Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value

Iryna Bogdanova and María Vásquez Callo-Müller***

ABSTRACT

The current legal vacuum regarding binding international norms regulating malicious conduct in cyberspace has paved the way for the emergence of a unilateral tool: cyber sanctions. They have already been introduced by the United States, the European Union, and the United Kingdom. Notwithstanding their obvious importance, their interrelations with international law—especially international economic law—have remained largely unexplored in academic research. This gap is perplexing given the fact that the existing unilateral cyber sanctions have been formulated in such a way as to be prone to misuse. In particular, they bear a significant potential to disrupt economic relations and undermine global value chains.

The objective of this Article is to explore the legality of unilateral cyber sanctions under international law, including WTO law and international investment agreements. Our analysis reveals that cyber sanctions might, in some instances, violate international law or commitments made under international economic law instruments. Furthermore, cyber sanctions may not be justified as countermeasures, and they most likely would not meet the threshold set by the WTO jurisprudence to be justifiable under the national security exception. Similarly, they could be challenged before investment tribunals for being inconsistent with the international investment standards of treatment. Yet, cyber sanctions might be an effective instrument with the normative potential to regulate behavior in cyberspace. Notwithstanding this, their undefined status under international law has paradoxical implications. On one hand, it can allow ruthless use of unilateral cyber sanctions and the reinforcement of the politics of unilateral power, thus causing significant economic harm. On the other hand, it can undermine the signaling function and deterrence potential embedded in unilateral cyber sanctions.

---

* World Trade Institute, University of Bern, Switzerland. Email: Iryna.Bogdanova@wti.org.

** University of Lucerne, Switzerland. Email: maria.vasquez@unilu.ch.

The authors sincerely thank Dr. Zaker Ahmad for his valuable comments on the earlier drafts.

TABLE OF CONTENTS

I. INTRODUCTION

Unilateral cyber sanctions (or, interchangeably, cyber sanctions) are restrictive economic measures imposed against individuals, legal entities, and government bodies that conduct or facilitate cyberattacks, and are gaining momentum. Cyber sanctions to deter and punish cyberattacks have been already introduced by the United States, the

European Union, and the United Kingdom.[1] Cyber sanctions tend to be a double-edged sword. On one hand, they outlaw certain behaviors in cyberspace. On the other hand, they may also be used as instruments of unfair competition and trade protectionism. The latter concern is especially valid given the recent trend to label technological supremacy as a matter of national security.[2]

Notwithstanding their obvious importance, cyber sanctions and their interrelations with international law have thus far remained largely unexplored in academic research.[3] The current state practice of imposing unilateral cyber sanctions merits further academic discussion for three reasons. First and foremost, the emergence of unilateral cyber sanctions reflects a much deeper problem in international law: the apparent inability to negotiate international rules to regulate conduct in cyberspace, either at the United Nations (UN) level or in multilateral and bilateral trade agreements. As long as no substantial progress is made in any of these forums, cyber sanctions will continue to proliferate. Second, the need for cyber sanctions could drastically increase as the ever-growing digitalization of all aspects of life paves the way for more cyberattacks—in addition to the already existing assaults directed at critical infrastructures, election processes, and personal information of millions of individuals. Third, existing cyber sanctions frameworks have been formulated in such a way as to be prone to misuse. In particular, they apply to a broad range of measures that cover not only conventional cyber threats but also cyber thefts and economic espionage. Furthermore, cyber sanctions target individuals, legal entities, government bodies, as well

---

1. In this article, we do not discuss diplomatic responses to cyberattacks and the invocation of criminal responsibility for such attacks. Put it differently, a narrow definition of sanctions as economic restrictive measures imposed against targeted individuals, legal entities and government bodies, is used.

2. *See generally* Anthea Roberts, Henrique Choer Moraes, & Victor Ferguson, *Toward a Geoeconomic Order in International Trade and Investment*, 22 J. INT'L ECON. L. 655, 666–69 (2019) (discussing technological competition between the United States and China).

3. There are some recent scholarly debates in international law that revolve around the applicability of current international law to cyberspace, including the attribution of cyberattacks and the compatibility of cybersecurity laws and regulations with the World Trade Organization (WTO) commitments. *See, e.g.*, HARRIET MOYNIHAN, THE APPLICATION OF INTERNATIONAL LAW TO STATE CYBERATTACKS: SOVEREIGNTY AND NON-INTERVENTION 3–6, 8–36, 48–51 (2019) (discussing the application and relationship of principles of sovereignty and non-intervention to cyberattacks), https://www.chathamhouse.org/sites/default /files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf (last visited July 25, 2021) [https://perma.cc/C3VH-NABA] (archived July 25, 2021); Monica Hakimi, *Introduction to the Symposium on Cyber Attribution*, 113 AJIL UNBOUND 189, 189–90 (2019) (introducing scholarship regarding cyber attribution challenges); Shin-yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, 18 J. INT'L ECON. L. 449, 457–62, 469–76 (2015) (discussing the relationship between cybersecurity policies and World Trade Organization commitments).

as anyone who provides support or assistance to alleged perpetrators of cyberattacks. Hence, cyber sanctions bear a significant potential to disrupt economic relations and undermine global value chains. Furthermore, in a world heading towards a new geo-economic order, such sanctions might also be abused as instruments of *realpolitik*.

Against this backdrop, the objective of this Article is to fill in the existing gap in the scholarly analysis of cyber sanctions. In particular, it will summarize the existing state practices as well as analyze the cyber sanctions' legality under international law *inter alia* the World Trade Organization (WTO) law and investment regulations. Furthermore, the normative value of cyber sanctions will be explored.

This Article proceeds in three Parts. In the first Part, cyber sanctions are defined, reasons for their increasing use are provided, and relevant state practices are documented. The second Part addresses the legality of cyber sanctions under international law. The final Part focuses on the relations between cyber sanctions and international economic law, in particular the WTO and investment law. The Article concludes with a discussion of the potentially positive contribution of cyber sanctions in signaling the emerging norms regulating cyberspace, as well as the threats associated with the sanctions' excessive use.

II. UNILATERAL CYBER SANCTIONS AS AN EMERGING TREND IN ATTEMPTS TO GOVERN CYBERSPACE

A. *Defining Unilateral Cyber Sanctions*

Unilateral cyber sanctions are restrictive economic measures of a temporary nature, used to punish individuals, entities, and/or government bodies engaged in malicious cyber-enabled activities or cyberattacks. They, as a rule, include asset freezes, restrictions on economic relations with sanctioned persons and/or entities, and travel bans. Contrary to UN-authorized sanctions, unilateral sanctions are enacted based on the domestic laws of individual states, without any prior authorization from any regional or international organization. While domestic regulations setting unilateral cyber sanctions establish criteria for determining their scope of application, the very concepts of "malicious cyber-enabled activities" and "cyberattacks" remain fuzzy.[4]

4. Different policy documents use the terms "malicious cyber activities," "cyber threats," "adverse cyber events," "cyber theft," and "cybercrime" interchangeably. *See, e.g.*, THE COUNCIL OF ECONOMIC ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 2–3 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf (last visited July 25, 2021) [https://perma.cc/CF6A-BT2A] (archived July 25, 2021). Similarly, the literature offers very broad definitions of cyberattacks. For instance, Hathaway et al. have defined cyberattacks as "any action taken to undermine the

In fact, those regulations focus on qualifying certain conduct rather than specifically naming the techniques or technologies used,[5] which often include Distributed Denial of Service Attacks (DDoS),[6] phishing,[7] malware distribution,[8] critical infrastructure vulnerability scanning, among others. This ambiguity in the formulation of cyber sanctions regulations is intentional and provides flexibility in light of the fast-paced evolution of cyber threats.

Unilateral cyber sanctions are imposed not only to deter attacks that are penalized by the existing international treaties and domestic cybercrime laws (e.g., illegal access to computer systems and data interception) but also to discourage attacks that put the stability of a state at risk. The latter category includes attacks detrimental to critical infrastructures and election processes, as well as theft of private firms' intellectual property (e.g., trade secrets).

---

functions of a computer network for a political or national security purpose." Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, & Julia Spiegel, *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 821 (2012).

5. Moyniham argues that "[a]n approach based on quantitative and/or qualitative effects in the target state, or some other form of *de minimis* threshold, is attractive from a practical and pragmatic point of view as it enables states to take action in relation to cyber intrusions that may not reach the threshold of intervention but that nevertheless cause harmful effects within the territory." MOYNIHAN, *supra* note 3, at 23.

6. Distributed Denial-of-Service (DDoS) attacks block access to a computer system for legitimate users. They are implemented by attacking a computer system with more requests than it can handle, thus preventing users from having access to the computer system. Such an attack essentially "overload[s] a victim's server by exploiting communication protocols." Examples of the DDoS attacks include the 2007 attack on Estonia, which resulted in the temporary degradation or loss of service of many commercial and government servers. Miranda Sieg, *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security*, 18 INT'L AFFS. REV. (2009), https://www.iar-gwu.org/blog/2009/04/04/denial-of-service-the-estonian-cyberwar-and-its-implications-for-u-s-national-security (last visited July 25, 2021) [https://perma.cc/8RCJ-DXNG] (archived July 25, 2021).

7. Phishing works by reaching victims through "authentic-looking—but bogus—e-mails to request information from users or direct them to a fake Web site that requests information." KAREN SCARFONE, MURUGIAH SOUPPAYA, AMANDA CODY, & ANGELA OREBAUGH, NAT'L INST. STANDARDS & TECH., SPECIAL PUBLICATION 800-115: TECHNICAL GUIDE TO INFORMATION SECURITY TESTING AND ASSESSMENT F-2 (2008), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial publication800-115.pdf (last visited July 25, 2021) [https://perma.cc/RNP8-2RVJ] (archived July 25, 2021) .

8. Malware distribution means that a program "is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system." MURUGIAH SOUPPAYA & KAREN SCARFONE, NAT'L INST. STANDARDS & TECH., NIST SPECIAL PUB. 800-83 REVISION 1: GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING FOR DESKTOPS AND LAPTOPS 2 (2013), https://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-83r1.pdf (last visited July 25, 2021) [https://perma.cc/GWD4-NWN4] (archived July 25, 2021).

Malicious cyber-enabled activities and cyberattacks have been on the rise for many years. Yet, their dangerous nature has taken new dimensions given attacks on critical infrastructures and health systems during the COVID-19 pandemic.[9] In the present context, the danger stems from the potential infiltration of servers[10] along with the potential spread of misinformation.[11] In fact, the latter has been one of the key concerns in democratic societies.

B. *Motivations behind the Adoption of Unilateral Cyber Sanctions*

1. Unsuccessful International Efforts to Regulate Cyberspace

Despite the fact that the scale and effects of malicious cyber-enabled activities and cyberattacks are transborder in nature, often "affecting users of cyber systems throughout the world,"[12] international norms regulating responsible state and non-state behaviors in cyberspace are nonexistent. In fact, the very concepts of "cybercrime," "cyberattack," and "cyber war" suffer from a lack of internationally accepted distinctions, thus making "concerted international action more difficult to achieve."[13]

This situation should not lead us astray. The deliberations on the rules of conduct in cyberspace are not new both in the policy and scholarly debates. The rapid development of the information and communication technologies and their interaction with international security engendered global discussions as early as 1999.[14] Since then, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE), has been the main forum for the discussion of global cyber norms.

---

9. Zeke Miller & Colleen Long, *US Officials: Foreign Disinformation is Stoking Virus Fears*, ASSOCIATED PRESS (March 16, 2020), https://apnews.com/7edbc93627b1040a422f2d07f50d4cda [https://perma.cc/94DZ-PY5R] (archived July 25, 2021).

10. *People's Republic of China (PRC) Targeting of COVID-19 Research Organizations,* US CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, (May 13, 2020), https://www.cisa.gov/news/2020/05/13/fbi-and-cisa-warn-against-chinese-targeting-covid-19-research-organizations [https://perma.cc/53LZ-8PPN] (archived July 26, 2021).

11. Marko Milanovic & Michael Schmitt, *Cyber Attacks and Cyber (Mis)information Operations during a Pandemic* 11 J. NAT'L SEC. L. & POL'Y 247, 266–70 (2020).

12. Abraham D Soafer, David Clark, & Whitfield Diffie, *Cyber Security and International Agreements*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 179, 179 (2010).

13. ANTONIA CHAYES, BORDERLESS WARS: CIVIL MILITARY DISORDER AND LEGAL UNCERTAINTY 138 (2015).

14. *See* G.A. Res. 53/70, at 1–3 (Jan. 4, 1999).

In certain areas the GGE's work has been fructiferous, while in others rather limited. For instance, in its reports issued in 2013[15] and 2015,[16] the GGE confirmed the applicability of international law, including the Charter of the United Nations (UN Charter), to cyberspace.[17] However, in 2017, the GGE members could not find a common stance on the application of particular norms of international law in cyberspace (i.e., countermeasures, state responsibility, and international humanitarian law), and therefore were unable to reach an agreement towards a final report.[18] Interestingly, the GGE has never suggested the involvement of the United Nations Security Council (UN Security Council) in cyber affairs. So far, none of the states participating in the GGE have brought to the attention of the UN Security Council "the acuteness of the politico-military threat, let alone a threat to international peace and security, breach of the peace or act of aggression that the UN Charter points to,"[19] that certain uses of information and communication technologies might entail. Despite these unsettled aspects, the GGE was tasked to study how to advance responsible state behavior in cyberspace in the context of international security.[20] A report is expected to be delivered in 2021.[21]

Parallel to the above, a separate UN resolution sponsored by the Russian Federation established an Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG).[22] This clearly showcases the frictions among the UN members regarding the setting of international

---

15. Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. & Telecomms. in the Context of Int'l Sec., ¶ 19, U.N. Doc. A/68/98 (June 24, 2013).

16. Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. & Telecomms. in the Context of Int'l Sec., ¶ 24, U.N. Doc. A/70/174 (July 22, 2015).

17. Chair's Summary: Informal Consultative Meeting of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the context of International Security, 4 (2019), https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf (last visited July 6, 2020) [https://perma.cc/S9Y9-TS4J] (archived July 26, 2021).

18. *See, e.g.*, Adam Segal, *The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?*, COUNCIL ON FOREIGN RELATIONS (June 29, 2017, 11:07 AM), https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what [https://perma.cc/V4UV-ZE8K] (archived July 26, 2021).

19. Eneken Tikk & Niels Nagelhus Schia, *The Role of the UN Security Council in Cybersecurity*, *in* ROUTLEDGE HANDBOOK OF INTERNATIONAL CYBERSECURITY, 5 (Eneken Tikk & Mika Kerttunen eds., 2020).

20. *See* G.A. Res. 73/266, ¶ 3 (Dec. 22, 2018).

21. *See* Rep. of the Grp. Of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of Int'l Sec. (May 28, 2021), https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf (last visited July 26, 2021) [https://perma.cc/BSX5-EJCL] (archived July 27, 2021) (providing an advanced copy of the report).

22. G.A. Res. 73/27, ¶ 5 (Dec. 5, 2018).

norms for cyberspace.[23] The main difference between the GGE and the OEWG is the nature of stakeholders involved: the latter includes not only governments but also non-government actors.[24] More recently, and upon the completion of the OEWG mandate, a new OEWG on security and the use of information and communications technologies was established for the period 2021–2025. The new OEWG is tasked *inter alia* to continue working on the development of "the rules, norms and principles of responsible behaviour of States and the ways for their implementation."[25]

Despite the ongoing discussions, scholars suggest that the expectations regarding the outcome of the UN processes should be "tempered."[26] There are different reasons for this, including geopolitics and a simple desire of states to use certain forms of malicious cyber activity in their own interests. These considerations discourage states from agreeing to binding international norms.

Besides efforts at the UN level, debates about regulation of behavior in cyberspace have also taken place in other forums. Yet, their impact remains insufficient. For instance, various regional groupings have discussed and advanced relevant frameworks, including the G7[27] and groups from regions such as Africa[28] and Asia.[29]

The WTO is another venue unlikely to discuss responsible state behavior in cyberspace. This conclusion stands despite the fact that one of the main causes of the current "trade war" between the United States and China emanates from the practices undertaken by the

---

23. *See* Alex Grigsby, *The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased,* COUNCIL ON FOREIGN RELS., (Nov. 15, 2018, 11:48 PM), https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased [https://perma.cc/3UKZ-Y53L] (archived July 26, 2021) (discussing the possible challenges of having separate groups).

24. *See Open-ended Working Group*, UNITED NATIONS, OFF. FOR DISARMAMENT AFFS. https://www.un.org/disarmament/open-ended-working-group/ (last visited July 26, 2021) [https://perma.cc/HQ2E-STY4] (archived July 26, 2021) (providing membership information).

25. G.A. Res. 75/240, ¶ 1 (Jan. 4, 2021).

26. Martin C. Libicki, *Norms and Normalization*, 5 CYBER DEF. REV. 41, 42 (2020).

27. G7, *Dinard Declaration on the Cyber Norm Initiative* 1–2 (Apr. 6, 2019), http://www.g7.utoronto.ca/foreign/g7_-_dinard_declaration_on_cyber_initiative.pdf (last visited July 27, 2021) [https://perma.cc/L3U4-VDV2] (archived July 27, 2021).

28. African Union, *African Union Convention on Cyber Security and Personal Data Protection,* 1, AU No. EX.CL/846(XXV), (June 27, 2014), https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [https://perma.cc/VG4L-76AH] (archived Aug. 12, 2021).

29. *Chairman's Statement of the 3rd ASEAN Ministerial Conference on Cybersecurity*, 1–2 (Sept. 19, 2018), https://asean.org/storage/2018/09/AMCC-2018-Chairmans-Statement-Finalised.pdf (last visited July 27, 2021) [https://perma.cc/RNX4-8L7F] (archived July 27, 2021).

latter with regard to cyber theft.[30] To further buttress this Article's assertion, it should be noted that WTO members' submissions for a plurilateral trade agreement on e-commerce do not address cybersecurity in depth. While a number of WTO members have stressed the need to strengthen capabilities to prevent and respond to cybersecurity incidents,[31] and some even have suggested the adoption of risk-based frameworks,[32] those suggestions do not prescribe specific cybersecurity obligations or rules regulating states' conduct in cyberspace. Furthermore, even if there would be rules penalizing malicious behavior, their enforceability may be hindered given the weakened WTO dispute settlement mechanism.[33]

Multilateral and bilateral trade agreements constitute another possible avenue to negotiate rules to limit malign state behavior in cyberspace. Notably, such agreeements have been less studied as sources of cyber norms, but countries agreeing on enforceable rules within trade agreements remain a bleak prospect. Indeed, while such treaties increasingly incorporate e-commerce and digital trade chapters, the provisions on cybersecurity are of a restricted scope and cooperative nature.[34] Even the recent Digital Economy Partnership Agreement does not go beyond recognizing that

> cybersecurity underpins the digital economy . . . The Parties further recognise the importance of: (a) building capabilities of their national entities responsible for computer security incident response; (b) using existing collaboration mechanism to cooperate to identify and mitigate malicious intrusions . . . and (c) workforce development in the area of cybersecurity, including through possible initiatives relating to mutual recognition of qualifications.[35]

---

30. *See, e.g.*, Julia Ya Qin, *Forced Technology Transfer and the US–China Trade War: Implications for International Economic Law*, 22 J. INT'L ECON. L. 743, 743 (2019) (discussing forced technology transfer and regulations on technology transfer).

31. Joint Statement on Electronic Commerce – Communication from Singapore, 3, WTO Doc. INF/ECOM/6 (Mar. 25, 2019); Joint Statement on Electronic Commerce – Communication from Ukraine, ¶ 9.1 WTO Doc. INF/ECOM/14 (Sept. 19, 2018); Joint Statement on Electronic Commerce – Communication from Brazil, 8, WTO Doc. INF/ECOM/17 (Mar. 25, 2019); Joint Statement on Electronic Commerce – Communication from China, ¶ 3.11, WTO Doc. INF/ECOM/19 (Apr. 24, 2019).

32. Joint Statement on Electronic Commerce initiative – Communication from the United States, ¶ 5.1, WTO Doc. INF/ECOM/5 (Mar. 25, 2019).

33. *See generally* TETYANA PAYOSOVA, GARY CLYDE HUFBAUER, & JEFFREY J. SCHOTT, THE DISPUTE SETTLEMENT CRISIS IN THE WORLD TRADE ORGANIZATION: CAUSES AND CURES (2018) (discussing challenges facing the WTO dispute resolution mechanism).

34. *See, e.g.*, Comprehensive and Progressive Agreement for Trans-Pacific Partnership, art. 14–16, Mar. 8, 2018, A.T.S. 23 (Austl.) [hereinafter CPTPP] (recognizing the importance of cooperation in cybersecurity matters).

35. Digital Economy Partnership Agreement (hereinafter cited as DEPA), art. 5.1, June 12, 2020, https://www.treaties.mfat.govt.nz/search/details/t/3945 [https://perma.cc/X76R-6BYK] (archived July 27, 2021).

Unfortunately, none of this is groundbreaking. For instance, many states already have agencies authorized to handle cyber incidents (e.g., Computer Incident Response Teams)[36] and there are even examples of regional cooperation (e.g., the Asia-Pacific Computer Emergency Response Team Programme).[37] The only novelty, in this context, is the preference towards a risk-based approach in norm-making, as reflected in Article 19.15 of the United States-Mexico-Canada Agreement, which underlines that "[g]iven the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats."[38]

Soft law instruments emerged to fill in the vacuum left by the lack of binding international norms. The Tallinn Manual 2.0,[39] possibly the most important contemporary document regarding the application of international law to cyberspace, contains 154 rules, including a general obligation to prevent malicious cross-border computer network operations,[40] and rules on countermeasures.[41] However, analysis of state practice reveals the lack of a general acceptance of these rules, making it "difficult to ascertain whether states accept the Tallinn Rules and wish them to become authoritative articulations of international law governing cyberoperations."[42] In this regard, Dan Efrony and Yuval Shany point out that "some states tend to go out of their way to avoid relying publicly and explicitly on specific rules of international law . . . in connection with cyberoperations, and opt instead for a policy of silence and ambiguity."[43]

Notwithstanding a great deal of effort, there is a vacuum of binding rules in international law regarding regulation of malicious cyber-enabled activities and cyberattacks. Some scholars suggest following closely the emergence of customary international law as a basis for the law applicable in cyberspace, but scarce state practice poses the main challenge for such an approach.[44] This is not surprising

---

36. ITU, National CIRT, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx (last visited July 27, 2021) [https://perma.cc/BQ2Z-7GUV] (archived July 27, 2021).

37. APCERT, Member Teams, https://www.apcert.org/about/structure/members.html (last visited July 27, 2021) [https://perma.cc/N2ZF-2PK3] (archived July 27, 2021).

38. Agreement between the United States of America, the United Mexican States, and Canada, art. 19.15, Can.-Mex-U.S., Dec. 10, 2019, 19 USCS §§ 4501 [hereinafter USMCA].

39. MICHAEL N. SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Cambridge Univ. Press 2017) [hereinafter TALLINN MANUAL 2.0].

40. *Id*. at 27–29.

41. *Id*. at 111–42.

42. Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 585 (2018).

43. *Id*. at 586.

44. MOYNIHAN, *supra* note 3, at 56.

given that only in the last decade many states have begun to enact cybersecurity laws, which often contain specific provisions directed at reducing the risks to critical infrastructure. These laws have already provoked heated debates in international forums.[45] In some cases, recent cybersecurity laws are inspired by the long-standing cybercrime treaties,[46] for instance the Council of Europe Convention on Cybercrime,[47] which is "[t]he closest to a formal norm for cyberspace."[48] In fact, the Council of Europe Convention on Cybercrime remains the most significant legally binding document that prescribes provisions to penalize illegal access and interception, data and system interference, and misuse of devices,[49] as well as provisions on mutual assistance in investigation and criminal proceedings.[50] Nonetheless, the convention's application to current cyberattacks is limited. One key reason for that is neither Russia nor China is a signatory to it. Another reason is that the existing cross-border information sharing and mutual legal assistance in the convention remains somewhat inadequate.

The private sector has also undertaken steps towards regulating conduct in cyberspace. In fact, the development of cybersecurity norms has always been led by the private sector. The following initiatives can illustrate this trend: the Cybersecurity Tech Accord proposed by Microsoft,[51] the Siemens Charter of Trust,[52] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[53]

---

45. *See* Council for Trade in Services, *Note by the Secretariat: Report of the Meeting Held on 7 December 2018*, WTO Doc. S/C/M/137, (Jan. 24, 2019) (providing information about comments from the delegations during the meeting).

46. Cristina Schulman, *Legislation and Legal Frameworks on Cybercrime and Electronic Evidence: Some Comments on Developments 2013 – 2018* (2018), https://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/SCHULMAN_Item_2.pdf (last visited July 27, 2021) [https://perma.cc/LRQ9-334Z] (archived on July 27, 2021).

47. Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13, 174, E.T.S. No. 185.

48. Libicki, *supra* note 26, at 42.

49. Convention on Cybercrime, *supra* note 47, at art. 2–6.

50. *Id.* at arts. 25, 29, 31.

51. Microsoft, *About the Cybersecurity Tech Accord*, CYBERSECURITY TECH ACCORD, https://cybertechaccord.org/about/ (last visited July 20, 2021) [https://perma.cc/6VJH-YN3A] (archived July 20, 2021).

52. Hubertus Breuer & Sebastian Webel, *Charter of Trust*, SIEMENS (Feb. 15, 2019), https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity/cybersecurity-charter-of-trust.html [https://perma.cc/LA42-QGYG] (archived July 20, 2021).

53. *See Cybersecurity Framework*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/industry-impacts/cybersecurity-framework (last visited July 20, 2021) [https://perma.cc/P8PL-ATFR] (archived July 20, 2021) (while the Cybersecurity Framework was facilitated by a public entity, private entities were the Framework's primary stakeholders).

In view of the foregoing, it should be emphasized that numerous attempts outlined above have not culminated in the creation of binding and enforceable international norms. Hitherto, international efforts did not bring significant results in terms of hard laws. Achievements so far are mainly composed of declarations or soft law instruments (e.g., the Tallinn Manual 2.0). Thus, malicious cyber-enabled activities and cyberattacks continue to evade scrutiny under international law. It follows logically that when international and multilateral frameworks of enforcement remain unattainable, unilateral measures are used more widely to fill in the existing lacuna.

