte uluslararası bir normatif düzenleme henüz bulunmamaktadır.

Ancak Türkiye’nin de diğer birçok devlet gibi tek taraflı yaptırımlara genel olarak temkinli bir yaklaşım içerisinde olduğu ifade edilebilir. Zira, Amerika ve Birleşik Krallık’ın aksine, Türkiye’nin ulusal bir yaptırım kanunu bulunmamaktadır. Her ne kadar Türkiye zaman zaman bazı tek taraflı yaptırımlar uygulamış olsa da bu tedbirleri açıkça bir “yaptırım rejimi” olarak ilan etmemiştir. Örneğin, 2012 yılında Esad rejimiyle diplomatik ilişkilerini kesmiş ve Şam’daki büyükelçisini geri çağırmıştır¹⁵³. Yine, Türkiye Mavi Marmara davası sonrasında İsrail ile bazı savunma ve ticaret anlaşmalarını askıya almıştır¹⁵⁴. Bu tedbirler doğrudan yaptırım niteliğinde olmasa da ekonomik ve diplomatik ilişkilerin sınırlandırılması şeklinde yorumlanabilir. Benzer şekilde, Fransa ile yaşanan karikatür krizi sonrasında Cumhurbaşkanı Erdoğan, Emmanuel Macron’un “mental tedaviye” ihtiyacı olduğunu söyleyerek Türk halkını ve Müslüman ülkeleri Fransız mallarını boykot etmeye davet etmiştir¹⁵⁵. Bu uygulama, devletin resmî bir yaptırımı olmasa da Cumhurbaşkanı Erdoğan’ın çağrısı toplumsal düzlemde bir yaptırım

¹⁵¹ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 108, para 205.

¹⁵² ibid. para 245. Detaylı bilgi için bkz. Şimşek (n127) 2059.

¹⁵³ Milliyet, ‘Türkiye Suriye Elçisini Geri Çekti’ (26 March 2012) <<https://web.archive.org/web/20140219172423/http://dunya.milliyet.com.tr/turkiye-suriye-elcisini-geri-cekti/dunya/dunyadetay/26.03.2012/1519878/default.htm>> 23.09.2024.

¹⁵⁴ Nergiz Başeğmez Bolaman, ‘1980 Sonrası Türkiye-Ortadoğu İlişkilerinin Türk Siyasal Hayatına Etkileri (İran, Irak, Suriye, İsrail, Mısır)’ in Ali Rıza Savaş ve Ahmet Hikmet Zabun (eds.), 1980’den Günümüze Türk Siyasal Hayatı: Siyaset, Ekonomi, Dış Politika (Özgür Yayınları 2023) 276.

¹⁵⁵ Panaroma, Türkiye – Fransa İlişkilerinde Karikatür Krizi – Zana Çitak, <https://www.globalpanorama.org/2020/11/turkiye-fransa-iliskilerinde-karikatur-krizi/> 29.09.2025.

olarak kabul edilmiştir. Bunlar gibi birçok örnekte de resmî bir yaptırım olarak ilan edilmemiştir, ancak uzun süreli ekonomik ve diplomatik izolasyon niteliğinde tedbirler alınmıştır¹⁵⁶. Sonuç olarak her ne kadar gayri-resmî tek taraflı yaptırımlar uygulanmış olsa da Türkiye'nin siber güvenlik alanındaki çalışmaları, ulusal altyapının korunması ve siber suçlarla mücadeleye odaklanmaktadır¹⁵⁷. Diğer devletlere yönelik açıkça ilan edilmiş tek taraflı siber yaptırımlar uyguladığına dair kamuya açık bir bilgi bulunmamaktadır.

SONUÇ

Siber uzayın giderek jeopolitik bir çatışma alanına dönüşmesi, klasik yaptırım mekanizmalarının günümüz koşullarına cevap vermekte yetersiz kaldığını ortaya koymaktadır. Bu bağlamda, hem BM Güvenlik Konseyi'nin çok taraflı kolektif yaptırımları hem de devletlerin tek taraflı olarak başvurduğu siber karşı önlemler, uluslararası hukukun yeni normatif sınamalarla karşı karşıya olduğunu göstermektedir.

