NATIONAL RESEARCH UNIVERSITY
HIGHER SCHOOL OF ECONOMICS

Vera Rusinova, Ekaterina Martynova,

Polina Kurakina

FIGHTING CYBER-ATTACKS WITH SANCTIONS: NEW THREATS, OLD RESPONSES

BASIC RESEARCH PROGRAM

WORKING PAPERS

SERIES: LAW

WP BRP 96/LAW/2020

Vera Rusinova,[1] Ekaterina Martynova,[2]
Polina Kurakina[3]

FIGHTING CYBER-ATTACKS WITH SANCTIONS: NEW THREATS, OLD RESPONSES[4]

This paper contributes to the understanding of why states resort to 'good old' sanctions to meet the relatively new threat of cyber intrusions and whether this type of response is a forced measure or an effective tool to halt, prevent and punish attacking states. The tools of analysis used in this paper are legal positivism, and political and economic theories, including Mancur Olson's theory of groups, Francesco Giumelli's analytical framework for sanction assessment, cost-benefit analysis and game theory. The authors address the effectiveness of sanctions as a reaction to cyber-enabled activities through the lens of regulation introduced in the US and the EU, which are the most developed counter-cyber sanction regimes, analyzing publicly known cases of cyber-related sanctions.

JEL Classification: Z

Keywords: sanctions, cyber operations, cybersecurity, retorsion, effectiveness.

[1] Vera Rusinova is Doctor of legal sciences, LL.M (Goettingen), Professor, Head of the School of International Law of the Law Faculty, the National Research University Higher School of Economics; leader of the Research and Study Group 'International Law in the Age of Cyber' (E-mail: vrusinova@hse.ru).

[2] Ekaterina Martynova is a Master's student, 'Law of International Trade, Finance, and Economic Integration', the National Research University Higher School of Economics; member of the Research and Study Group 'International Law in the Age of Cyber' (E-mail: eamartynova_1@edu.hse.ru).

[3] Polina Kurakina is a Master's student, 'Law of International Trade, Finance, and Economic Integration', the National Research University Higher School of Economics; member of the Research and Study Group 'International Law in the Age of Cyber' (E-mail: pol.kurakina@yandex.ru).

[4] The article was prepared within the framework of the Academic Fund Program at the National Research University Higher School of Economics (HSE University) in 2020 (grant № 20-04-020) and within the framework of the Russian Academic Excellence Project '5-100'.

Introduction

Cyber incidents have become daily events. According to Kaspersky statistics, in 2019, 19.8% of computers user were subjected to at least one malware-class attack. Almost 1 billion attacks were launched all over the world, and about 273.8 million unique URLs were recognized as malicious.[5] Only some cyber attacks are suspected of being state sponsored. The Council of Foreign Relations has tracked significant cyber operations since 2005 and has a list of 33 countries suspected of sponsoring cyber operations with China, Russia, Iran, and North Korea designated as responsible for 77% of all cyber operations of this type.[6] In 2019, about 77 allegedly inter-state operations, mostly espionage, were reported.[7]

Responses from the states suffering from cyber operations include sanctions, the expulsion of diplomats, criminal indictments under domestic law and, rarely, openly announced 'hacking back'. Sanctions have been applied in response to 12 cyber operations by the US and the EU.[8] The US imposed sanctions on North Korea in response to the Sony Pictures Hacking in 2015[9] and for an attack against crypto-currency exchanges in March 2020.[10] US sanctions against Russian 'cyber actors' were imposed for the meddling in the US presidential elections in 2016,[11] phishing campaigns against crypto-currency exchanges in September 2020[12] and the cyber attacks that used Triton malware in October 2020.[13] Six Nigerians were sanctioned by the US for business email and romance fraud in June 2020.[14] The Iranian cyber group 'APT39', 45 associated individuals, and a front company, Rana Intelligence, which were designated as being backed by the Iran's Ministry of Intelligence and Security, were sanctioned by the US for a series of cyber attacks in September 2020.[15] The US in 2018 and 2019 and the EU in 2020 used targeted sanctions against Russian citizens and entities for the Petya and NotPetya ransomware,[16] and North Korean and Chinese

---

[5] Kaspersky Security Bulletin'19. *Statistics*, available at: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf (accessed on 15 October 2020).

[6] Council of Foreign Relations, *Cyber Operation Tracker*, available at: https://www.cfr.org/cyber-operations/ (accessed on 15 October 2020).

[7] *Ibid.*

[8] The UK implemented the EU sanctions so far, however, when the UK Cyber (Sanctions) (EU Exit) Regulations 2020 will come into force, they will replace the EU sanctions regime by its own (The Cyber (Sanctions) (EU Exit) Regulations 2020 and The Sanctions (EU Exit) (Miscellaneous Amendments) (No. 4) Regulations 2020, SI, 2020 Nos. 597, 951, available at: https://www.legislation.gov.uk/uksi/2020/597/introduction/made (accessed on 11 November 2020)).

[9] US Secretary of State, press statement *Condemning Cyber-Attack by North Korea*, 19 December 2014, available at: https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm (accessed on 10 August 2020).

[10] US Department of the Treasury, press-release *Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group*, 2 March 2020, available at: https://home.treasury.gov/news/press-releases/sm924 (accessed on 10 October 2020).

[11] US Department of the Treasury, press-release *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 US Elections and Malicious Cyber-Attacks*, 15 March 2018, available at: https://home.treasury.gov/news/press-releases/sm0312 (accessed on 10 August 2020).

[12] US Department of the Treasury, press-release *Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft*, 16 September 2020, available at: https://home.treasury.gov/news/press-releases/sm1123 (accessed on 16 October 2020).

[13] US Department of the Treasury, press-release *Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware*, 23 October 2020, available at: https://home.treasury.gov/news/press-releases/sm1162 (accessed on 4 November 2020).

[14] US Department of the Treasury, press-release *Treasury Sanctions Nigerian Cyber Actors for Targeting US Businesses and Individuals*, 16 June 2020, available at: https://home.treasury.gov/news/press-releases/sm1034 (accessed on 10 October 2020).