2. Unilateralism as an Alternative Approach for Cyberspace Regulation

Against the background of failed international attempts to regulate cyberspace, the angle of the discussion shifted—scholars and policymakers have focused on unilateral measures and their potential. To demonstrate the potential of unilateralism in the creation of cyber norms, Libicki argues that normalization (which is defined as actual state conduct or *de facto* norms), rather than norms, is more likely to determine the activities that are deemed legitimate or illegitimate in cyberspace.[54] Eneken Tikk contends that cyber consequences, defined as unilateral responses of states to malicious behavior in cyberspace, clarify international law,[55] reflect national ambitions and capabilities,[56] contribute to the formulation of norms and customary international law,[57] and may even convene similarly minded coalitions of states.[58] Discussing the potential contributions of unilateralism to international law, Monica Hakimi has previously highlighted the normative role that unilateralism plays in shaping and setting new international norms.[59] Hence, it is reasonable to put forward the hypothesis that current cyber sanctions imposed by the United States, the European Union, and the United Kingdom could be signaling red lines in cyberspace.[60] Thus, unilateral cyber sanctions should be

54. Libicki, *supra* note 26, at 44, 50.

55. Eneken Tikk, *Will Cyber Consequences Deepen Disagreement on International Law?*, 32 TEMP. INT'L & COMPAR. L.J. 185, 187 (2018) ("States clarify international law by condemning certain behavior . . . .").

56. *Id.* at 191.

57. *Id.*

58. *Id.* at 191–92.

59. Monica Hakimi, *Unfriendly Unilateralism*, 55 HARV. INT'L L.J. 105, 109, 125–41 (2014).

60. This conclusion is in line with the academic literature on economic sanctions wherein it is argued that economic sanctions contribute to the formulation of an international norm. *See generally* CLARA PORTELA, TARGETED SANCTIONS AGAINST INDIVIDUALS ON GROUNDS OF GRAVE HUMAN RIGHTS VIOLATIONS – IMPACT, TRENDS AND PROSPECTS AT EU LEVEL 10 (2018).

carefully studied: they could substantiate the crystallization of customary international law regarding responsible state behavior in cyberspace.

Furthermore, unilateral cyber sanctions could also play a part in wider cyber deterrence strategies.[61] Cyber deterrence is a concept associated with cyberwar, which has been thoroughly explored in policy discussions and academic research. However, cyber deterrence is not easy to apply in practice. One of the main difficulties is the attribution of cyberattacks to a particular actor given the anonymous nature of the internet.[62] Taking into account this complexity, some have argued that "cyber deterrence started to fade to the extent that it is now intentionally neglected."[63] The growing number of unilateral cyber sanctions imposed to deter cyberattacks could contribute to the reevaluation of the concept of cyber deterrence and spark the debate on the role of economic instruments in deterring malign behavior in cyberspace.

To bolster this view, it should be noted that during the G7 summit in 2019 the participating states discussed financial sanctions as a possible deterrence mechanism against cyberattacks.[64] Despite the fact that the final declaration of the G7 summit does not reflect these discussions,[65] they demonstrate that the debate on the role of economic sanctions to deter cyberattacks is pertinent and timely.

Legal scholars have not discussed unilateral cyber sanctions in depth, despite their normative significance in signaling the emergence of customary international law, as well as their practical utility in facilitating cyber deterrence.[66] In particular, contributions in the field of international economic law mostly examine the content and trade-related aspects of emerging cybersecurity laws, their possible implications for cross-border data flows,[67] or the practice of leveraging

---

61. In the context of international economic law, the use of cyber sanctions as wider deterrence measures has been already advanced by Claussen, albeit with emphasis on the US practice. Kathleen Claussen, *Beyond Norms: Using International Economic Tools to Deter Malicious State-Sponsored Cyber Activities*, 32 TEMP. INT'L & COMPAR. L.J. 113, 122 (2018).

62. *See, e.g.*, David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 350–51 (2011).

63. Max Smeets & Stefan Soesanto, *Cyber Deterrence Is Dead. Long Live Cyber Deterrence!*, COUNCIL ON FOREIGN RELS. (Feb. 18, 2020, 10:27 AM), https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence (last visited July 21, 2021) [https://perma.cc/EU8M-BN3B] (archived July 21, 2021).

64. Victor Mallet, *G7 Plans Strategy to Protect Against Cyber Attacks*, FIN. TIMES (Apr. 6, 2019), https://www.ft.com/content/25db4acc-5845-11e9-939a-341f5ada9d40 (subscription required) [https://perma.cc/F4Z4-HHEM] (archived July 22, 2021).

65. *Id.*

66. *See, e.g.*, Claussen, *supra* note 61, at 120–24 (highlighting that Claussen is among the few scholars considering how unilateral sanctions facilitate cyber deterrence).

67. *See* Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, 21 J. INT'L ECON. L. 769, 769–72, 777–79 (2018);

market access on the requirement to disclose a source code of software.[68] Yet, cyber sanctions have not been examined, partially because of their novelty but also because they are not a part of general cybersecurity laws.[69] In view of this, the next subpart sheds light on states' practices of applying unilateral cyber sanctions and the extent to which this complies with international law, particularly international economic law.

C. *Current State Practices*

The United States, the European Union, and the United Kingdom have specific regulatory frameworks allowing the imposition of cyber sanctions. As of this writing, the United States, the European Union, and the United Kingdom have already relied upon these legal frameworks to sanction individuals, legal entities, and governmental bodies for various types of malicious cyber-enabled activities, including cyberattacks.

1. The United States

The United States has imposed targeted cyber sanctions against individuals and entities engaged in significant malicious cyber-enabled activities since 2015.[70] Since December 2016, US cyber sanctions have also covered malicious cyber-enabled activities that undermine democratic processes or institutions.[71] The previous Trump administration[72] and the current Biden administration have been

---

see also Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 21 J. INT'L ECON. L. 245 (2018); AMY PORGES & ALICE ENDERS, THE E15 INITIATIVE, DATA MOVING ACROSS BORDERS: THE FUTURE OF DIGITAL TRADE POLICY (Apr. 2016), http://e15initiative.org/wp-content/uploads/2015/09/E15-Digital-Economy-Porges-and-Enders-Final.pdf (last visited May 17, 2020) [https://perma.cc/6BC2-WPXG] (archived July 26, 2021); Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015).

68. *See, e.g.*, Ya Qin, *supra* note 30, at 745–46.

69. Cyber sanctions, as reviewed in Part II.C, are stand-alone instruments applied on an *ad hoc* basis. In contrast, cybersecurity laws establish which acts are considered to constitute cybercrime and set legal responses in the form of administrative, civil, and criminal measures. *See* THE WORLD BANK & UNITED NATIONS, COMBATTING CYBERCRIME: TOOLS AND CAPACITY BUILDING FOR EMERGING ECONOMIES 157–70 (2017), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cyber crime-toolkit.pdf (last visited July 26, 2021) [https://perma.cc/9UUY-5QS6] (archived July 26, 2021).

70. Exec. Order No. 13,694, 3 C.F.R. § 297 (2016), *amended by* Exec. Order. No. 13,757, 3 C.F.R. § 659 (2017).

71. *See* 3 C.F.R. § 659.

72. DONALD J. TRUMP, CONTINUATION OF THE NATIONAL EMERGENCY WITH RESPECT TO SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES, H.R. DOC. NO. 116-111 (2020).

prolonging cyber sanctions regulations annually, and the last of such extensions took place in March 2021.[73]

According to the US framework, there are three main categories of malicious cyber-enabled activities: (i) malicious attacks on computers/computer networks supporting critical infrastructure sectors or causing significant disruptions,[74] (ii) cyber theft and trade secrets misappropriation through cyber-enabled means,[75] and (iii) "misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions."[76]

Malicious cyber-enabled activities are remedied by economic sanctions if those activities "are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States."[77] If this is the case, sanctions can be imposed against "any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State" on the grounds of being "responsible for or complicit in" or for having "engaged in, directly or indirectly" the abovementioned activities.[78] In this regard, some scholars have argued that the U.S. Secretary of the Treasury "has the discretion to rely upon whatever level of confidence he chooses"[79] in establishing cyber sanctions. Furthermore, cyber sanctions are imposed without prior judicial review or independent evaluation, and attempts to challenge them before domestic courts may not always be successful.[80]

The US framework for cyber sanctions also contemplates sanctions against persons that have "materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of" malicious cyber-enabled activities.[81] For example, in 2018, two Iranians were sanctioned for providing material support to a malicious cyber activity.[82]

---

73. Joseph R. Biden, Jr., *Notice on the Continuation of the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities*, WHITE HOUSE (Mar. 29, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/03/29/notice-on-the-continuation-of-the-national-emergency-with-respect-to-significant-malicious-cyber-enabled-activities/ [https://perma.cc/X2H7-SPYF] (archived July 25, 2021).

74. 3 C.F.R. § 659(1)(a)(ii)(A)–(C).

75. *Id.* at § 659(1)(a)(ii)(D).

76. *Id.* at § 659(1)(a)(ii)(E).

77. *Id.* at § 659(1)(a)(ii).

78. *Id.*

79. *See, e.g.*, Kathleen Claussen, *Economic Cybersecurity Law*, *in* ROUTLEDGE HANDBOOK OF INTERNATIONAL CYBERSECURITY 341, 348 (Eneken Tikk & Mika Kerttunen eds., 2020).

80. *See infra* Part III.A.2.

81. 3 C.F.R. § 659(1)(a)(iii)(B).

82. *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses*, U.S.

Moreover, the US cyber sanctions apply to the legal entities that are "owned or controlled" by sanctioned individuals/entities and to anyone who has "acted or purported to act for or on behalf of, directly or indirectly," sanctioned individuals/entities.[83] What is more, anyone who has attempted to engage in any of the abovementioned activities could also be sanctioned.[84]

Cyber sanctions take the form of (i) blocking of property and interests in property, (ii) travel bans, and (iii) a blanket ban on the donations to and from targets.[85] The regulations provide a broad definition of "property and interests in property."[86] As a result, not only can financial assets (bank deposits, financial instruments, etc.) be blocked, but the provision of "services of any nature whatsoever," signature of "contracts of any nature," and transactions related to "any other property" are also completely prohibited.[87] The US sanctions prohibit ransom payments to be paid to the targeted malicious cyber actors, and, likewise, persons facilitating ransomware payments on behalf of a victim may violate such sanctions.[88]

Other executive orders, which pursue objectives of detecting and deterring malicious cyber-enabled activities, have been recently issued.[89] Rules prescribed by these regulations might significantly undermine both importation and exportation of the information and communications technology and services to and from the United States, thus undermining the existing supply chains.[90] The particular

---

DEP'T OF THE TREASURY (Nov. 28, 2018), https://home.treasury.gov/news/press-releases/sm556 [https://perma.cc/F8NQ-E6DX] (archived July 26, 2021).

83. 3 C.F.R. § 659(1)(a)(iii)(C).

84. *Id.* at § 659(1)(a)(iii)(D).

85. *Id.* at § 659(1)(a); 3 C.F.R. §297(2)–(4) (2016).

86. 31 C.F.R. §§ 578.301, 578.305, 578.309 (2015).

87. 31 C.F.R. §§ 578.201, 578.309 (2015).

88. U.S. DEP'T OF THE TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISKS FOR FACILITATING RANSOMWARE PAYMENTS 2–3, (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf (last visited July 25, 2021) [https://perma.cc/3RQZ-KDCK] (archived July 25, 2021).

89. Exec. Order No. 13,873, 84 Fed. Reg. 22689 (May 17, 2019); Exec. Order No. 13,984, 86 Fed. Reg. 6837 (Jan. 25, 2021).

90. For example, Executive Order 13873 grants the Secretary of Commerce the authority to prohibit "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology" and services if the Secretary of Commerce, in consultation with other agency heads, determines that such technology and/or services were "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" and pose an unacceptable risk. Exec. Order No. 13,873, 84 Fed. Reg. at 22689-90. The proposed list of "foreign adversaries" for the purposes of this regulation includes China, Cuba, Iran, North Korea, Russia, and Venezuelan politician Nicolás Maduro (Maduro Regime). 15 C.F.R. § 7.4 (2021). Executive Order 13984 prescribes rules that pursue the objective of restricting the use of the "United States infrastructure as a service" by foreign malicious cyber actors. To achieve this ambitious goal, persons engaged in export transactions must follow numerious procedures to verify their customers. Such

rules implementing these new policies are still under consideration and should be announced later this year.[91] Although these regulations are not economic sanctions in the meaning of the US legislation, their application might imply import and export restrictions analogous to targeted sanctions (i.e., either deprive foreign-based companies from market access or prohibit exportation of goods and/or services of US origin). What is more, ambiguous formulations and broad categories of goods and services to which restrictions apply would further reinforce their detrimental effects.

The United States invoked cyber sanctions to respond to a number of events. For instance, in March 2016, the United States introduced sanctions against North Korea, in particular against persons that "have engaged in significant activities undermining cybersecurity through the use of computer networks or systems against targets outside of North Korea on behalf of the Government of North Korea or the Workers' Party of Korea."[92] In accordance with these sanctions, the North Korean computer programmer Park Jin Hyok as well as the entity for which he worked, Chosun Expo Joint Venture, was added to the list of sanctioned persons.[93] In September 2019, these sanctions were extended to three North Korean state-sponsored cyber groups—Lazarus Group, Bluenoroff, and Andariel.[94]

Furthermore, in 2018, the United States sanctioned Russian individuals as well as legal entities to counter "malign Russian cyber activity, including their attempted interference in U.S. elections, destructive cyberattacks, and intrusions targeting critical infrastructure."[95] In late December 2018, a new wave of cyber

---

procedural hurdles may have a "chilling effect" on exportation of technology and services. Furthermore, restrictions targeting foreign jurisdictions or foreign persons may be implemented to reinforce the objectives of this regulation. *See* Exec. Order No. 13,984, 86 Fed. Reg. at 6837–39.