Çalışmada da detaylı biçimde ele alındığı üzere, BM Güvenlik Konseyi'nin siber yaptırımlar uygulama yetkisi, BM Şartı'nın VII. Bölümü çerçevesinde hukuki temele sahiptir. Ancak bu tür yaptırımların uygulanabilirliği ve meşruiyeti, özellikle insan hakları hukuku ve insancıl hukuk açısından dikkatle değerlendirilmelidir. İfade özgürlüğü, iletişim hakkı ve özel hayatın gizliliği gibi temel haklar, siber yaptırımların hukuki sınırlarını belirlemekte önemli rol oynamaktadır.

Öte yandan, tek taraflı siber karşı önlemler, devletlerin artan biçimde başvurduğu araçlar olmakla birlikte, bağlayıcı bir uluslararası normatif düzenleme eksikliği nedeniyle ciddi meşruiyet sorunları barındırmaktadır. Atfedilebilirlik, orantılılık, geçicilik ve yalnızca zarar gören devlet tarafından uygulanma koşulları gibi unsurlar, karşı önlemlerin uluslararası hukukta hukuka uygun sayılabilmesi için zorunlu kriterlerdir. Ancak siber alanın teknik doğası, bu koşulların sağlanmasını oldukça karmaşık hâle getirmektedir.

Sonuç olarak, siber yaptırımlar ve karşı önlemler, uluslararası hukukun klasik kavramlarını dönüştürme potansiyeline sahip yeni nesil araçlardır. Ancak bu araçların etkin ve meşru şekilde kullanılabilmesi, yalnızca teknik yeterlilikle değil; aynı zamanda açık tanımlara, bağlayıcı normatif düzenlemelere ve insan haklarına duyarlı bir yaklaşımın geliştirilmesine bağlıdır. Uluslararası toplumun,

¹⁵⁶ VOA Türkçe, 'Türkiye ve Mısır Arasında Diplomatik Gerginlik' <<https://www.voaturkce.com/a/misirla-turkiye-arinda-diplomatik-gerginlik/1796256.html>> 23.03.2024. Diken, 'Suudi Arabistan'ın Türk Ürünlerine "Gayriresmi Boykotu" Büyüyor' <<https://www.diken.com.tr/suudi-arabistanin-turk-urunlerine-gayriresmi-boykotu-buyuyor/>> 23.03.2024. T.C. Dışişleri Bakanlığı, 'Türkiye-Ermenistan Siyasi İlişkileri' <<https://www.mfa.gov.tr/turkiye-ermenistan-siyasi-iliskileri.tr.mfa>> 23.03.2024.

¹⁵⁷ Bkz. Ulaştırma ve Altyapı Bakanlığı, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024–2028)* (2024) <<https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf>> 12.04.2024.



siber alana ilişkin kuralları netleştirmek ve mevcut hukuki boşlukları doldurmak amacıyla daha yapıcı ve kapsayıcı girişimlerde bulunması artık bir gereklilik hâline gelmiştir.

KAYNAKÇA

AALCO, *Extraterritorial Application of National Legislation: Sanctions Imposed against Third Parties* (2014) 22 <<http://www.aalco.int/53rdsession/extraterritorial%202014.pdf>> E.T.07.03.2025.

Air Services Agreement of 27 March 1946 (United States v France), Decision of the Arbitral Tribunal

Akdağ İ, *Birleşmiş Milletler Tarafından Gerçekleştirilen Silahsızlanma Çalışmaları ve Türkiye'nin Bu Çalışmalara Yaklaşımı* (Master's thesis, Sosyal Bilimler Enstitüsü 2014).

AP, Russian Cybercrime Network Targeted for Sanctions Across US, UK And Australia, <<https://apnews.com/article/treasury-sanctions-uk-australia-russia-361e788f5482bfd787af01002af2ff4c>> E.T. 12.04.2025 .

Bayram M, 'Angola İç Savaşının Ana Aktörleri ve Uluslararası Ramifikasyonları' (2016) 6(15) *Ordu Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Araştırmaları Dergisi* 365–383.

Benatar M and Gombeer K, 'Cyber Sanctions: Exploring a Blind Spot in the Current Legal Debate' (ESIL 2011 4th Research Forum, 2011).

Birleşmiş Milletler İnsan Hakları Konseyi, *Report of the Special Rapporteur on the Negative Impact of Unilateral Coercive Measures on the Enjoyment of Human Rights*, Idriss Jazairy, UN Doc A/HRC/30/45 (10 August 2015).

Bogdanova I and Callo-Muller M V, 'Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value' (2021) 54 *Vanderbilt Journal of Transnational Law* 911-954.