[15] US Department of State, press statement *The United States Sanctions Cyber Actors Backed by Iranian Intelligence Ministry*, 17 September 2020, available at: https://www.state.gov/the-united-states-sanctions-cyber-actors-backed-by-iranian-intelligence-ministry/ (accessed on 25 October 2020).

[16] US Department of the Treasury, press-release *Treasury Sanctions Russian Federal Security Service Enablers*, 11 June 2018, available at: https://home.treasury.gov/news/press-releases/sm0410 (accessed on 10 August 2020); Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber attacks threatening the Union or its Member States, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R1125&from=EN (accessed on 10 August 2020) (hereinafter: *EU Regulation of 30 July 2020*).

citizens for the WannaCry virus.[17] The EU also imposed sanctions against the Main Centre for Special Technologies of the GRU, the military intelligence wing of the Russian armed forces, and four of its officers for the attempted cyber attack against the Organization for the Prohibition of Chemical Weapons[18] and for the alleged cyber attack on the *Bundestag* in October 2020,[19] and against two Chinese citizens and one legal entity for 'Operation Cloud Hopper' in July 2020.[20]

Even taking into consideration the average percentage of espionage operations, which are usually not followed by economic sanctions,[21] the use of this tool could have been conceived as an exception to the rule. However, should these statistics be juxtaposed with the number of cases when states that suffered from alleged inter-state cyber operations officially attributed these malicious acts to other states and used other means of response, the role of sanctions becomes significant and is growing. This raises the question of why states resort to 'good old' sanctions to meet the relatively new threat of cyber intrusions. Is this type of response a forced measure or an effective tool to halt, prevent and punish attacking states?

In economic theory the term 'sanctions' is generally referred to the deliberate 'withdrawal, or threat of withdrawal, of customary trade or financial relations', wherein 'customary' indicates those levels of trade and capital flows between the state imposing sanctions (the sender) and the targeted state (the target).[22] Alongside traditional forms of sanctions as 'trade-restricting policies between sovereign nations',[23] including boycotts, embargoes, tariffs and non-tariff barriers, export and/or import restriction such as quotas,[24] states can also resort to direct financial sanctions and impede the flow of capital, in particular by delaying or interrupting publicly funded loans or grants, or freezing assets controlled by the state imposing sanctions.[25] Although sanctions can also take form of the restriction of movement of particular individuals ('travel ban'), they are predominantly economic or financial. Contemporary studies usually highlight the political nature and functions of sanctions — they are not viewed as a purely economic phenomenon to be assessed only from an economic perspective.[26] Sanctions are considered to be 'politically motivated'[27] and their direct target is not

---

[17] US Department of the Treasury, press-release *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, 13 September 2019, available at: https://home.treasury.gov/index.php/news/press-releases/sm774 (accessed on 10 August 2020); EU Regulation of 30 July 2020.

[18] EU Regulation of 30 July 2020.

[19] Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber attacks threatening the Union or its Member States, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.LI.2020.351.01.0001.01.ENG&toc=OJ%3AL%3A2020%3A351I%3ATOC (accessed on 24 October 2020) (hereinafter: *EU Regulation of 22 October 2020*); Press release *UK Enforces New Sanctions against Russia for Cyber Attack on German Parliament* of 22 October 2020, available at: https://www.gov.uk/government/news/uk-enforces-new-sanctions-against-russia-for-cyber-attack-on-german-parliament#:~:text=The%20UK%20has%20announced%20it,cyber%20attacks%20on%20Germany's%20Parliament (accessed on 24 October 2020).

[20] EU Regulation of 30 July 2020.

[21] Imposition of sanctions for the cyber-espionage 'Operation Cloud Hopper' by the EU is the sole example (EU Regulation of 30 July 2020).

[22] Hufbauer G.C., Schott J.J., Elliott K. A., Oegg B. *Economic Sanctions Reconsidered* (3rd Edition), Washington, DC: Peterson Institute, 2007, p. 3.

[23] Smeets M. Can Economic Sanctions Be Effective? World Trade Organization, Economic Research and Statistics Division; *Staff Working Paper ERSD-2018-03*, 15 March 2018, p. 4.

[24] For discussion of compatibility of economic sanction with WTO obligations see, e.g.: Neuwirth R.J., Svetlicinii A., The Economic Sanctions over the Ukraine Conflict and the WTO: 'Catch-XXI' and the Revival of the Debate on Security Exceptions, *Journal of World Trade*, 2015, Issue 5, pp. 891-914. Available at: https://kluwerlawonline.com/journalarticle/Journal+of+World+Trade/49.5/TRAD2015035 (accessed on 10 October 2020).

[25] Hufbauer et al. *Op.cit*, p. 63.

[26] Baldwin, D. A., Pape, R. A. Evaluating Economic Sanctions, *International Security*, 1998, 23(2), pp. 189-198.

[27] Giumelli, F. *Coercing, Constraining and Signaling: Explaining UN and EU Sanctions after the Cold War*. Colchester, UK: ECPR Press, 2011, p. 15.

necessarily the ultimate target of the sanctions, for sanctions can be imposed on private actors with the purpose of influencing the decision-making of state authorities.

Economic sanctions are common in international politics, and the question of this tool's effectiveness has been studied for decades.[28] The most authoritative methodological basis for the assessment of the effectiveness of sanctions was by Hufbauer, Schott, and Elliot,[29] who proposed guidelines for the estimation of the potential sanctions success based on indicators including policy goals and the security, political, or other costs incurred by the sender.[30] A legal strand of sanction research is represented by inquiries focusing on the legal nature and legality of unilateral sanctions.[31] The legality of sanctions not authorized by the UN Security Council remains in a grey area of international law,[32] dividing scholars into those supporting[33] and those challenging it.[34]

---

[28] Among scholarship before the 1990s see, e.g.: Galtung J. On the Effects of International Economic Sanctions: With Examples from the Case of Rhodesia, *World Politics*, 1967, vol. 19(3), pp. 378–416; Doxey M. P. *International Sanctions in Contemporary Perspectives*, New York: St. Martin's Press, 1987; Nossal, K. R. International Sanctions as International Punishment, *International Organization*, 1989, vol. 43 (2), pp. 301 –322.