91. The regulation implementing Exec. Order No. 13984 68 Fed. Reg. 6837 has not been announced yet.

92. Exec. Order No. 13,722, 3 C.F.R. § 446 (2017) [hereinafter Exec. Order No. 13,722].

93. *Treasury Targets North Korea for Multiple Cyber-Attacks*, U.S. DEP'T OF THE TREASURY (Sept. 6, 2018), https://home.treasury.gov/news/press-releases/sm473 [https://perma.cc/662Y-SM8Z] (archived July 25, 2021) ("Park Jin Hyok is part of the conspiracy responsible for conducting, among others, the February 2016 cyber-enabled fraudulent transfer of $81 million from Bangladesh Bank, the ransomware used in the May 2017 'WannaCry 2.0' cyber-attack, and the November 2014 cyber-attack on Sony Pictures Entertainment. Park Jin Hyok worked for Chosun Expo Joint Venture (a.k.a Korea Expo Joint Venture or 'KEJV'), which OFAC is simultaneously sanctioning today for being an agency, instrumentality, or controlled entity of the Government of North Korea").

94. *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, U.S. DEP'T OF THE TREASURY (Sept. 13, 2019), https://home.treasury.gov/news/press-releases/sm774 [https://perma.cc/32U4-7KVK] (archived July 25, 2021).

95. Three entities and 13 individuals were designated pursuant to Executive Order 13694, which targets malicious cyber actors, including those involved in

sanctions directed against Russian individuals, legal entities, and government officials was announced.[96]

On June 16, 2020, Nigerian nationals were included on the US cyber sanctions list.[97] These individuals were sanctioned for masterminding and implementing two types of cyber fraud, namely business email compromise[98] and romance fraud.[99] According to the U.S. Department of the Treasury, the sanctioned individuals have stolen "over six million dollars from victims across the United States."[100]

In September 2020, Russian nationals, who are employed by the Internet Research Agency, were added to the list of sanctioned individuals.[101] Additionally, in October 2020 a Russian government research institution, which is allegedly connected to the destructive Triton malware, was designated pursuant to Section 224 of the Countering America's Adversaries Through Sanctions Act.[102] Section 224 of this Act allows imposition of unilateral sanctions against any person on the territory of the Russian Federation who knowingly engages in significant activities undermining cybersecurity.[103]

---

interfering with election processes or institutions. Two entities and six individuals were designated pursuant to Section 224 of the Countering America's Adversaries Through Sanctions Act (CAATSA), which targets cyber actors operating on behalf of the Russian government. *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks*, U.S. DEP'T OF THE TREASURY (Mar. 15, 2018), https://home.treasury.gov/news/press-releases/sm0312 [https://perma.cc/4945-VHCE] (archived July 25, 2021); *see* Countering America's Adversaries Through Sanctions Act § 224, 22 U.S.C. § 9524.

96. *Treasury Targets Russian Operatives over Election Interference, World Anti-Doping Agency Hacking, and Other Malign Activities*, U.S. DEP'T TREASURY (Dec. 19, 2018), https://home.treasury.gov/news/press-releases/sm577 [https://perma.cc/SV38-KJSD] (archived July 25, 2021).

97. *Treasury Sanctions Nigerian Cyber Actors for Targeting U.S. Businesses and Individuals*, U.S. DEP'T TREASURY (June 16, 2020), https://home.treasury.gov/news/press-releases/sm1034 [https://perma.cc/623X-GE77] (archived July 25, 2021).

98. Business email compromise is a fraud scheme, in which scammers "impersonated business executives and requested and received wire transfers from legitimate business accounts." *Id.*

99. Romance fraud is a fraud scheme, in which scammers "masqueraded as affectionate partners to gain trust from victims." *Id.*

100. *Id.*

101. Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Russia-Linked Election Interference Actor (Sept. 10, 2020), https://home.treasury.gov/news/press-releases/sm1118 [https://perma.cc/CYM3-TM86] (archived July 24, 2021).

102. Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware (Oct. 23, 2020), https://home.treasury.gov/news/press-releases/sm1162 [https://perma.cc/3RQY-WYF4] (archived July 24, 2021).

103. Countering America's Adversaries Through Sanctions (CAATSA), Pub. L. No. 115-44 (2017) (codified as amended at 22 U.S.C. 9501 § 224).

In April 2021, new US sanctions against the Russian Federation were announced.[104] Some of the newly imposed restrictions target Russian technology companies "that support the Russian Intelligence Services' efforts to carry out malicious cyber activities against the United States" and are enacted pursuant to the cyber sanctions framework.[105]

Although the current cyber sanctions regime prescribes sanctions for cyber theft, no such measures have been imposed according to the cyber sanctions framework. The only example of US action against cyber-enabled theft and cyber-hacking is the imposition of additional *ad valorem* duties imposed on products imported from China.[106]

2. The European Union

The EU announced the development of a framework to respond to cyberattacks in 2017.[107] The new framework for cyber sanctions was introduced in 2019.[108] In May 2020, the EU renewed its cyber sanctions regime for another year.[109] A number of non-EU states have expressed their intention to align themselves with the EU cyber sanctions.[110] Norway, for example, has considered amendments to its existing laws

---

104. Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Russia with Sweeping New Sanctions Authority (Apr. 15, 2021), https://home.treasury.gov/news/press-releases/jy0127 [https://perma.cc/H764-MHS9] (archived July 24, 2021).

105. *Id.*

106. *See* Panel Report, *United States – Tariff Measures on Certain Goods from China*, ¶¶ 1.1, 7.113, WTO Doc. WT/DS543/R and Add.1 (adopted on Sept. 15, 2020, under appeal since Oct. 27, 2020) (explaining that China questioned the legality of such additional tariffs before the WTO).

107. *See* Council of the European Union Press Release, Cyber Attacks: EU Ready to Respond With a Range of Measures, Including Sanctions (June 19, 2017), http://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/ [https://perma.cc/8WN8-YGMG] (archived July 24, 2021).

108. *See* Council Regulation 2019/796 of 17 May 2019, Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States, 2019 O.J. (L 129I) 1, 2 (EU); *see also* Council Decision 2019/797 of 17 May 2019 Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States, 2019 O.J. (L 129I) 13, 14 (CFSP) (setting forth the cyber sanctions framework and defining which cyber-attacks it applies to).

109. *See* Council Decision 2020/651 of 14 May 2020, Amending Decision 2019/797 Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States, 2020 O.J. (L 153) 4 (CFSP).

110. *See* Council of the European Union Press Release, Declaration by the High Representative on Behalf of the EU on the Alignment of Certain Third Countries Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States (July 2, 2019), http://www.consilium.europa.eu/en/press/press-releases/2019/07/02/declaration-by-the-high-representative-on-behalf-of-the-eu-on-the-alignment-of-certain-third-countries-concerning-restrictive-measures-against-cyber-attacks-threatening-the-union-or-its-member-states/ [https://perma.cc/5PKF-EXR8] (archived July 24, 2021).

that would allow it to impose EU unilateral sanctions, including cyber sanctions.[111]

Under the EU regime, cyberattacks are defined as the following actions:

> (a) access to information systems; (b) information system interference; (c) data interference; or (d) data interception, where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned.[112]

Similar to the United States, data interference also covers theft of data, funds, economic resources, or intellectual property.[113]

To be sanctioned, the abovementioned actions need to have a significant effect on and constitute an external threat to the union or its member states.[114] The following factors should be taken into account for the determination of whether a cyberattack has a significant effect:

> (a) the scope, scale, impact, or severity of disruption caused, including to economic and societal activities, essential services, critical state functions, public order, or public safety; (b) the number of natural or legal persons, entities, or bodies affected; (c) the number of Member States concerned; (d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources, or intellectual property; (e) the economic benefit gained by the perpetrator, for himself or for others; (f) the amount or nature of data stolen or the scale of data breaches; or (g) the nature of commercially sensitive data accessed.[115]

Regarding the second precondition, a cyberattack constitutes an external threat to the union or its member states if it is conducted from abroad[116] and if such a cyberattack affects information systems related to critical infrastructure,[117] services necessary for the maintenance of

---

111. *See* Ministry of Foreign Affairs Press Release, Government Proposes New Sanctions Act (Dec. 18, 2020), https://www.regjeringen.no/en/aktuelt/new-sanctions-act/id2815141/ [https://perma.cc/U6VL-LHKW] (archived July 24, 2021).

112. Council Regulation 2019/796 art. 1(3).

113. *Id.* at art. 1(7)(c).

114. *See id.* at art. 1(1).

115. *Id.* at art. 2.

116. *See id.* at art. 1(2) ("Cyber-attacks constituting an external threat include those which: (a) originate, or are carried out, from outside the Union; (b) use infrastructure outside the Union; (c) are carried out by any natural or legal person, entity or body established or operating outside the Union; or (d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union").

117. *Id.* at art. 1(4)(a) ("[C]ritical infrastructure, including submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security, and economic or social well-being of people").

essential social and/or economic activities,[118] critical state functions,[119] the storage or processing of classified information,[120] and the government emergency response teams.[121] The cyberattacks that cause a threat to the union are those that are "carried out against its institutions, bodies, offices and agencies, its delegations to third countries or to international organisations, its common security and defence policy (CSDP) operations and missions and its special representatives."[122] The EU cyber sanctions can also be imposed if cyber activities target the third states or international organizations and such attacks have a significant effect.[123] Hence, contrary to the United States, the EU cyber sanctions framework appears to be more precise in formulating criteria for cyber sanctions application.

Restrictive measures under the EU sanctions regime include freezing of funds,[124] freezing of economic resources,[125] prohibition against providing funds and/or economic resources to sanctioned targets,[126] prohibition from participating in the activities aimed at circumventing the imposed restrictive measures,[127] as well as travel bans.[128] The EU regime stipulates that sanctions may be imposed against natural or legal persons, entities, or bodies.[129] The recently imposed EU cyber sanctions target individuals, legal entities, and the Russian government agencies.[130]

---

118. *Id.* at art. 1(4)(b) ("[S]ervices necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil and gas); transport (air, rail, water and road); banking; financial market infrastructures; health (healthcare providers, hospitals and private clinics); drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned").

119. *Id.* at art. 1(4)(c) ("[C]ritical State functions, in particular in the areas of defence, governance and the functioning of institutions, including for public elections or the voting process, the functioning of economic and civil infrastructure, internal security, and external relations, including through diplomatic missions").

120. *Id.* at art. 1(4)(d).

121. *Id.* at art. 1(4)(e).

122. *Id.* at art. 1(5).

123. *See id.* at art. 1(6).

124. *See id.* at art. 3(1).

125. *See id.* at art. 3(1).

126. *See id.* at art. 3(2).

127. *Id.* at art. 9.

128. *See* Council Decision 2019/797 at art. 4.

129. Council Regulation 2019/796 at art. 3(3).

130. *See* Council Decision 2020/1127 of 30 July 2020, Amending Decision 2019/797 Concerning Restrictive Measures Against Cyber-attacks threatening the Union or its Member States, 2020 O.J. (L 246) 12 (CFSP); *see also* Council Implementing Regulation 2020/1125 of 30 July 2020, Implementing Regulation 2019/796 Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States, 2020 O.J. (L 246) 4 (EU) (defining which bodies the EU cyber sanctions target).

In July 2020, the EU announced its first designations under the cyber sanctions regime.[131] These designations target individuals as well as legal entities that are found responsible for the cyberattacks commonly referred to as "WannaCry,"[132] "NotPetya,"[133] and "Operation Cloud Hopper,"[134] as well as the attempted cyberattack to undermine the integrity of the Organisation for the Prohibition of Chemical Weapons (OPCW).[135] The imposed restrictive measures pursue the objectives "to prevent, discourage, deter and respond to continuing and increasing malicious behavior in cyberspace."[136] A new wave of the EU cyber sanctions enacted in October 2020 targets those responsible for a cyberattack against the German federal parliament (Deutscher Bundestag) in April and May 2015.[137]

The EU cyber sanctions regime has attracted scholarly attention. Yuliya Miadzvetskaya conducted an analysis of the new EU regime in order to identify deficiencies that might undermine its effectiveness.[138] According to her analysis, such deficiencies are the challenge of attributing a cyberattack; the lack of a common approach toward cyberattacks between the EU member states; the possible inconsistency of cyber sanctions with the fundamental human rights; and finally, the absence of evidence upon which the attribution of

---

131. *See* Council Decision 2020/1127, *supra* note 130, at 12; *see also* Council Implementing Regulation 2020/1125 at 4 (providing the designations under the cyber sanctions).

132. Council Decision 2020/1127, *supra* note 130, at 17 ("'WannaCry' disrupted information systems around the world by targeting information systems with ransomware and blocking access to data. It affected information systems of companies in the Union, including information systems relating to services necessary for the maintenance of essential services and economic activities within Member States.").

133. *Id.* at 18 ("'NotPetya' or 'EternalPetya' rendered data inaccessible in a number of companies in the Union, wider Europe and worldwide, by targeting computers with ransomware and blocking access to data, resulting amongst others in significant economic loss.").

134. *Id.* at 14 ("'Operation Cloud Hopper' targeted information systems of multinational companies in six continents, including companies located in the Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss.").

135. *Id.* ("The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work.").

136. *Id.*

137. Council Decision 2020/1537 of 22 October 2020, Amending Decision 2019/797 Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States, 2020 O.J. (L 351) 5 (CFSP); Council Implementing Regulation 2020/1536 of 22 October 2020, Implementing Regulation 2019/796 Concerning Restrictive Measures Against Cyber-attacks Threatening the Union or its Member States, 2020 O.J. (L 351) 1 (EU).