Bolaman N B, '1980 Sonrası Türkiye-Ortadoğu İlişkilerinin Türk Siyasal Hayatına Etkileri (İran, Irak, Suriye, İsrail, Mısır)' in Savaş AR and Zabun AH (eds), *1980'den Günümüze Türk Siyasal Hayatı: Siyaset, Ekonomi, Dış Politika* (Özgür Yayınları 2023).

Boyle A, 'Soft Law in International Law-Making' in Malcolm D. Evans (ed), *International Law* (Oxford University Press 2014) 118–137.

Bryant R, 'What Kind of Space is Cyberspace' *Minerva-An Internet* (2001) 5 *Journal of Philosophy* 138-155.

Chatinakrob T, 'Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty' (2024) 23(1) *Chinese Journal of International Law* 25-72.

Countering America's Adversaries Through Sanctions Act, Pub L No 115-44, 131 Stat 886 (2 August 2017) <<https://congress.gov/115/plaws/publ44/PLAW-115publ44.pdf>> E.T. 13.05.2025.

Crawford J and Baetens F, 'The Creation of States in International Law' in D Lyons (ed), *Leading Works in International Law* (Routledge 2023) 37-53.

Crawford J, 'The Relationship Between Sanctions and Countermeasures' in Mariano Garcia Rubio and Hassiba Hadj-Sahraoui (eds), *United Nations Sanctions and International Law* (Graduate Institute of International and Development Studies Vol 1, Kluwer Law International 2001).

Crawford J, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge University Press 2002).

Çokışler E, 'Uluslararası Hukukta İkincil Yaptırımlar Açısından Amerika'nın Hasımlarıyla Mücadele Yasası' (2021) 18(69) *Uluslararası İlişkiler Dergisi* 71-86.

Demirkasımoğlu N, 'Nitel Araştırma Geleneğinde Nicel Göstergelerin Kullanımı ve Genellenebilirlik Üzerine Bir Değerlendirme' (2021) 42 *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 231-242.

Denk E, *Uluslararası Örgütler Hukuku: Birleşmiş Milletler Sistemi* (Siyasal Kitabevi 2015).

Dias T, *Countermeasures in International Law and Their Role in Cyberspace* (Research Paper, International Law Programme, May 2024).

Domain Nedir, <<https://www.turk.net/internet-hiz-altyapi-sorgulama>> E.T. 06.05.2025.

Eckert C, Gatzert N and Schubert M, 'Analyzing Spillover Effects from Data Breaches to the US (Cyber) Insurance Industry' (2023) 29(6) *The European Journal of Finance* 669-692.

Elagab O Y, *The legality of non-forcible counter-measures in international law* (PhD Thesis, University of Oxford 1986).

Eslam H. And Tiwari G, 'Cyberspace: Reimagining Cybersecurity and Its Impact on State Sovereignty' in Mohamed Chawki and Ajith Abraham (eds), *Cybercrime Unveiled: Technologies for Analysing Legal Complexity* (Springer 2025).

European Council, Timeline - Sanctions Against Cyber-Attacks, <<https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/timeline-sanctions-cyber-attacks/>> E.T. 13.05.2025).

European Union, Decision (CFSP) 2019/797 — restrictive measures against cyber-attacks threatening the EU or its Member States (2019).

European Union, Regulation 2019/796 — restrictive measures against cyber-attacks threatening the EU or its Member States (2019) <<https://eur-lex.europa.eu/EN/legal-content/summary/eu-restrictive-measures-against-cyber-attacks.html>> E.T.03.03.2025.

Evans D M, *International Law* (2nd edn, Oxford University Press 2006).

Executive Order, ‘Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber Enabled Activities’ (1 April 2015) <<https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>> E.T. 28.05.2024.

Gabčíkovo-Nagymaros Project (Hungary/Slovakia) (Judgment) [1997] ICJ Rep 7.

Ghironi F, Kim D, and Ozhan G. K, ‘International Economic Sanctions and Third-Country Effects’ (2024) 72(2) *IMF Economic Review* 611-652.

Giegerich T, ‘Retorsion’, *Max Planck Encyclopedia of Public International Law* (online edn, Oxford University Press, 2021) <<https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e983?prd=MPIL>> E.T. 15.01.2025.

Cihangir N, ‘The Role of Soft Law and the Interplay Between Soft Law and Hard Law in the Context of International Human Rights’ (2017) 8(14) *Law & Justice Review* 201-219.