[29] In 1985 Hufbauer, Schott, and Elliot published the first edition of *Economic Sanctions Reconsidered: History and Current Policy* based on case studies of 103 sanctions episodes and analysis of sanctions-related public policies. The second edition of *Economic Sanctions Reconsidered* of 1990 (Hufbauer G.C., Schott J.J., Elliott K.A. *Economic Sanctions Reconsidered: History and Current Policy* (2nd Edition), Washington D.C.: Institute for International Economics, 1990) and the third edition of 2007 (Hufbauer G.C., Schott J.J., Elliott K.A., Oegg B. *Economic Sanctions Reconsidered* (3rd Edition), Washington D.C.: Peterson Institute, 2007) remain among the most cited studies on the subject. A number of quantitative studies followed the work of Hufbauer et al, most of which demonstrated that while sanctions sometimes make targets change their behavior, some identifiable factors do contribute to sanctions success (e.g. Dashti-Gibson J., Davis P., Radcliff B. On the Determinants of the Success of Economic Sanctions: An Empirical Analysis, *American Journal of Political Science*, 1997, vol. 41, pp. 608–618; Drezner D.W. Conflict Expectations and the Paradox of Economic Coercion, *International Studies Quarterly*, 1998, 42, pp. 709–731). Nonetheless, this approach of Hufbauer, Schott, and Elliot is not free from critique (see: Pape R. A. Why Economic Sanctions Do Not Work, *International Security*, 1997, vol. 22 (2), pp. 90–136). The UN Targeted Sanctions database by Biersteker, Eckert, and Tourinho (Biersteker T. J., Eckert S. E., Tourinho M. (Eds.), *Targeted Sanctions*, Cambridge, UK: Cambridge University Press, 2016) is another heavily cited data source for research on whether economic sanctions work. Based on analysis of 23 UN targeted sanctions episodes, Biersteker, Eckert, and Tourinho assess only 22% of sanctioning cases as successful which is lower than the overall success rate reported by Hufbauer et al. (34%). Rosenberg et al. (Rosenberg E., Goldman Z. K., Drezner D., Solomon-Strauss J., *The New Tools of Economic Warfare: Effects and Effectiveness of Contemporary US Financial Sanctions*, Washington, DC: Center for a New American Security, 2016) examine effectiveness of particularly financial sanctions and conclude that this type of sanctions is relatively more effective (in up to 40% of cases) than other types of sanctions. Lektzian and Patterson (Lektzian D., Patterson D., Political Cleavages and Economic Sanctions: The Economic and Political Winners and Losers of Sanctions, *International Studies Quarterly*, 2015, 59 (1), pp. 46–58) and Pond (Pond A., Economic Sanctions and Demand for Protection, *Journal of Conflict Resolution*, 2017, 61 (5), pp. 1073–1094) study economic and political costs incurred by senders and targets as well as micro-dynamics of sanctions success. For a detailed and critical review of literature on economic sanctions' effectiveness refer to Peksen D., When Do Imposed Economic Sanctions Work? A Critical Review of the Sanctions Effectiveness Literature, *Defense and Peace Economics*, published online on 31 May 2019, DOI: 10.1080/10242694.2019.1625250.

[30] Hufbauer et al, *Economic Sanctions Reconsidered* (3rd Edition), pp. 158-159.

[31] On these issues, see, e.g.: Marcuss S. J., Mathias D.S., US Foreign Policy Export Controls: Do They Pass Muster Under International Law? *International Tax and Business Lawyer*, 1984, vol. 2, p. 1; Curtis B., Goldsmith J.L., Customary International Law as Federal Common Law: A Critique of the Modern Position, *Harvard Law Review*, 1997, vol. 110, no. 4, pp. 815–76.

[32] Hofer A., The Developed/Developing Divide on Unilateral Coercive Measures: Legitimate Enforcement or Illegitimate Intervention?, *Chinese Journal of International Law*, 2017, vol. 16, no. 2, pp. 175–214.

[33] The first general justification for legality of economic coercive measures is the *Lotus* principle (the Case of the S.S Lotus (*France v. Turkey*), Judgment, PCIJ 1927 (http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf), 18). States are free to conduct economic relations at their own discretion provided they respect their obligations under treaties and legal norms that have been recognized as customary international law. In light of this principle, economic sanctions are *prima facie* legal (see Hofer A., *Op.cit*, para 9). The second justification is based on the law of countermeasures. In this sense, Marco Gestri has described the European Union as 'a trailblazer' in implementing the doctrine of 'collective countermeasures'. (Gestri M., Sanctions Imposed by the European Union: Legal and Institutional Aspects, in Ronzitti N., (ed.), *Coercive Diplomacy, Sanctions and International Law*, 2016, p. 99. See also: Joyner D., United Nations Counter-Proliferation Sanctions and International Law, in: van den Herik L. (Ed.), *Research Handbook on U.N. Sanctions and International Law*, 2017, pp. 7-8; and Hovell, D., Unfinished Business of International Law: The Questionable Legality of Autonomous Sanctions, *AJIL Unbound*, 2019, vol. 113, pp. 140-145.

[34] Mohamad R., Unilateral Sanctions in International Law: A Quest for Legality in Marossi A.Z., Bassett M. R. (Eds.), *Economic Sanctions under International Law. Unilateralism, Multilateralism, Legitimacy, and Consequences*. The Hague, the Netherlands: Springer, 2015, pp. 71-81. See also: Happold M., Economic Sanctions and International Law: An Introduction in Happold M., Eden P. (Eds.) *Economic Sanctions and International Law*, Hart Publishing, 2016.