138. *See* Yuliya Miadzvetskaya, *Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy (CFSP)*, *in* SECURITY AND LAW: LEGAL AND ETHICAL ASPECTS OF PUBLIC SECURITY, CYBER SECURITY AND CRITICAL INFRASTRUCTURE SECURITY 277, 280 (Anton Vedder et al. eds., 2019).

cyberattacks were conducted and as a result, the possibility to annul imposed sanctions.[139] Another study identified ten questions that define the effectiveness of imposed sanctions and evaluated the new EU cyber sanctions regime against the background of these ten principles.[140] This analysis revealed possible deficiencies and paved the way for suggestions regarding how to improve the new regime.[141]

3. The United Kingdom

Despite Brexit, the United Kingdom closely follows the developments regarding the EU unilateral sanctions (restrictive measures). Shortly after the EU cyber sanctions regime was adopted, UK legislation aimed at aligning with the EU sanctions was introduced.[142] Later, the United Kingdom enacted the Cyber Sanctions Regulations, which came into force on an exit day.[143] Pursuant to this regulation, the United Kingdom imposed cyber sanctions targeting the same actors as the EU.[144]

III. UNILATERAL CYBER SANCTIONS AND INTERNATIONAL LAW

Unilateral sanctions are introduced in accordance with the domestic legislation of the states implementing them and they are not authorized by any regional or international organizations. Their legality against the background of norms and principles of international law is debatable, and they might violate various norms of international law.

This Part is devoted to the analysis of international law obligations that unilateral cyber sanctions may breach. Furthermore, this analysis will be followed by a discussion of the possible legal defenses, such as retorsions and countermeasures. The compatibility of cyber sanctions with WTO law and international investment law will be examined in the next Part.

---

139. *See id.* at 290.

140. KARINE BANNELIER, NIKOLAY BOZHKOV, FRANÇOIS DELERUE, FRANCESCO GIUMELLI, ERICA MORET, MAARTEN VAN HORENBEECK, INST. FOR SEC. STUD., GUARDIAN OF THE GALAXY: EU CYBER SANCTIONS AND NORMS IN CYBERSPACE 15–18 (Patryk Pawlak & Thomas Biersteker eds., 2019), https://www.iss.europa.eu/content/guardian-galaxy-eu-cyber-sanctions-and-norms-cyberspace (last visited July 24, 2021) [https://perma.cc/CE7D-AKL3] (archived July 24, 2021).

141. *See id.*

142. *See* The Cyber-Attacks (Asset-Freezing) Regulations 2019, SI 2019/956.

143. *See* The Cyber (Sanctions) (EU Exit) Regulations 2020, SI 2020/597.

144. Foreign, Commonwealth & Development Office, *Guidance: the UK sanctions list*, (Feb. 1, 2021), https://www.gov.uk/government/publications/the-uk-sanctions-list [https://perma.cc/5R34-ZT5P] (archived July 30, 2021).

A. *Potential Breaches of International Law*

1. Customary International Law of State Immunity

Customary international law of state immunity embodies immunity from jurisdiction (immunity from adjudication) and immunity from enforcement.[145] Immunity from jurisdiction protects a state from the jurisdiction of the courts of another state in administrative, civil, and criminal proceedings.[146] Immunity from enforcement shields state property against enforcement measures of a foreign state.[147] It should be noted that state property benefits from an extended protection under the immunity from enforcement.[148] Such protection covers "any measures of constraint, including attachment, arrest, and execution."[149]

Immunity guarantees are accorded not only to states but also to high-ranking government officials. The ambit of such immunity entitlements is related to the functional need.[150] In this regard, the International Court of Justice (ICJ) has eloquently concluded:

> The Court would observe at the outset that in international law it is firmly established that, as also diplomatic and consular agents, certain holders of high-ranking office in a State, such as the Head of State, Head of Government and Minister for Foreign Affairs, enjoy immunities from jurisdiction in other States, both civil and criminal.[151]

---

145. HAZEL FOX & PHILIPPA WEBB, THE LAW OF STATE IMMUNITY 23 (3rd ed. 2015) ("The UNCSI [UN Convention on Jurisdictional Immunities of States and their Property], national legislation and State practice observes this distinction between immunity from adjudication and immunity from enforcement.").

146. Peter-Tobias Stoll, *State Immunity*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW [MPEPIL] (Apr. 2011) ¶ 1, https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1106.

147. *Id.*

148. *See id.*; *see also* Jurisdictional Immunities of the State (Ger. v. It.: Greece intervening), Judgment, 2012 I.C.J. Rep. 99, ¶ 113 (February 3) (pointing out the following: "the Court observes that the immunity from enforcement enjoyed by States in regard to their property situated on foreign territory goes further than the jurisdictional immunity enjoyed by those same States before foreign courts").

149. Stoll, *supra* note 146, ¶ 52.

150. Sir Arthur Watts, *Heads of Governments and Other Senior Officials*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW [MPEPIL] ¶ 19 (Oct. 2010) ("[I]t is now clear that the underlying basis for their [senior state officials] special treatment is their functional need for it.").

151. Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.), Judgment, 2002 I.C.J. Rep. 3, ¶ 51 (Feb. 14).

The existing cyber sanctions target government bodies[152] as well as senior government officials.[153] Unilateral cyber sanctions, such as the freezing of assets, are perceived as temporary administrative prohibitions that do not entail any criminal charges brought against sanctioned individuals or entities.[154] But the question demanding further elaboration is whether customary international law of state immunity could be impeded by a state that freezes assets of a government body of another state. Or could it be violated by the prohibition restricting senior government officials of another state to enter its territory?

It is debatable if the freezing of government bodies' assets violates customary international law of state immunity. Freezing of assets can be defined as "measures of constraint" in the context of immunity from enforcement.[155] However, such restrictions are implemented through decisions issued by administrative bodies outside of court proceedings, and hence, it remains unclear whether enforcement immunity guarantees could be invoked. More specifically, the immunity from jurisdiction is invoked in the course of court proceedings, yet there is

---

152. Among cyber sanctions imposed by the US, there are those directed against the government bodies of the Russian Federation. In particular, the list of sanctioned entities attached to the Executive Order 13757 includes the following government agencies: Main Intelligence Directorate (Glavnoe Razvedyvatel'noe Upravlenie) (GRU); Federal Security Service (Federalnaya Sluzhba Bezopasnosti) (FSB). Exec. Order. No. 13,757, *supra* note 70, at 3. In February 2017, the Office of Foreign Assets Control (OFAC) published a general license, which authorized certain transactions with the Russian Federal Security Service (FSB). This general license allows the US exporters to pay the fees to the FSB, which are necessary for the renewal of licenses and as a result, to be able to export their goods and technologies to the Russian Federation, which is not prohibited under the cyber sanctions in place. *See* OFF. OF FOREIGN ASSETS CONTROL, GENERAL LICENSE NO. 1 (2017). In a similar vein, the EU sanctioned the Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU). Council Decision 2020/1127, *supra* note 130; Council Implementing Regulation 2020/1125, *supra* note 130.

153. Besides targeting government agencies that were allegedly involved in cyberattacks, the US also implemented sanctions against the holders of high-ranking government positions. *See* Exec. Order. No. 13,757, *supra* note 70 at 3. The EU targeted a number of Russian military intelligence officers. *See* Council Decision 2020/1127, *supra* note 130; Council Implementing Regulation 2020/1125, *supra* note 130.

154. Taking into account the practice of the UN as well as the EU in imposing financial restrictions in a form of asset freezing, some scholars undertook an effort to analyze whether such restrictions can be qualified as a criminal charge for the purposes of applying additional human rights guarantees to sanctioned individuals. As their analysis demonstrates, financial restrictions in a form of asset freezing cannot qualify as a criminal charge. *See* Melissa van den Broek, Monique Hazelhorst, & Wouter de Zanger, *Asset Freezing: Smart Sanction or Criminal Charge?*, 27 UTRECHT J. INT'L EUR. L. 18, 24 (2011).

155. "The expression 'measures of constraint' has been chosen as a generic term, not a technical one in use in any particular internal law. Since measures of constraint vary considerably in the practice of States, it would be difficult, if not impossible, to find a term which covers each and every possible method or measure of constraint in all legal systems." FOX & WEBB, *supra* note 145, at 499–500.

no agreement if the same applies to immunity from enforcement.[156] In other words, if state property benefits from the enforcement immunity irrespective of an existence of court proceeding, then cyber sanctions implemented by administrative decisions encroach on state immunity.

Travel bans preventing senior government officials from fulfilling their functions encroach on the immunities guaranteed to such officials under international law. This conclusion can be reached based on the analysis of the relevant ICJ jurisprudence. The court pronounced that the arrest warrant issued for a Minister for Foreign Affairs prevented this high-ranking government official from traveling and thus fulfilling functions on behalf of a state and, as a result, impeded immunities accorded under international law.[157] One more clarification is warranted in this regard: not all government officials are entitled to such immunities. The ICJ jurisprudence demonstrates that the immunity entitlements are guaranteed to the officials who represent the government and hence travel to other states for that purpose.[158]

The EU regime of cyber sanctions takes the abovementioned consideration into account. In particular, travel restrictions could be lifted under certain circumstances.[159] The US cyber sanctions

---

156. Natalino Ronzitti argues that the enforcement immunity guarantees protection to state property not only from "acts of constraints that are the continuation of a judgment, but also measures autonomously dictated by the legislative or the executive branch" and thus unilateral economic sanctions might impede such guarantees. Natalino Ronzitti, *Sanctions as Instruments of Coercive Diplomacy: An International Law Perspective*, *in* COERCIVE DIPLOMACY, SANCTIONS AND INTERNATIONAL LAW 1, 21–22 (Natalino Ronzitti ed., 2016). To the contrary, Tom Ruys expressed the view that the enforcement immunity can be invoked only in the course of court proceedings and if unilateral sanctions are imposed by an administrative agency, such restrictions are consistent with the customary international law of immunities. Tom Ruys, *Immunity, Inviolability and Countermeasures – A Closer Look at Non-UN Targeted Sanctions*, *in* THE CAMBRIDGE HANDBOOK OF IMMUNITIES AND INTERNATIONAL LAW 670 (Tom Ruys & Nicolas Angelet eds., 2019).

157. "The Court accordingly concludes that the functions of a Minister for Foreign Affairs are such that, throughout the duration of his or her office, he or she when abroad enjoys full immunity from criminal jurisdiction and inviolability. That immunity and that inviolability protect the individual concerned against any act of authority of another State which would hinder him or her in the performance of his or her duties." Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.), Judgment, 2002 I.C.J. Rep. 3, ¶ 54 (Feb. 14).

158. The ICJ denied personal immunities to Procureur de la Republique and Head of National Security. Certain Questions of Mutual Assistance in Criminal Matters (Djib. v. Fr.), Judgment, 2008 I.C.J. Rep. 177, ¶¶ 196–97 (June 4). However, in the court's view, the Minister of Foreign Affairs represents a state and thus the immunities guaranteed to this position should include the right to travel and represent a state. *See* Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.), Judgment, 2002 I.C.J. Rep. 3, ¶ 55 (Feb. 14).

159. The following exceptions are prescribed: "[A] Member State is bound by an obligation of international law, namely: (a) as a host country of an international intergovernmental organisation; (b) as a host country to an international conference convened by, or under the auspices of, the United Nations; (c) under a multilateral

framework does not prescribe such exceptions explicitly. Notwithstanding this, an exception to travel bans can be granted if "entry of the person into the United States would not be contrary to the interests of the United States, as determined by the Secretary of State."[160]

Hence, both the EU and the US cyber sanctions frameworks prescribe exceptions to travel bans aimed at reducing their potential inconsitencies with the immunity entitlements guaranteed under international law. Nevertheless, inept administration of these exceptions could still give rise to claims of their inconsistency with the immunity guarantees.

2. Human Rights Law

A decade ago, the impact of human rights law on the right of states to freeze assets of individuals and impose travel restrictions became the subject matter of a heated debate.[161] The debate revolved around procedural rights and guarantees of the individuals whose assets were frozen and for whom travel was restricted due to their alleged involvement in terrorism financing.[162] These constraints were put in place without prior notification or court decision, and sanctioned individuals were deprived of their right to have access to an effective remedy.[163]

What is noteworthy in the context of cyber sanctions is that their consistency with the minimum due process rights may be questioned. For example, the EU sanctions (restrictive measures) are often questioned before the EU courts, that is, the EU General Court (at first instance) and the EU Court of Justice (on appeal).[164] Persons targeted under the EU cyber sanctions regime benefit from the guarantees enshrined in the Charter of Fundamental Rights of the European Union, in particular the right to good administration and the right to

---

agreement conferring privileges and immunities; or (d) pursuant to the 1929 Treaty of Conciliation (Lateran Pact) concluded by the Holy See (Vatican City State) and Italy." Council Regulation 2019/796, *supra* note 108, at art. 4(3).

160. Proclamation No. 8693, 76 Fed. Reg. 44,751, 44,751 (July 24, 2001).

161. *See, e.g.*, Marko Milanovic, *Norm Conflict in International Law: Whither Human Rights?*, 20 DUKE J. COMPAR. & INT'L L. 69 (2009); BARDO FASSBENDER, UNITED NATIONS Off. Of Legal Affs., TARGETED SANCTIONS AND DUE PROCESS 4–8 (2006).

162. *See, e.g.*, Devika Hovell, *Due Process in the United Nations*, 110 AM. J. INT'L L. 1, 3 (2016).

163. *See* FASSBENDER, *supra* note 161, at 4–5.