Hofer A, ‘The Developed/Developing Divide on Unilateral Coercive Measures: Legitimate Enforcement or Illegitimate Intervention?’ (2017) 16(2) *Chinese Journal of International Law* 175-214.

International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries* (2001).

Joint Communiqué of the 14th Meeting of the Foreign Ministers of the Russian Federation, the Republic of India and the People’s Republic of China (19 April 2016) <http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t1356652.shtml> E.T.05.07.2024.

Jones L, *Societies Under Siege: Exploring How International Economic Sanctions (do not) Work* (Oxford University Press, 2015).

Kafadar M F, ‘Uluslararası Hukukta Devletlerin Sorumluluğu Bağlamında Siber Saldırıların Atfedilebilirliği Meselesi’ (2020) 2 *Galatasaray Üniversitesi Hukuk Fakültesi Dergisi* 1027-1054.

Köchler H, 'Sanctions and International Law' (2019) 14(3) *International Organisations Research Journal* 27-47.

Melzer N, *Cyberwarfare and International Law* (United Nations Institute for Disarmament Research 2011).

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 108.

Milliyet, Türkiye Suriye Elçisini Geri Çekti <<https://web.archive.org/web/20140219172423/http://dunya.milliyet.com.tr/turkiye-suriye-elcisini-geri-cekti/dunya/dunyadetay/26.03.2012/1519878/default.htm>> 23.09.2024.

Mohamad R, 'Unilateral Sanctions in International Law: A Quest for Legality' in Ali Z Marossi and Marisa R Bassett (eds), *Economic Sanctions under International Law* (T.M.C. Asser Press 2015).

Note by the Secretary-General, *Economic measures as a means of political and economic coercion against developing countries*, UN Doc A/48/535 (25 October 1993).

Özkerim Güner N, *İklim Değişikliği Nedeniyle Devletlerin Sorumluluğu* (1st edn, Seçkin Yayıncılık 2018).

Pazarcı H, *Uluslararası Hukuk* (Gözden geçirilmiş 21. baskı, Turhan Kitabevi 2022).

Peksen D, 'Better or worse? The Effect of Economic Sanctions on Human Rights' (2009) 46(1) *Journal of Peace Research* 59-77.

Prosecutor v Duško Tadić aka "Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) (ICTY, 2 October 1995).

Responsabilité de l'Allemagne à raison des dommages causés dans les colonies portugaises du sud de l'Afrique (Portugal v Germany) (Naulilaa Arbitration) (1928) 2 RIAA 1011.

Reuters, UK Discovers Russian 'Espionage Tool', Sanctions GRU Officers over Cyberattacks, <<https://www.reuters.com/world/uk/uk-discovers-russian-espionage-tool-sanctions-gru-officers-over-cyberattacks-2025-07-18/>> E.T.12.04.2025.

Reveron D. S, (ed), *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Georgetown University Press 2012).

Rodríguez F, 'The Human Consequences of Economic Sanctions' (2024) 51(4) *Journal of Economic Studies* 942-963.

Rusinova V and Martynova E, 'Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses' (2024) 57 *Israel Law Review* 135-174.

Ruys T, ‘Sanctions, Retortions and Countermeasures: Concepts and International Legal Framework’ in (eds) *Research Handbook on UN Sanctions and International Law* (Edward Elgar Publishing 2017) 19–51.

Schmitt M N (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017).

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

Schmitt N M, ‘Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law’ (2013) 54 *Virginia Journal of International Law* 697.

Shackelford S J and Andres B R, ‘State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem’ (2010) 42 *Georgetown Journal of International Law* 971-1016.

Špaček S, Laštovička M, Horák M and Plesník T, ‘Current Issues of Malicious Domains Blocking’ in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (IEEE 2019).

Şimşek G. E, ‘Uluslararası Hukuk Açısından Ekonomik Yaptırımlar ve ABD’nin Tek Taraflı Yaptırımlarının Kısa Bir Değerlendirilmesi’ (2020) 78(4) *İstanbul Hukuk Mecmuası* 2049-2078.

T.C. Dışişleri Bakanlığı, ‘Türkiye- Ermenistan Siyasi İlişkileri’ <<https://www.mfa.gov.tr/turkiye-ermenistan-siyasi-iliskileri.tr.mfa>> 23.03.2024.