Studies have also been conducted on improving the legal regime and regulatory policies concerning sanctions.[35] However, sanctions taken in response to malicious cyber operations, although mentioned in general in a number of publications[36] or with respect to particular cases,[37] have not yet become the subject of separate legal research.

This paper contributes to the understanding of how the resort to and the effectiveness of economic sanctions implemented in response to cyber operations can be assessed. The research is characterized by three key features. First, the analysis is informed by legal, political and economic theories. The legal analysis represents a positivistic explanation of the resort to sanctions, which outlines the continuum of managerial and consensus-based approaches to the normative framework based on international law. This inquiry was underpinned by the opinions of the states with respect to the legal qualification of cyber operations expressed at meetings of the UN Open-Ended Working Group (OEWG) held in 2019–2020 and written statements made thereupon,[38] or articulated in other official documents. The political and economic methods applied in this research include Mancur Olson's theory of groups, Francesco Giumelli's analytical framework for sanction assessment, cost-benefit analysis and game theory. In particular, we include some estimations of the costs that targets and senders incur by imposing sanctions, and analyze the interaction between a cyber attack and a sanction as a zero-sum, non-zero-sum or cooperative game. Secondly, we address the question of the effectiveness of sanctions as a reaction to cyber activities using examples of the regulation introduced in the US and the EU that are the most developed counter-cyber sanction regimes. Thirdly, the analysis is empirically based on a poll of 12 cases, when sanctions were imposed by the US and/or the EU in response to alleged inter-state cyber operations. This dataset was collected from publicly available sources, including legal acts, press releases and statements available on the websites of the sanctioning states.

The paper is structured as follows. Part I discusses the legal considerations underpinning and explaining the resort to sanctions from the perspective of international law. Part II summarizes the legal regimes and practices of imposing sanctions in response to cyber operations by the US and the EU. Part III addresses the question of how to measure sanction effectiveness and describes some analytical tools that can be used to answer this question. Part IV concludes by outlining the prospects for cyber-related sanctions on the basis of the interaction between the legal and extra-legal layers of their assessment.

I. Resort to Sanctions from a Legal Perspective

From a legal perspective, sanctions adopted by states in response to cyber operations can take the form of either countermeasures or retorsions. A countermeasure is a means taken by an injured state to induce the state committing a wrongful act to comply with its obligations[39] and presupposes that a cyber operation, as an initial act of injury, breaches international law and is subject to

---

[35] The Carter's work on reforming the US sanctions regime can be distinguished as a particularly comprehensive (Carter B. E., International Economic Sanctions: Improving the Haphazard US Legal Regime, *Georgetown Law Faculty Publications and Other Works*, 1998, p. 1585). See also: Egle S., The Learning Curve of Sanctions – Have Three Decades of Sanctions Reform Taught Us Anything?, *Currents: Int'l Trade LJ*, 2010, p. 19; Cleveland S.H., Norm Internalization and US Economic Sanctions, *Yale J. Int'l L.*, 2001, p. 26; de Vries A., Portela C., Guijarro-Usobiaga B., Improving the Effectiveness of Sanctions: A Checklist for the EU, *CEPS Special Reports*, 2014, no. 95.

[36] See, e.g.: Delerue F., *Cyber Operations and International Law*, Cambridge: Cambridge University Press, 2020; Henriksen, A. Lawful State Responses to Low-Level Cyber-Attacks, *Nordic Journal of International Law*, 2015, vol. 84, p. 323-351.

[37] See, e.g.: Lam C. A., Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 US Presidential Election, *Boston College Law Review*, vol. 59, no. 6, p. 2167.

[38] The Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security held two substantive sessions: 9–13 September 2019 and on 10–14 February 2020, available at: http://webtv.un.org/ (accessed on 1 November 2020) (hereinafter: *OEWG, 1st or 2nd subs. session*).

[39] General Assembly Resolution 56/83 of 12 December 2001, Articles on Responsibility of States for internationally wrongful acts, Art. 49 (1) (hereinafter: *ARSIWA*).

requirements, including the proportionality and reversibility of the response, the on-going character of the initial wrongful act, and a duty of notification.[40] A retorsion is defined as 'unfriendly conduct which is not inconsistent with any international obligation of the state engaging in it' and being taken in response to an unfriendly act[41] does not necessitate a qualification of the cyber operation as violating any international legal obligation.

Sanctions taken by the US and the EU in response to cyber operations point to a clear tendency to shape them as acts of retorsion, not countermeasures. This can be explained (not excluding the relevance of other perspectives) by different but interconnected legal reasons. There is difficulty in qualifying a cyber operation as an internationally wrongful act under the primer rules, and there is difficulty in applying secondary norms. The latter include international responsibility and countermeasures, and they presuppose the necessity to attribute a malicious cyber act committed by individuals to a particular state — a duty that has a requirement to reach the standard of proof applicable in international law.

A. The Legal Qualification of Cyber Operations: from Managerialism to Consensualism

The first set of problems concerns the legal qualification of cyber operations under *lex lata*. Potentially, inter-state cyber operations can breach a number of primary rules, including the obligation to respect the sovereignty of other states, the principle of non-interference in domestic affairs, international human rights law, the prohibition to use force and, when such operations are conducted during an armed conflict, also norms of international humanitarian law. A legal obligation of 'cyber due diligence', requiring states to ensure that 'their territory is not used as a base for state or non-state hostile cyber operations against another state that cause serious adverse consequences with regard to a right of the target state',[42] in the part exceeding a general duty of the states 'not to allow knowingly its territory to be used for acts contrary to the rights of other States' as it was formulated by the ICJ in the *Corfu Channel case,*[43] is still in a nascent form and, despite the positions of some states,[44] is widely considered *lex ferenda*.[45]

The stance that cyberspace is far from being a 'wild west' and is governed by non-cyber specific norms of international law, and in particular the Charter of the UN, is well represented in

---

[40] Art. 49-53 of the ARSIWA.

[41] International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, 2001. *Yearbook of the International Law Commission, 2001*, vol. II, Part Two. P. 128, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (hereinafter: *ARSIWA with Commentaries*).