164. "In the period from 2010 to 2014, cases concerning sanctions became the third most recurrent issue area among the cases heard by EU Courts, placing it only after intellectual property rights and competition quarrels. By 2017, cases regarding restrictive measures had displaced competition cases, becoming the second most frequent issue heard by the Court." PORTELA, *supra* note 60, at 12.

an effective remedy and to a fair trial,[165] which are frequently invoked in disputes questioning the EU economic sanctions.[166] In the course of the last years, the EU courts developed case-law that is illustrative of the courts' attitude towards the appropriate balance between human rights considerations and other policy objectives pursued by economic sanctions.[167]

The US designations can be questioned either before the Office of Foreign Assets Control (OFAC) or before domestic courts. However, applications challenging US unilateral sanctions, even on human rights grounds, often fail. For example, in one of the recent cases, a company brought a claim against US unilateral sanctions based on alleged violations of the Fifth Amendment.[168] More specifically, the complainant argued that its procedural and substantive due process rights were violated because there was no prior notice or an opportunity to be heard before the designation.[169] Furthermore, it was contended that the Takings Clause of the Fifth Amendment, which states that "private property [shall not] be taken for public use, without just compensation," was violated by the imposed sanctions.[170] After quoting the U.S. Supreme Court, which pronounced that "non-resident aliens without substantial connections to the US are not entitled to Fifth Amendment protections," the district judge dismissed all the constitutional claims.[171] Overall, the US procedures to question unilateral sanctions' legality grant fewer rights to the sanctioned individuals/entities in comparison with the EU guarantees.[172]

Besides the requirement of due process rights, another possible ground to question the legality of sanctions is the right to property that is guaranteed under various international human rights treaties as well as domestic laws.[173] However, the right to property is not an

---

165. *See* Charter of Fundamental Rights of the European Union, arts. 41, 47, 2012 O.J. (C 326).

166. *See* Matthew Happold, *Targeted Sanctions and Human Rights*, *in* ECON. SANCTIONS & INT'L L. 87, 99 (Matthew Happold & Paul Eden eds., 2016).

167. "Thanks to frequent litigation, EU Courts have established in their case-law the requirements that need to be satisfied for individual listings, regarding the specification of designation criteria, statements of reasons and supporting evidence, all of which had been absent in the early days of blacklisting." PORTELA, *supra* note 60, at 12; *see also* Arnoud Willems & Alessandra Moroni, *Defeating Economic Sanctions in the EU: A Strategic Analysis of Litigation Options*, 1 INT'L TRADE L. & REGUL. 39, 40 (2020).

168. *See* Fulmen Co. v. Off. of Foreign Assets Control, No. 18-2949, 2020 WL 1536341, at *4 (D. D.C. Mar. 31, 2020).

169. *Id.*

170. U.S. CONST. amend. V (alteration in original); *see id.*

171. *See Fulmen Co.*, 2020 WL 1536341, at *5.

172. Rachel Barnes, *United States Sanctions: Delisting Applications, Judicial Review and Secret Evidence*, *in* ECONOMIC SANCTIONS AND INTERNATIONAL LAW 197, 223–24 (Matthew Happold & Paul Eden eds., 2016).

173. *See, e.g.*, Jacob Mchangama, *The Right to Property in Global Human Rights Law*, CATO INST. (2011), https://www.cato.org/policy-report/may/june-2011/right-

absolute right and may be restricted under certain circumstances.[174] This view is endorsed not only by scholars[175] but also by court practice. As a matter of fact, the EU courts are frequently confronted with the need to adjudicate the legality of the EU unilateral sanctions against the background of human rights standards, including the right to property.[176] The EU courts are more willing to acknowledge the violation of due process rights than the right to property.[177]

Restrictions to enter the territory of a state (i.e., travel bans) may interfere with the right for family and private life[178] and constitute an attack on the targeted individuals' honor and reputation.[179] Yet the practice of international courts and quasi-judicial bodies confirms that travel bans violate the enumerated rights only in exceptional circumstances, and the threshold for any such finding is set high.[180]

3. Bilateral International Agreements

Cyber sanctions may potentially violate bilateral agreements of economic nature. To illustrate this possibility, the Treaty of Amity, Economic Relations, and Consular Rights signed between Iran and the United States of America (Treaty of Amity) in 1955 can be taken as an example.[181] This choice is not a coincidence: Iran, in its attempt to question the legality of the US unilateral sanctions, relied upon the provisions of this agreement in two ongoing disputes before the ICJ.[182]

---

property-global-human-rights-law (last visited July 30, 2021) [https://perma.cc/HC7U-PYUV] (archived July 30, 2021).

174. "[T]he right to property is a relative right, not an absolute one. By definition, the scope of the right may be affected by cultural, social, and economic factors which may evolve over time." John G. Sprankling, *The Global Right to Property*, 52 COLUM. J. TRANSNAT'L L. 464, 498–99 (2014).

175. *See, e.g.*, Happold, *supra* note 166, at 94–95.

176. Arnoud Willems and Alessandra Moroni name these four pleas as the most frequently argued by the individuals/entities targeted by the EU unilateral sanctions: "1. The EU institutions fail to state reasons and breach their right of defence by failing to support factual and legal allegations with adequate evidence; 2. The EU institutions make manifest errors of assessment in determining whether listing criteria are satisfied; 3. The EU institutions disproportionately restrict fundamental rights, including rights to property and reputation and the freedom to conduct a business; and 4. The EU institutions breach their right to an effective remedy." Willems & Moroni, *supra* note 167, at 44.

177. *See id.* at 45.

178. Nada v. Switzerland, 2012-II Eur. Ct. H.R. at 44.

179. Sayadi and Vinck v. Belgium, Comm. 1472/2006, U.N. Doc. CCPR/C/94/D/1472/2006, ¶ 10.12 (Dec. 29, 2008).

180. *See* Happold, *supra* note 166, at 96–99.

181. *See* Treaty of Amity, Economic Relations, and Consular Rights, U.S.-Iran, Aug. 15, 1955, 8 UST 899, 903 [hereinafter Treaty of Amity].

182. *See* Certain Iranian Assets (Iran v. U.S.), Judgment, 2016 I.C.J. 2 (June 14); Alleged Violations of the 1955 Treaty of Amity, Economic Relations, and Consular Rights (Iran v. U. S.), 2018 I.C.J. 2 (July 16).

The unilateral economic sanctions disputed in those cases include freezing of assets and prohibitions on various business transactions, among other restrictions.

Asset freezes and other prohibitions on transactions in property and interests in property could violate certain provisions of the Treaty of Amity as well as other bilateral treaties that incorporate similar language. Take for instance Article IV (2) of the Treaty of Amity, which reads as follows:

> Property of nationals and companies of either High Contracting Party, including interests in property, shall receive the most constant protection and security within the territories of the other High Contracting Party, in no case less than that required by international law. Such property shall not be taken except for a public purpose, nor shall it be taken without the prompt payment of just compensation. Such compensation shall be in an effectively realizable form and shall represent the full equivalent of the property taken; and adequate provision shall have been made at or prior to the time of taking for the determination and payment thereof.[183]

Additionally, under this treaty nationals and companies of each contracting party shall be permitted "to dispose of property of all kinds by sale, testament or otherwise" within the territory of another contracting party.[184]

As this Article pointed out above, freezing of assets, restrictions on transactions in property, and interests in property are temporary measures, which do not entail that such property is taken from an owner. Yet, such restrictions imply that an owner is deprived of the right to exercise control over the property. Furthermore, the duration of those restrictive measures remains undefined. In fact, restrictive measures are regularly extended by the states invoking them. For these reasons, it can be argued that the factual inability to exercise any control over the property, reinforced by a possible extended duration of such prohibitions, is tantamount to a *de facto* expropriation.[185]

The Treaty of Amity and other bilateral treaties of economic nature, as a rule, prescribe a number of exceptions to their substantive obligations.[186] The national security exception is often among the possible exemptions, and this exception would most probably be invoked by a state justifying its cyber sanctions.[187] Notably, the ICJ jurisprudence demonstrates that the court attributes significant weight to the exact wording of the national security exception to define

---

183. Treaty of Amity, *supra* note 181, at 903, art. IV (2).

184. *Id.* at 904, art. V.

185. For a more detailed discussion of this argument, *see infra* Part IV.2.

186. *See* Treaty of Amity, *supra* note 181, at 912, art. XX.

187. Article XX of the Treaty of Amity, in the relevant part, reads as follows: "The present Treaty shall not preclude the application of measures: (d) […] necessary to protect its essential security interests." *Id.*

the scope of the self-judging nature of those exceptions.[188] In light of the previous jurisprudence, the court may review the necessity and proportionality of cyber sanctions before deciding if they could be justified on national security grounds.[189]

B. *Legal Defenses*

1. Acts of Retorsion or Countermeasures?

From an international law perspective, unilateral cyber sanctions might either fall into the category of retorsion or, alternatively, be tantamount to countermeasures. Retorsions can be defined as "unfriendly act[s] at most, ie acts which are wrongful not in the legal but only in the political or moral sense, or a simple discourtesy."[190] Given that acts of retorsion are legal *per se*, their invocation is not conditional on the existence of a prior violation of international law. Some forms of cyber sanctions can be retorsions. Thus, they do not violate international obligations of a state imposing them.

To the contrary, the right to rely upon countermeasures is only permitted if there was a preceding violation of international law that can be attributed to a particular state, which is ultimately targeted by countermeasures.[191] Put differently, countermeasures are "unilateral measures adopted by a State (the 'injured State') in response to the breach of its rights by the wrongful act of another State (the 'wrongdoing' or 'target' State) that affect the rights of the target State and are aimed at inducing it to provide cessation or reparations to the injured State."[192]

The determination of whether unilateral cyber sanctions are acts of retorsion or countermeasures serves more than a rhetorical purpose. Our previous analysis has defined the circumstances under which unilateral cyber sanctions may be inconsistent with international law and as a result require justification as countermeasures. Countermeasures are illegal acts under international law that entail international responsibility, and yet they may be justified provided a number of preconditions are met. The next Part is devoted to the analysis of whether cyber sanctions can fulfil all the preconditions to be countermeasures.

---

188. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 186 (June 27); Djib. v. Fr., *supra* note 158, ¶ 154.

189. *See* Nicar. v. U.S., *supra* note 188, ¶ 194.

190. Thomas Giegerich, *Retorsion*, *in* MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L L., ¶ 2 (Sept. 2020).

191. *See* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at art. 49 (2001) [hereinafter ARSIWA].

192. Federica I Paddeu, *Countermeasures*, *in* MAX PLANCK ENCYCLOPEDIA OF PUB. INT'L L., ¶ 1 (Sept. 2015).

2. Can Unilateral Cyber Sanctions Be Justified as Countermeasures?

Cyber sanctions targeting government agencies or high-ranking government officials may encroach on customary international law of state immunity. In certain instances, cyber sanctions can violate bilateral agreements and may not be justified on national security grounds. Against this backdrop, states could advance an argument that such restrictive measures are justified as countermeasures.

The existing rules on states' international responsibility entitle states to rely upon self-help measures, such as countermeasures.[193] A state is allowed to impose countermeasures if certain preconditions are met. First, countermeasures are remedies to redress a previous violation of international law.[194] Such previous violation should be attributed to a state.[195] The attribution of conduct to a particular state is an aspect that plays a significant role for cyber sanctions: the element of attribution in the context of cyberattacks is not only technically burdensome[196] but also often legally impractical.[197] Second, the right to impose countermeasures is guaranteed only to injured states in the meaning of the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA).[198]

---

193. Countermeasures are defined as: "Countermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State." ARSIWA, *supra* note 191, at art. 49(2).

194. "An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under Part Two." *Id.* at art. 49(1).

195. Chapter II of the ARSIWA contains a list of principles and rules based on which certain conduct can be attributed to a state. *See id.* at art. 49.

196. "While recent technological developments have meant that accurate cyber tracing is now possible, it is still extremely difficult." Russell Buchan, *Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm*, 21 J. CONFLICT & SEC. L. 429, 430–31 (2016).

197. "One of the existing challenges in the implementation of a sanctions regime…is the difficulty in clearly establishing links between states and the perpetrators of cyber operations." GUARDIAN OF THE GALAXY: EU CYBER SANCTIONS AND NORMS IN CYBERSPACE, *supra* note 140, at 5; *see* Kubo Mačák, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, 21 J. CONFLICT & SEC. L. 405 (2016), for an example on the legal difficulties that relate to the possibility to attribute conduct of non-state actors to a particular state for the purposes of invoking state responsibility.

198. Article 42 prescribes the definition of an injured state and Article 49 defines that only injured states can impose countermeasures. Articles 48 and 54, which deal with the right of non-injured states to invoke the responsibility of a state, do not entitle such states to rely upon countermeasures. *See* ARSIWA, *supra* note 191, at arts. 42, 48, 49, 54.

Furthermore, countermeasures should meet other requirements, including: proportionality,[199] temporary nature,[200] and procedural prerequisites that must precede their imposition.[201] Countermeasures can be imposed only against a state; thus, non-state actors cannot be targeted by countermeasures.

The possibility to justify cyber sanctions as countermeasures is hindered by a number of substantive and procedural hurdles. Our subsequent analysis will focus on two of them: the lack of internationally agreed obligations regulating behavior in cyberspace and the attribution of cyberattacks to a state under the rules of state responsibility.