The Declaration of the Russian Federation and the People’s Republic of China on the Promotion of International Law (25 June 2016) <http://www.mid.ru/en/foreign_policy/news//asset_publisher/cKNonkJE02Bw/content/id/2331698> E.T.01.02.2024.

Tzanakopoulos A, ‘The Right to Be Free From Economic Coercion’ (2015) 4 *Cambridge Journal of International and Comparative Law* 616-633.

UK Government, *Sanctions and Anti-Money Laundering Act 2018* (2018) <<https://www.legislation.gov.uk/ukpga/2018/13/contents>> E.T.01.02.2025.

UK Statutory Instruments, *The Cyber (Sanctions) (EU Exit) Regulations 2020*, No 597 (2020) <<https://www.legislation.gov.uk/ukxi/2020/597/contents/made>> E.T.01.02.2025.

Ulaştırma ve Altyapı Bakanlığı, *Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024–2028)* (2024) <<https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf>> E.T. 12.04.2024.

Uluslararası Hukuk Komisyonu (International Law Commission), *Articles on Responsibility of States for Internationally Wrongful Acts*, 2001).

UN Reports of International Arbitral Awards (RIAA) 415 (1978).

UNGA Res 2131 (XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, UN Doc A/RES/20/2131 (21 December 1965) <<https://www.ilsa.org/Jessup/Jessup15/Declaration%20on%20the%20Inadmissibility%20of%20Intervention%20in%20the%20Domestic%20Affairs%20of%20States%20and%20the%20Protection%20of%20Their%20Independence%20and%20Sovereignty.pdf>> E.T.01.03.2025.

UNGA Res 3281 (XXIX), Charter of Economic Rights and Duties of States (adopted 12 December 1974) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/2778/download>> E.T.04.06.2025> E.T. 12.03.2025.

UNGA Res 56/83, *Articles on Responsibility of States for Internationally Wrongful Acts* (12 December 2001) UN Doc A/RES/56/83 (ARSIWA).

United Nations Human Rights Council, 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' UN Doc A/HRC/32/L.20 (27 June 2016).

United Nations Security Council, 'Resolution 1718 (2006)' (14 October 2006) UN Doc S/RES/1718 (2006).

United Nations Security Council, 'Resolution 2199 (2015)' (12 February 2015) UN Doc S/RES/2199 (2015).

United Nations Security Council, 'Resolution 2341 (2017)' (13 February 2017) UN Doc S/RES/2341 (2017).

United Nations Security Council, 'Resolution 253 (1968)' (29 May 1968) UN Doc S/RES/253.

United Nations Security Council, 'Resolution 277 (1970)' (18 March 1970) UN Doc S/RES/277.

United Nations Security Council, 'Resolution 864 (1993)' (15 September 1993) UN Doc S/RES/864.

United Nations Security Council, *Letter dated 12 October 2001 from the Chairman of the Security Council Committee established pursuant to resolution 864 (1993) concerning the situation in Angola addressed to the President of the Security Council* (12 October 2001) UN Doc S/2001/966.

United Nations Security Council, *Letter dated 27 August 2019 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council* (30 August 2019) UN Doc S/2019/691.

Uzun E, *Devletin Milletlerarası Hukuka Aykırı Eyleminden Sorumluluğu* (PhD thesis, Anadolu University 2007).

Weiss T. G, ‘Sanctions as a Foreign Policy Tool: Weighing Humanitarian Impulses’ (1999) 36(5) *Journal of Peace Research* 499-509.

What Is An IP Address? How Does It Work?, <[https://www.fortinet.com/resources/cyberglossary/what-is-ip-address#:~:text=An%20Internet%20Protocol%20\(IP\)%20address,use%20the%20internet%20to%20communicate](https://www.fortinet.com/resources/cyberglossary/what-is-ip-address#:~:text=An%20Internet%20Protocol%20(IP)%20address,use%20the%20internet%20to%20communicate)> E.T.05.02.2025.

World Trade Organization (WTO), *European Communities – Regime for the Importation, Sale and Distribution of Bananas*, Recourse to Arbitration by the European Communities under Article 22.6 of the DSU, Decision by the Arbitrators, WT/DS27/ARB, 9 April 1999.

Yearbook International Law Commission, 1979 Vol 2, Part 2, Report of the Commission to the General Assembly on the Work of Its Thirty-first Session, <https://legal.un.org/ilc/publications/yearbooks/english/ilc_1979_v2_p2.pdf> E.T.14.02.2025.