[42] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Ed. Schmitt M.). Cambridge: Cambridge University Press, 2017, p. 30-50 (hereinafter: *Tallinn 2.0*).

[43] ICJ, *Corfu Channel Case* (United Kingdom v. Albania), Judgment, 9 April 1949, ICJ Reports (1949) 4, p. 22.

[44] The Netherlands: Ministry of Foreign Affairs. Netherlands. Letter to the Parliament on the International Legal Order in Cyberspace, 5 July 2019, p. 4-5, available at: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (accessed on 1 November 2020); France: Ministère des Armées. France. International Law Applied to Operations in Cyberspace, October 2019, p. 6, 9-10, available at: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (accessed on 1 November 2020).

[45] The GGE Report of 2015 envisages a negative obligation of states 'not knowingly allow their territory to be used for internationally wrongful acts using ICTs' as a 'voluntary, non-binding norms, rules or principles of responsible behaviour of States' (Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 26 June 2015, A/70/174, para. 13 (3)), available at: https://undocs.org/A/70/174 (accessed on 1 November 2020) (hereinafter: *GGE Report 2015*). See: US, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011, p. 10, available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (assessed on 1 November 2020). See also: Shackelford S. J., Russell S., Kuehn A., Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors, *Chicago Journal of International Law*, 2016, Vol. 17, Issue 1, p. 22-23; Delerue F., Cyber Operations and the Principle of Due Diligence, In *Cyber Operations and International Law* (Cambridge Studies in International and Comparative Law), Cambridge University Press, 2020, pp. 353-376.

legal scholarship[46] and—at least, as a matter of principle—affirmed by states.[47] However, even this level of abstraction is not free from discontent.[48] The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security was not able to adopt final reports in 2016–2017 due to the position articulated by Cuba[49] and backed by Russia[50] and China,[51] under which applicability of *jus ad bellum* and *jus in bello* (international humanitarian law) may lead to the establishment of the 'equivalence between the malicious use of ICTs and the concept of "armed attack"'[52] under Article 51 of the UN Charter, and, thereby militarize the use and the response to ICT. The same divergence was found in the positions of the states expressed at the OEWG meetings in 2019–2020.[53] While the majority of states confirmed applicability of international law in its entirety to cyberspace,[54] it was contested by a group of states using arguments related to the importance of state consent for the extension of the scope of non-cyber specific norms, indeterminate thresholds of 'armed attack' by cyber means and the doubtful applicability of international humanitarian law to hybrid warfare and to civilian perpetrators of cyber attacks.[55] Some states took an intermediate position by appealing to the need to adopt new legally binding instruments.[56]

Apart from the question of whether it is uncontested, the question of how international law applies to cyberspace needs clarification. This clarification takes place in the *ex cathedra* managerial (or interventionist) form of the logical adaptation and the detailing of general norms by experts and scholars,[57] or originate from state behavior shaping either law-making or law-

---

[46] See, *inter alia*: *Tallinn 2.0*; Routledge Handbook of War, Law and Technology (Ed. by Gow J., Dijxhoorn E., Kerr R., Verdirame G.), Routledge, 2019; Dinstein Y., Dahl A. W., *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary*, Springer, 2020 (hereinafter: *Oslo Manual*).

[47] The General Assembly welcomed this affirmation of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) on numerous occasions (Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455)]. 70/237. Developments in the field of information and telecommunications in the context of international security). Significant number of states confirmed this applicability during the sessions of the OEWG.

[48] See also: Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Remarks. Markoff M. G., Deputy Coordinator for Cyber Issues Office of the Coordinator for Cyber Issues, 23 June 2017, available at: https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ (accessed on 1 November 2020).

[49] Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. New York, 23 June 2017, available at: http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information (accessed on 1 November 2020).

[50] Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere, 29 June 2017, available at: http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288 (accessed on 1 November 2020).

[51] China did not publically share its position, see: Korzak E., UN GGE on Cybersecurity: The End of an Era? *The Diplomat*, 31 July 2017, available at: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe (accessed on 1 November 2020).

[52] Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. New York, 23 June 2017, available at: https://www.justsecurity.org/wp-content/uploads/2017/06/cuban-expert-declaration.pdf (accessed on 1 November 2020).

[53] For instance, Pakistan, Russia, The Syrian Arab Republic (OEWG, 1st subs. session, 11 September 2019; 2st subs. session, 11 February 2020).

[54] Austria, Brazil, Canada, Chile, the Czech Republic, the European Union, Italy, Lichtenstein, New Zealand, Pacific Islands Forum, Sweden, Switzerland, the United Kingdom and others (OEWG, 2st subs. session, 11 February 2020).

[55] Russia raised a question on how does the application of international law in cyberspace correlate with voluntary principle (OEWG, 2st subs. session, 11 February 2020).

[56] Cuba, Egypt, Jordan, Pakistan, Singapore, Syria, (OEWG, 2st subs. session, 11 February 2020).

[57] *Tallinn 2.0*; *Oslo Manual*.

interpreting (as the subsequent application of the relevant rules) paths. The challenges underpinning the managerial path are well reported and lie either in the thresholds or in the limited scope of the application of *lex lata*, which lead to their under-inclusivity or inadequacy in respect of allegedly inter-state cyber operations,[58] or in the contested applicability of general, non-cyber specific rules in a cyber context. Taking into account recently articulated positions of states officially expressed at OEWG sessions and elsewhere, these challenges can be outlined as follows.