To begin with, the main precondition for imposing countermeasures is a prior violation of an obligation under international law—an internationally wrongful act. Such an internationally wrongful act can consist of an action or omission.[202] In this regard, the question that needs to be tackled is whether international law as it stands today constrains states' behavior in cyberspace. As mentioned in the first section of this Article, the answer is no. International obligations of states on how to behave in cyberspace are not established yet. In particular, an international treaty, which would stipulate obligations regarding states' behavior in cyberspace, has not been agreed to yet. Even cybersecurity cooperation provisions included in the recently negotiated trade agreements only include language such as "[t]he Parties recognise,"[203] or "the Parties shall endeavor,"[204] all of which denote a non-enforceable legal obligation. In addition, while the Tallinn Manual and the Tallinn Manual 2.0 (Rule 4) include relevant provisions stating that states must not conduct cyber operations that violate the sovereignty of another space, these rules constitute at most soft law but not binding obligations.

Scholarly debates revolve around the idea that non-interference in cyberspace is embedded in the concept of sovereignty.[205] Or,

---

199. "Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question." *Id.* at art. 51.

200. "Countermeasures shall be terminated as soon as the responsible State has complied with its obligations under Part Two in relation to the internationally wrongful act." *Id.* at art. 53.

201. The following procedural prerequisites are enlisted: call on the responsible state to fulfil its obligations, an obligation to notify the responsible state of any decision to take countermeasures as well as an obligation to offer to negotiate with that state. *Id.* at art. 52.

202. *Id.* at art. 2.

203. CPTPP, *supra* note 34, at art. 14.16.

204. USMCA, *supra* note 38, at art. 19.15.

205. In this regard, the Tallinn Manual expounds:

alternatively, that cyber interference encroaches on the principle of non-intervention,[206] and the argument that cyber warfare is prohibited under Article 2(4) of the UN Charter that outlaws the use of force.[207] However, these debates do not go beyond theoretical discussions, and it is unlikely that states would endorse any of them to become a binding rule.

The argument that a violation of an obligation set out in the Tallinn Manual or the Tallinn Manual 2.0 constitutes an internationally wrongful act does not go far. It is true that an internationally wrongful act can also consist of an omission to fulfill an obligation under international law.[208] It is also true that the Tallinn Manual puts forward an international obligation to prohibit use of the state's cyber infrastructure to the detriment of other states.[209] It was even contended that this obligation should be binding irrespectively of whether such acts can be attributed to a state[210] under the condition that a state knew about cyberattacks.[211] According to the Tallinn Manual, a violation of this obligation entails international responsibility, including the right to impose countermeasures.[212] However, the Tallinn Manual is a non-binding document, and thus it cannot be a source of a binding international obligation that can be redressed by countermeasures when violated.

> A cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage. The International Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty.

MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 16 (2013). Furthermore, it is noted that "there is an embryonic view proffered by some scholars that cyber operations conducted by non-State actors may also violate a State's sovereignty (in particular the aspect of territorial integrity)." *Id.* at 18. Michael Schmitt echoes the abovementioned views: "[H]ostile cyber operations against cyber infrastructure on another State's territory amount to, *inter alia*, a violation of that State's sovereignty if they cause physical damage or injury." Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 704 (2014). Schmitt admits that some scholars suggest a lower threshold: "Some international law experts take the position that sovereignty can at times be violated even when no damage results, as in the case of emplacement of malware designed to monitor a system's activities." *Id.* at 705.

206. "If such cyber operations are intended to coerce the government (and are not otherwise permitted under international law), the operation may constitute a prohibited 'intervention.'" SCHMITT, *supra* note 205, at 17 (internal citations omitted).

207. *Id.* at Rules 10–12.

208. *See* ARSIWA, *supra* note 191, at art. 2.

209. Rule 5 reads as follows: "A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States." SCHMITT, *supra* note 205, at 26.

210. *See id.* at 26.

211. *See id.* at 28.

212. *See id.* at 29.

Scholars also argue in favor of due diligence obligations in cyberspace. For example, Russell Buchan explored the possibility to transpose the customary international law obligation to prevent transboundary harm into cyberspace, including due diligence obligations.[213] Despite being thought-provoking, this argument is far-fetched, in particular against the background of the absence of a general due diligence obligation in international law.[214]

In light of the above, it would be difficult to establish what norm of international law was violated by a state that conducted a cyberattack. Furthermore, an obligation of due diligence in cyberspace is not well established yet. Against this background, it should be noted that international responsibility of states is not implicated for acts that are unregulated in international law.[215] Thus, the first precondition for imposing countermeasures is hard to meet.

The second difficulty that arises is an attribution of conduct. Attribution is fairly straightforward when a government body is involved in an internationally wrongful act.[216] Despite the seeming simplicity of this rule, the attribution of conduct in cyberspace appears to be burdened by technical complexity,[217] as well as by the possibility of concealing the identity of an initiator of an attack by carrying it out through a non-government cyber infrastructure.[218]

The acts are also attributable to a state when a state empowered a person or an entity, which is not an organ of the state, to exercise elements of the governmental authority.[219] Moreover, actions of private actors can be attributed to a state if those private actors are "acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[220] The latter rule was clarified in

---

213. *See* Buchan, *supra* note 196, at 434–53.

214. Due diligence obligations exist in various legal regimes, yet a general obligation that would apply to all international obligations is not yet established. Eneken Tikk emphasizes: "Some states do not believe there is sufficient support in state practice to conclude that due diligence is a binding concept of international law. Others derive the binding nature of the concept from the rulings of the International Court of Justice (ICJ)." Tikk, *supra* note 55, at 188.

215. SCHMITT, *supra* note 205, at 30.

216. *See* ARSIWA, *supra* note 191, at art. 4.

217. See Marcus Schulzke, *The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty*, 16 PERSPECTS. ON POL. 954, 956 (2018) (noting that because of their difficulties and complexities, cyberattacks offer much less attributional certainty than kinetic attacks), as an example of a lengthier discussion.

218. "Over the years, through the use of deception narratives, nation states have intentionally contrived stratagems cloaking their nexus to attacks by appearing as non-nation state-sponsored organizations." Cameron H. Malin, Terry Gudaitis, Thomas Holt, & Max Kilger, *Asymmetric Warfare and Psyops: Nation State-Sponsored Cyber Attacks*, *in* DECEPTION IN THE DIGITAL AGE 207, 214 (Cameron H. Malin et al. eds., 2017).

219. ARSIWA, *supra* note 191, at art. 5.

220. *Id.* at art. 8.

the ICJ jurisprudence, which sets a high threshold to be met.[221] The possibility to attribute private actors' conduct in cyberspace to a state is particularly burdensome. Even if it is possible to trace the actors responsible for malicious cyber-enabled activities, it is very difficult to establish the legally required connection ("instruction," "direction," or "control") between them and a government.[222] In this regard, the Council of the EU distinguishes between the attribution of responsibility for cyberattacks and the imposition of unilateral cyber sanctions. It repays quoting the Council:

> Targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State.[223]

This analysis reveals that unilateral cyber sanctions would not meet the prerequisites necessary for being justified as countermeasures under the law of state responsibility.

IV. UNILATERAL CYBER SANCTIONS AND INTERNATIONAL ECONOMIC LAW

A. *Consistency with WTO Law*

Unilateral cyber sanctions may potentially violate various obligations under WTO law. In particular, broad prohibitions on economic relations with sanctioned entities prescribed by cyber sanctions entail restrictions on importation and exportation of goods and services.

For instance, the US cyber sanctions prohibit the following:

> (a) the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order; and (b) the receipt of any contribution or provision of funds, goods, or services from any such person.[224]

---

221. The ICJ pronounced the "effective control" as a standard applicable to an attribution of private actors' conduct to a state. Nicar. v. U.S., 1986 I.C.J. ¶115; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶ 399–407.

222. For more *see, e.g.*, Mačák, *supra* note 197, at 411.

223. Council Decision 2019/797, *supra* note 108, at 13–14.

224. Exec. Order No. 13,694, *supra* note 70, at Sec. 3.

This restriction is formulated in such a way as to effectively prohibit any transaction with sanctioned individuals and legal entities.

Similarly, the EU cyber sanctions framework prescribes the following prohibition: "No funds or economic resources shall be made available, directly or indirectly, to or for the benefit of natural or legal persons, entities or bodies listed in Annex I."[225] Annex I includes a list of sanctioned individuals, entities, and bodies. The ambit of this prohibition is further clarified in the EU Best Practices for the effective implementation of restrictive measures (unilateral sanctions), which reiterates: "Making funds available to a designated person or entity, be it by way of payment for goods and services, as a donation, in order to return funds previously held under a contractual arrangement, or otherwise, is generally prohibited."[226] Moreover, the prohibition on making economic resources available to sanctioned individuals, entities, and bodies is extremely broad, effectively banning any business transactions with them and affecting the importation and exportation of goods and services:

> The term 'making economic resources available' . . . has been interpreted by the Court of Justice as having a wide meaning. . . . The prohibition on making economic resources available applies to any mode of making available an economic resource, whatever the consideration. The fact that economic resources are made available against payment of a consideration which may be regarded as adequate is therefore irrelevant.[227]

The aforesaid restrictions might violate cornerstone principles of WTO law. In particular, prohibitions to import and export goods from/to sanctioned entities may infringe Article I:1 (Most-Favoured-Nation Treatment) of the General Agreement on Tariffs and Trade 1994 (GATT 1994).[228] Article I:1, in the relevant part, reads as follows:

> [W]ith respect to all rules and formalities in connection with importation and exportation . . . any advantage, favour, privilege or immunity granted by any contracting party to any product originating in or destined for any other country shall be accorded immediately and unconditionally to the like product originating in or destined for the territories of all other contracting parties.

To establish a violation of the MFN obligation under Article I:1 of the GATT 1994, WTO panels follow an analytical framework to determine:

---

225. Council Regulation 2019/796, *supra* note 108, at art. 3.

226. Council of the European Union, EU Best Practices for the Effective Implementation of Restrictive Measures 8519/18, at 19 (2018), https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf (last visited July 20, 2021 [https://perma.cc/HAN6-BFBQ] (archived July 20, 2021).

227. *Id.* at 21.

228. General Agreement on Tariffs and Trade 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, Apr. 15, 1994, 1867 U.N.T.S. 187 [hereinafter GATT 1994].

> (i) that the measure at issue falls within the scope of application of Article I:1; (ii) that the imported products at issue are 'like' products within the meaning of Article I:1; (iii) that the measure at issue confers an 'advantage, favour, privilege, or immunity' on a product originating in the territory of any country; and (iv) that the advantage so accorded is not extended 'immediately' and 'unconditionally' to 'like' products originating in the territory of all Members.[229]

Based on the above, a WTO member willing to question the compatibility of cyber sanctions with Article I:1 of the GATT 1994 can put forward the following argument. Unilateral cyber sanctions that restrict importation and exportation of goods fall within the scope of "rules and formalities in connection with importation and exportation," and thus within the scope of the application of Article I:1. Such restrictions target all products imported from or exported to designated entities. In view of this, "likeness" of the products can be presumed.[230] Regarding the existence of "advantage, favour, privilege, or immunity," import restrictions imposed against a subset of entities deprive these entities and, as a result, a WTO member, where such entities are incorporated, of having an "advantage" in the form of market access. Similarly, export restrictions deprive sanctioned entities of "advantage, favour, privilege, or immunity" to export necessary components, technology, equipment, etc. Hence, prohibitions on importation and exportation of goods from/to sanctioned entities grant an advantage to the entities incorporated in other WTO members, and this advantage is not extended "immediately" and "unconditionally" to the goods of sanctioned entities. An additional factor that may reinforce this line of argument is that the existing sanctions target individuals, entities owned by them, legal entities, and bodies located only in a few countries, thus making it possible to argue that sanctions regulations apply discretion.

Furthermore, prohibitions to import and export goods from/to sanctioned entities are inconsistent with Article XI:1 (General Elimination of Quantitative Restrictions) of the GATT 1994.[231] Article XI:1 reads as follows:

> No prohibitions or restrictions other than duties, taxes or other charges, whether made effective through quotas, import or export licences or other measures, shall

---

229. Appellate Body Reports, *European Communities—Measures Prohibiting the Importation and Marketing of Seal Products*, ¶ 5.86, WTO Doc. WT/DS400/AB/R/WT/DS401/AB/R (adopted June 18, 2014).

230. The WTO adjudicators have recognized that the presumption of "likeness" could be accepted. It was pointed out that "where a measure provides for a distinction based exclusively on origin, there will or can be services and service suppliers that are the same in all respects except for origin and, accordingly, 'likeness' can be presumed and the complainant is not required to establish 'likeness' on the basis of the relevant criteria set out above." Appellate Body Report, *Argentina—Measures Relating to Trade in Goods and Services*, ¶ 6.38, WTO Doc. WT/DS453/AB/R (adopted May 9, 2016).

231. GATT 1994, *supra* note 228, at art. XI:1.

> be instituted or maintained by any contracting party on the importation of any product of the territory of any other contracting party or on the exportation or sale for export of any product destined for the territory of any other contracting party.[232]

The WTO jurisprudence, in which the ambit of Article XI:1 was analyzed, proves that the scope of the obligation to eliminate quantitative restrictions is comprehensive. In particular, it was concluded that: "[T]he text of Article XI:1 is very broad in scope, providing for a general ban on import or export restrictions or prohibitions 'other than duties, taxes or other charges'."[233]

Moreover, restrictions on trade in services might violate the Most-Favoured-Nation obligation embedded in Article II:1[234] and market access obligations under Article XVI:1[235] of the General Agreement on Trade in Services (GATS), if a state undertook commitments in a specific sector and mode of supply. Few clarifications are warranted here. The obligations under the GATS are undertaken in each specific services sector and with regard to four modes of supply.[236] Once a particular commitment is inscribed in a WTO member's schedule of commitments, it becomes a subject of the MNF obligation enshrined in Article II:1 as well as the market access obligation of Article XVI:1 of the GATS.