The application of the well-established principle of international law to respect sovereignty[59] in cyberspace encounters not only the problem of the indeterminacy of its threshold and the scope of protected infrastructure,[60] but also a split in the official positions of different states with respect to the legal nature of this principle as giving rise to a rule or merely being a fundamental principle. The US and the UK articulated their positions that sovereignty is solely a principle, not a rule.[61] In contrast, France reserved a maximal wide approach claiming that any cyber attacks at 'information systems located on its territory', including 'equipment and infrastructure located on national territory; connected objects, logical components and content operated or processed via electronic communication networks which cover the national territory or from an IP address attributed to France' and 'domains belonging to national registers' will violate its sovereignty.[62] The Netherlands explicitly articulated its position supporting the 'sovereignty as a rule' approach, appealing to the two-element test in *Tallinn 2.0* and the necessity of a minimal threshold.[63] Finland has recently expressed a comparable position at the OEWG.[64]

In contrast to sovereignty, the application of the non-interference principle to cyber operations is not contested by states, instead problems arise from its material scope. This principle can be regarded as captured by the dichotomy between types of interventions, which states do not want to allow in respect of themselves and which they would like to be free to conduct in respect of others. Thus, at the international level, although not contesting the normativity of the non-interference principle, states reserved a very high level of abstraction for it and by the use of the two-pronged test elaborated in the ICJ judgement in the *Nicaragua case* of 1986[65] apply a very broad grid to outlawed behavior. Therefore, the non-interference principle, which was under-inclusive in non-cyber operations, became extremely under-inclusive in cyber operations.

---

[58] D'Aspremont J., Cyber Operations and International Law: An Interventionist Legal Thought, *Journal of Conflict and Security Law*, 2016, Vol. 21, Issue 3, p. 580–590.

[59] International Court of Justice (hereinafter: *ICJ*), Corfu Channel (*The UK. v. Albania*), Judgment of 9 April 1949, I.C.J. Reports. 1949; ICJ, Military and Paramilitary Activities in and against Nicaragua *(Nicaragua v. United States of America*), Judgment (Merits) of 27 November 1986, I.C.J. Reports. 1986; ICJ, Certain Activities Carried out by Nicaragua in the Border Area (*Costa Rica v. Nicaragua*) and Construction of a Road in Costa Rica Along the San Juan River (*Nicaragua v. Costa Rica*), Judgment of 16 December 2015, I.C.J. Reports, 2015.

[60] Experts of the *Tallinn 2.0.* were strongly divided in respect of this issue (see *Tallinn 2.0*, p. 20-27).

[61] Memorandum from Jennifer M.O Connor, General Counsel of the Department of Defense, International Law Framework for Employing Cyber Capabilities in Military Operations, 19 January 2017, cit. on: The Application of International Law to State Cyberattacks Sovereignty and Non-intervention. Research Paper. December 2019, p. 9. Fn. 36, available at: https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf (accessed on 1 November 2020); Wright J., Cyber and International Law in the 21st Century, 2018, available at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (accessed on 1 November 2020).

[62] Ministère des Armées, France, International Law Applied to Operations in Cyberspace, October 2019, p. 6, available at: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (accessed on 1 November 2020).

[63] Ministry of Foreign Affairs, the Netherlands, Letter to the Parliament on the International Legal Order in Cyberspace, available at: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace (accessed on 1 November 2020); Schmitt M. The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis, *Just Security*, 14 October 2019, available at: https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/ (accessed on 1 November 2020).

[64] Finland's National Positions, International Law and Cyberspace, 2020, available at: https://front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf (accessed on 1 November 2020).

[65] *Nicaragua* v. *United States of America*, para. 205.

There is a strong tendency in the legal literature to problematize the element of coercion as rendering the non-interference principle almost unworkable in the cyber context (for attacks having malicious or retaliatory aims cannot be qualified as coercive),[66] but there are also reasons to claim, that the first element (*domaine réservé*) also significantly restricts the applicability of this principle to cyber-operations. According to the *Nicaragua* test, a prohibited intervention must be one bearing on 'matters in which each State is permitted, by the principle of State sovereignty to decide freely'.[67] The notion of *domaine réservé* was and remains bound with realization by the state of its powers and competences, but cannot be regarded as a 'shelter, fully covering entire areas of politics'.[68] For instance, although the election process falls under *domaine réservé*, this does not mean that all activities related thereto are protected by the non-interference principle. Elections belong to *domaine réservé*, but it covers only governmental functions related to this process. If we take the meddling into the US elections of 2016 as an example, this operation was multilayer, and such actions as reported attempts to hack voting machines, although apparently no votes were affected,[69] fall under *domaine réservé*. Other acts, arguably, do not. Among them are hacking by the so-called 'Cozy Bear' and 'Fancy Bear' hacking groups and the subsequent publication on WikiLeaks of the emails of the Democratic National Committee and hacking the account of John Podesta, chairman of Hillary Clinton's campaign, and a massive informational operation in social networks, based on use of 'bots' and 'trolls'. This example can serve as an illustration of the very modest role of the non-interference principle.

Application of *jus ad bellum* norms of international law is based on the two-threshold approach envisaged in the UN Charter in the duality of the 'use of force' and 'an armed attack',[70] which was further supported by the 'scale and effects' doctrine elaborated by the ICJ in the *Nicaragua case.*[71] Although the military paradigm to treat inter-state cyber operations received the bulk of attention,[72] the application of these norms to cyberspace is not free from controversy. The reason for that is not only the ever-used indeterminacy argument in respect of the threshold of 'use of force' and 'armed attack'.[73] The problem is that the commonly used logic of application of *jus ad bellum* to cyber operations is based on the acknowledgment that the prohibition of the use of force may be violated by any use of force, regardless of the type of weapon,[74] and is underpinned by the permissibility of the consequential use of the analogy with kinetic attacks (causing deaths, injury or the destruction of physical objects), notwithstanding the fact that the chain of consequences launched by a cyber operation might be significantly longer in comparison to the conventional use of force. Not challenging the fact that some cyber operations can take a military form, the use of analogy can be overstretched to produce results contrasting the well-known refusal of the drafters of

[66] Declaration on Principles of International Law Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations provides for that: 'no State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind' (General Assembly Resolution 26/25 (XXV), 24 October 1970).

[67] *Nicaragua* v. *United States of America*, para. 205.

[68] Ziegler K. S. Domaine Réservéin: *The Max Planck Encyclopedia of Public International Law* (Ed. by R. Wolfrum), Oxford: Oxford University Press, 2012, vol. III, p. 213.

[69] Sanger D. E., Edmondson C., Russia Targeted Election Systems in All 50 States, Report Finds, *The New York Times*, 25 July 2019, available at: https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html (accessed on 1 November 2020).

[70] Art. 2 (4) and 51 of the UN Charter; *Nicaragua* v. *United States of America*, para. 191.

[71] *Nicaragua* v. *United States of America*, para. 195.

[72] Schmitt M.N. (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Prepared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press, 2013, p. 48–51; Roscini M., *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press, 2014, p. 53–60.

[73] See Corten O., *The Law against War*, Oxford and Portland, Oregon: Hart Publishing, 2012, p. 5-27.

[74] ICJ, *Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons*, I.C.J. Reports, 1996, p. 18, para. 39.

the Charter to understand 'economic coercion' as falling under the scope of prohibited behavior.[75]

The OEWG meeting held on 11 February 2020 reflected the affirmation of the applicability of the *jus ad bellum* norms of international law to cyber operations, underpinned by the consequential logic, as a mainstream.[76] Four states expressed their concerns and doubts. Brazil and India underscored the lack of clarity in respect of the threshold of 'use of force' and 'armed attack', whereas Pakistan in general noted its concerns on the applicability of Article 51 of the UN Charter to cyber acts and Russia took the most stringent position that this provision can be applied in the context of an armed attack only, and that a cyber attack without this context does not meet this criterion.[77] Should one not doubt the soundness of the consequentialist approach, the majority of publicly known cyber operations[78] do not reach the threshold of the 'use of force' because of their low intensity.[79]

This explains the desire of some states to extend the scope of the internationally prohibited 'use of force' by domestic efforts that count as an indication of state practice and *opinio juris*. France set forth that a 'cyber operation without physical effects' may also be qualified as the use of force and suggested using a not-exhaustive list of criteria, i.e. 'the circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not), the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target'.[80] The Dutch Minister of Foreign Affairs articulated that 'it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force'.[81] Finally, the UK Cyber Primer, although acknowledging the necessity for a cyber operation to cause 'the same or similar effects as a kinetic attack', in a footnote made a clarification permitting such a qualification for attacks, like 'a sustained attack against the UK banking system, which could cause severe financial damage to the state leading to a worsening economic security situation for the population'.[82]

The application of another set of norms—international human rights law—to alleged inter-state cyber operations is also theoretically possible in respect of cyber operations, which, inter alia, can intrude into the privacy, freedom of expression and association (following the concept of 'human rights online'[83]). However, this is dependent on the extent to which the norms of the human

---

[75] Simma B. (Ed.), *The Charter of the United Nations. A Commentary* (2nd Edition), 2002, vol. I, p. 118.

[76] OEWG, 2st subs. session, 11 February 2020; Australia: Department of Foreign Affairs and Trade, Australia's Cyber Engagement Strategy, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace, 2019; Australia's Cyber Engagement Strategy, Annex A: Australia's Position on How International Law Applies to State Conduct in Cyberspace, 2017; Germany: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE. Krieg im 'Cyber-Raum' – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung, Drucksache 18/6989, 10.12.2015, p. 10; the UK: Cyber and International Law in the 21st Century, The Attorney General Jeremy Wright QC MP Speech on the UK's Position on Applying International Law to Cyberspace; the US: Harald Hongju Koh, International Law in Cyberspace, Remarks by Harald Hongju Koh, Legal Adviser to the US Department of State, 18 September 2012, *Harvard International Law Journal Online*, 2012, vol. 54, pp. 1-12.

[77] *Ibid.*

[78] Significant Cyber Incidents Since 2006, Center for Strategic and International Studies, available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/200901_Significant_Cyber_Events_List.pdf (accessed on 1 November 2020).

[79] Watts S., Low-Intensity Cyber Operations and the Principle of Non-Intervention, in: Ohlin J.D., Govern K., Finkelstein C. (Eds.), *Cyber War: Law and Ethics for Virtual Conflicts*, Oxford: Oxford University Press, 2015, pp. 249–250.

[80] Ministry of Armed Forces, International Law Applied to Operations in Cyberspace, October 2019, p. 7, available at: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (accessed on 1 November 2020).

[81] Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace. Appendix: International Law in Cyberspace, p. 4.

[82] UK Ministry of Defence, Cyber Primer, 2nd ed., 2016, Annex 1A – International Law aspects, p. 12.

[83] General Assembly Resolution 68/167 'The Right to Privacy in the Digital Age', 18 December 2013.

rights treaties[84] can be applied extraterritorially.[85] Since the UN Human Rights Committee[86] and later the ICJ[87] admitted a disjunctive approach to the reading of the 'within its territory and subject to its jurisdiction' clause of the International Covenant on Civil and Political Rights[88] and the European Court of Human Rights (ECtHR) has elaborated spatial (control over the territory or a limited space[89]) and personal approaches (control and authority over the individuals[90]) to the notion of 'jurisdiction',[91] contained in the Convention on Protection of Human Rights and Fundamental Freedoms (EConvHR), it is possible to extend the application of these treaties to extraterritorial modes of data interception.[92] There are at least three cases adjudicated by the ECtHR: *Weber and Saravia v. Germany,*[93] *Liberty v. United Kingdom,*[94] and the *Big Brother Watch and Others v. the UK*[95] that prove that this is not a purely hypothetical scenario.

Nonetheless, the extension of the scope of international human rights instruments to extraterritorial cyber operations does not predetermine the results of the application of material human rights norms. It is especially relevant in the case of individual (targeted) interception of data or in cases of mass surveillance. The judgments rendered by ECtHR Chambers in 2018 in two cases—*Centrum för Rättvisa v. Sweden*[96] and the *Big Brother Watch and Others v. the United Kingdom*[97]—acknowledged that mass surveillance *per se* does not violate the EConvHR. As the court put it, 'the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security' falls within the wide 'margin of appreciation', which states enjoy in choosing 'how best to achieve the legitimate aim of protecting national security'.[98] While not outlawing the mass surveillance, in the *Big Brother Watch* case, the Chamber rendered a very detailed judgment, which, alongside paving the way for similar cases in the future, was designed to provide the governments of the Members of the Council of Europe with a 'road map' for the legal

---

[84] Art. 17 of the International Covenant on Civil and Political Rights, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976) (hereinafter: *the ICCPR*); Art. 8 of the Convention on Protection of Human Rights and Fundamental Freedoms, signed 4 November 1950, ETS No.005 (entered into force 3 September 1953) (hereinafter: *the EConvHR*).