The violation of the commitments under WTO law could only be justified under the exceptions embedded in the relevant WTO agreements. Regarding cyber sanctions, the most plausible justification, which could be invoked by a state that implements such measures, is the national security exception.[237] The national security exception, in the relevant part, reads as follows: "Nothing in this Agreement shall be construed: . . . (b) to prevent any Member from taking any action which it considers necessary for the protection of its

---

232. *Id.*

233. Panel Report, *India—Quantitative Restrictions on Imports of Agricultural, Textile and Industrial Products*, ¶ 5.128, WTO Doc. WT/DS90/R (adopted Sep. 22, 1999), upheld by Appellate Body Report WTO Doc. WT/DS90/AB/R.

234. Article II:1 reads as follows: "With respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country." General Agreement on Trade in Services, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, Apr. 15, 1994, 1869 U.N.T.S. 183 [hereinafter GATS].

235. Article XVI:1 reads as follows: "With respect to market access through the modes of supply identified in Article I, each Member shall accord services and service suppliers of any other Member treatment no less favourable than that provided for under the terms, limitations and conditions agreed and specified in its Schedule." *Id.* at art. XVI:1.

236. *Id.* at art. I:2.

237. GATT 1994, *supra* note 228, at art. XXI; GATS, *supra* note 234, at art. XIV *bis*.

essential security interests . . . (iii) taken in time of war or other emergency in international relations."

The WTO jurisprudence, wherein the invocation of the national security exception has been deliberated, provides a guidance on how WTO adjudicators define the ambit of this clause.[238] In particular, the panel in *Russia – Traffic in Transit* has left a considerable right to the WTO members invoking the national security justification to decide the situations in which this clause could be invoked. In a nutshell, the WTO adjudicators' right to review the invocation of this exception is confined to a determination if an objective element—"taken in time of war or other emergency in international relations," is fulfilled; whether a member communicated "essential security interests" in good faith, and if there is a minimum degree of plausibility between the imposed measures and declared national security interests.[239]

The prerequisite "taken in time of war or other emergency in international relations" was interpreted as an objective standard.[240] The wording "emergency in international relations" was defined as "a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state."[241] In the issued panel reports, the military conflict between Ukraine and the Russian Federation and the severance of diplomatic, consular, economic, and trade relations between Saudi Arabia and Qatar were qualified as an "emergency in international relations" for the purposes of the national security exception.[242]

It is debatable and a matter of further research whether cyberattacks can meet the threshold of being acknowledged as an "emergency in international relations."[243] Although, it can be argued that cyberattacks on critical infrastructure that undermine the

---

238. Panel Report, *Russia—Measures Concerning Traffic in Transit*, WTO Doc. WT/DS512/R (adopted Apr. 26, 2019); Panel Report, *Saudi Arabia—Measures Concerning the Protection of Intellectual Property Rights*, WTO Doc. WT/DS567/R (under appeal since July 28, 2020).

239. Panel Report, *Russia—Measures Concerning Traffic in Transit*, *supra* note 238, ¶¶ 7.29, 7.138.

240. "The Panel understands this phrase to require that the action be taken *during* the war or other emergency in international relations. This chronological concurrence is also an objective fact, amenable to objective determination." *Id.* ¶ 7.70.

241. *Id.* ¶ 7.76.

242. "By December 2016, the situation between Ukraine and Russia was recognized by the UN General Assembly as involving armed conflict." *Id.* ¶ 7.122.; Panel Report, *Saudi Arabia—Measures Concerning the Protection of Intellectual Property Rights*, *supra* note 238, ¶¶ 7.257–7.270.

243. Indeed, the growing body of literature explores the possibility of applying the concept "use of force" for cyberattacks. However, there is no consensus on this matter yet. *See, e.g.*, MOYNIHAN, *supra* note 3, at 52.

exercise of state functions should be acknowledged as "other emergency in international relations."[244]

To sum up, cyber sanctions may violate WTO commitments, and it is debatable whether they could be justified under the national security clause as it has been interpreted in the current WTO jurisprudence.

B. *Consistency with International Investment Law*

Cyber sanctions could also violate the standards of treatment incorporated in International Investment Agreements (IIAs) (a notion that includes both bilateral investment treaties (BITs) and preferential trade agreements (PTAs) with investment chapters).[245] These instruments are designed to protect foreign investments and regulate conduct of host states. According to the United Nations Conference on Trade and Development (UNCTAD), there are 2,339 BITs in force and 319 treaties with investment provisions.[246]

In this context, cyber sanctions, such as freezing of assets, property, and interests in property can result in legal claims of indirect expropriation. These claims could be substantiated by the factual inability to exercise any control over an investor's property, reinforced by a potentially extended duration of cyber sanction.[247] Even though

---

244. For a similar view, *see,* for example, George-Dian Balan, *On Fissionable Cows and the Limits to the WTO Security Exceptions* (2018), https://papers.ssrn.com/abstract=3218513 (last visited July 20, 2021) [https://perma.cc/R42G-5PLM] (archived July 20, 2021).

245. Some authors have briefly explored this issue with regard to economic sanctions. *See, e.g.*, Jessica Beess & Jessica Chrostin, *Unilateral and Multilateral Sanctions in Investment Treaty Arbitration*, 110 PROC. ANN. MEETING AM. SOC'Y INT'L L. 207, 207 (2016); Anne van Aaken, *International Investment Law and Targeted Sanctions: An Uneasy Relationship,* BUCERIUS L. J., https://law-journal.de/archiv/jahrgang-2015/heft-1/international-investment-law-and-targeted-sanctions-an-uneasy-relationship/ (last visited July 20, 2021) [https://perma.cc/UA69-P9VX] (archived July 20, 2021).

246. International Investment Agreements Navigator, UNCTAD INVESTMENT POLICY HUB (2020), https://investmentpolicy.unctad.org/international-investment-agreements (last visited July 20, 2021) [https://perma.cc/YQ7E-CPRD] (archived July 20, 2021).

247. This was stated, for instance, in *Compañía de Aguas del Aconquija S.A. and Vivendi Universal S.A. v. Republic of Argentina*, ICSID Case No. ARB/97/3, Award, ¶ 7.5.20 (Aug. 20, 2007): "*There is extensive authority for the proposition that the state's intent, or its subjective motives are at most a secondary consideration. While intent will weigh in favour of showing a measure to be expropriatory, it is not a requirement, because the effect of the measure on the investor, not the state's intent, is the critical factor*." Notwithstanding that there may be a variation in the assessment of cases among arbitral tribunals, there is a general understanding that the key determinant for a case of indirect expropriation is the effect caused by a certain measure, subject to certain, qualified exceptions, not the intent of the state. For a summary of the qualifying exceptions see, for example, JONATHAN BONNITCHA, SUBSTANTIVE PROTECTION UNDER INVESTMENT TREATIES: A LEGAL AND ECONOMIC ANALYSIS 244 (2014) (ebook),

such restrictions are of a temporary nature, they can be extended almost indefinitely, hence depriving an investor of the right to exercise control over the property.

Additionally, restrictions on the use of an investor's property, as well as restrictions on transactions with sanctioned parties, could give rise to the investors' claims of a violation of the Fair and Equitable Treatment (FET). The FET clauses are frequently incorporated in the IIAs and can be breached if the "legitimate expectations" of investors were compromised. In the *Tecmed* dispute, investors' basic expectations were understood through the lens of the principle of good faith:

> [F]oreign investor expects the host State to act in a consistent manner, free from ambiguity . . . and . . . may know beforehand any and all rules and regulations that will govern its investments, as well as the goals of the relevant policies and administrative practice or directives, to be able to plan its investment and comply with such regulation.[248]

The legitimate expectations of an investor may include the legitimate expectation to use its property and transact business with the entities that are not obviously involved in malicious cyber-enabled activities. These expectations may be hindered by unilateral cyber sanctions.

Finally, cyber sanctions can also be imposed against persons that facilitate or enable malicious cyber-enabled activities or that are involved in transactions with the sanctioned entities. Broad application of cyber sanctions can provoke investment disputes initiated not only by the investors from states directly affected by designations, such as Russia, China, or Iran, but also by investors from other jurisdictions.[249] In this regard, sanctions imposed on Huawei and their immediate effect on the UK and Taiwanese companies in the semiconductor sector are an excellent example of the repercussions these restrictions can cause for investments and investors in third states.[250]

---

http://ebooks.cambridge
.org/ref/id/CBO9781107326361 (subscription required) (last visited July 20, 2021).

248. Técnicas Medioambientales Tecmed, S.A. v. Mex., ICSID Case No. ARB(AF)/00/2, Award, 61 (May 29, 2003).

249. It should be noted that the US has no BITs or IIAs with the Russian Federation, Iran, or North Korea. Furthermore, the current US China Phase One agreement does not contain provisions on investment. On the other hand, the UK has BITs with the Russian Federation (since 1989) and China (since 1986), both with clauses on expropriation. Finally, several EU Member States have BITs in force with the Russian Federation, Iran and China. *See* International Investment Agreements Navigator, *supra* note 246.

250. Will Knight, *Trump's Feud with Huawei and China Could Lead to the Balkanization of Tech*, MIT TECH. REV., (May 24, 2019) https://www.technologyreview.com/s/613587/trumps-feud-with-huawei-and-china-could-lead-to-the-balkanization-of-tech/ [https://perma.cc/M79P-RNDW] (archived July

Contrary to international trade disputes, investors themselves (i.e., without the need to be represented by their states) can initiate investment disputes before investment tribunals. Since there is no precedent in international investment law, it is hard to predict if investment tribunals could adjudicate whether cyber sanctions are justified under such exceptions as public security, international peace, and security clauses enshrined in BITs or IIAs non-precluded measure clauses (NPM).[251] Furthermore, other justifications potentially invoked by states (e.g., the imposition of cyber sanctions as countermeasures) are difficult to sustain. As discussed before, at present there are no well-established international law obligations applicable to the states' behavior in cyberspace.[252]

This analysis reveals two points. First, the potential liability of states imposing cyber sanctions should not be underestimated under international investment law. More specifically, sanctioned entities or their counterparts could initiate investment disputes before international investment tribunals, and if successful, they can entail the payment of substantial economic damages. Second, while the peril of investment disputes may be a positive restrain on the use of cyber sanctions, paradoxically, it might hinder the potential of cyber sanctions to signal inappropriate behavior in cyberspace.

V. CONCLUSION AND REFLECTIONS

This Article has explored unilateral cyber sanctions and their legality *vis-à-vis* public international law as well as international economic law. The pressing need for such analysis can be explained by a number of reasons. First, unilateral cyber sanctions are a growing trend in the United States and the European Union—two jurisdictions that are known for being standard-setters for other states in formulating sanctions policies. What is more, the recent EU cyber sanctions were met with a great appreciation in the United States, indicating a common understanding of the value of those instruments. Second, as of today, international efforts to regulate cyberspace have been unsuccessful. In fact, there is a lack of general binding rules regulating state and non-state behavior in cyberspace. Thus, states are left with a limited number of self-help instruments (e.g., unilateral cyber sanctions) to respond to malicious activities in cyberspace. Third,

---

20, 2021); For a deeper analysis see, for example, Summary of the NCSC Analysis of May 2020 US Sanction, https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction (last visited July. 20, 2021) [https://perma.cc/RF3A-H2KC] (archived July 20, 2021).

251. *See* Wei Wang, *The Non-Precluded Measure Type Clause in International Investment Agreements: Significances, Challenges, and Reactions*, 32 ICSID REV. - FOREIGN INVEST. L. J. 447, 447 (2017).

252. For more details, *see infra* Part III.B.2.

there is a growing tendency to rely upon unilateral economic sanctions, which reflects a new geo-economic world order. To curb overenthusiastic resorts to such measures, the constraints on their use should also be discussed.

Against this background, this analysis has revealed that cyber sanctions might, in some instances, violate international law or commitments undertaken under international economic law instruments. Yet, unlike other types of sanctions regimes, such as sanctions against the perpetrators of grave human rights violations or sanctions against the proliferation of nuclear weapons, there is a legal vacuum of binding international norms that can allow states to justify cyber sanctions as countermeasures. Furthermore, cyber sanctions might not meet the threshold set by the WTO jurisprudence to be justifiable under the national security exception. Similarly, they could be successfully challenged before investment tribunals for being inconsistent with the IIAs' standards of treatment.

An undefined status of cyber sanctions in international law has two major implications. On one hand, legitimate cyber sanctions may breach various obligations under international law. On the other hand, cyber sanctions might be abused by states as instruments of technological supremacy by depriving competitors of certain legitimate benefits, such as market access. In fact, the ruthless use of cyber sanctions can reinforce the politics of unilateral power and cause economic harm.

This paradoxical outcome may backfire against the positive contributions of unilateral cyber sanctions discussed in this Article, namely the signaling function and deterrence potential in regulating malign behavior in cyberspace.

In light of the above, this Article contends that states harmed by cyberattacks could and should be legitimately allowed to rely upon unilateral cyber sanctions. This entitlement stems from the lack of other instruments to impact and deter malign behavior of state and non-state actors in cyberspace. In this context, international law should adapt by developing new interpretations, or there should be an increased coordination towards regulating the use of cyber sanctions.

Recognizing the novelty of the subject matter, this Article has attempted to set the stage for upcoming discussions by defining the main problems. Future research is expected to determine the appropriate forums where the use of cyber sanctions should be successfully deliberated as well as incentives for setting mechanisms of coordination between states.