[85] Milanovic M., Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, *Harvard International Law Journal*, 2015, vol. 56, no. 1, pp. 120-130.

[86] U.N. Human Rights Comm., General Comment No. 31: Nature of the General Legal Obligation on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004), para. 10.

[87] ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 9 July 2004, I.C.J. Reports 2004, pp. 178, 180, paras. 108, 111.

[88] Article 2 (1) of the ICCPR.

[89] ECtHR, *Loizidou v. Turkey*, Judgment (Preliminary Objections), 23 March 1995, para. 62. available at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57920 (accessed on 1 November 2020); ECtHR, *Al-Saadoon and Mufdhi v. the United Kingdom*, 2 March 2010 (final: 4 October 2010), paras. 86–89, available at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-97575 (accessed on 1 November 2020).

[90] *Al-Skeini and Others v. the United Kingdom*, Judgment (Grand Chamber), 7 July 2011, paras. 138–140, available at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105606 (accessed on 1 November 2020); ECtHR (Grand Chamber), *Jaloud v. The Netherlands*, Judgment, 20 November 2014, available at: http://hudoc.echr.coe.int/eng?i=001-148367 (accessed on 1 November 2020).

[91] Art. 1 of the EConvHR.

[92] Milanovic M., *Op. cit*., p. 129.

[93] ECtHR, *Weber and Saravia v. Germany*. Application no. 54934/00. Decision on Admissibility of 29 June 2006, available at: http:// hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-76586 (accessed on 1 November 2020).

[94] ECtHR, *Liberty and Others v. the United Kingdom*, App. no. 58243/00, Judgment of 1 July 2008, available at: http://hudoc.echr.coe.int/fre?i=001-87207 (accessed on 1 November 2020).

[95] ECtHR, *Big Brother Watch and Others v. The United Kingdom*, Applications Nos. 58170/13, 62322/14 and 24960/15, Judgment (Merits and Just Satisfaction), 13 September 2018, available at: http://hudoc.echr.coe.int/eng?i=001-186048 (accessed on 1 November 2020).

[96] ECtHR, *Centrum för Rättvisa v. Sweden*, Application No 35252/08, Merits and Just Satisfaction, 19 June 2018, para 112, available at: http://hudoc.echr.coe.int/eng?i=001-183863 (accessed on 1 November 2020). See also Lubin A., Legitimizing Foreign Mass Surveillance in the European Court of Human Rights, *Just Security*, 2 August 2018, available at: https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/ (accessed on 1 November 2020).

[97] *Big Brother Watch and Others v. The United Kingdom*, para. 314.

[98] *Id*.

regulation of the mass interception of data.[99] Whilst judgments on the *Centrum för Rättvisa* and the *Big Brother Watch* cases were pending before the ECtHR Grand Chamber, on 6 October 2020 the Grand Chamber of the Court of the European Union delivered two Judgments on the requests for preliminary rulings in cases of the *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* and the *La Quadrature du Net and Others v. Premier Ministre and Others*, where it found general and indiscriminate retention and transmission of traffic data by providers of electronic communications services to a state authority to violate the EU law.[100] However, depending on the judgment of the ECtHR Grand Chamber, the enhanced level of international protection of privacy can remain applicable only for 27 states-members of the EU.

Against the backdrop of the problematic application of the *lex lata* non-cyber specific provisions, law making path to concretize how international law applies to cyberspace does not currently play a significant role. First, the overwhelming majority of states, at the moment, prefer not to create any new legally binding instruments.[101] Explicitly articulated grounds for this include references to the sufficiency of the current 'strategic framework' for regulation of cyber sphere[102] or to the danger that the creation of new legally binding instruments will undermine or create uncertainty in respect to existing ones,[103] a lack of state practice[104] or consensus among states[105] or the lengthy character of international law making, which contrasts with the speed of technological developments.[106] Only a minority of states preferred law making,[107] some of them did so with a reservation that they consider the development of new binding norms as a medium to long-term objective.[108]

Secondly, standard-setting, which is a mainstream track at this stage, should consider the content of the standards endorsed by the UN General Assembly. Neither the initial (11 non-binding norms of responsible state behavior)[109] nor extended (14 norms)[110] versions brought any 'added

---

[99] At the request of the applicants, the judgments on the *Centrum för Rättvisa* and *Big Brother Watch* have been referred to the Grand Chamber, available at: https://hudoc.ECHR.coe.int/eng-press#{"itemid":["003-6321717-8260093"]} (accessed on 1 November 2020).

[100] Court of the European Union (the Grand Chamber), *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, Request for a preliminary ruling from the Investigatory Powers Tribunal – London*, Judgment, 6 October 2020, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=14724754 (accessed on 1 November 2020); Court of the European Union (the Grand Chamber), *La Quadrature du Net and Others v. Premier ministre and Others, Requests for a preliminary ruling from the Conseil d'État (Council of State, France) and from the Cour constitutionnelle (Constitutional Court, Belgium)*, Judgment, 6 October 2020, available at: http://curia.europa.eu/juris/document/document.jsf?docid=232084&doclang=en (accessed on 1 November 2020).

[101] See: Delerue F., Reinterpretation or Contestation of International Law in Cyberspace? *Israel Law Review*, 2019, Vol. 52, No. 3, p. 315-316.

[102] EU statement; Portugal joined (OEWG, first session, 9 and 10 September 2019).

[103] Bulgaria; Italy (OEWG, first session, 9 September 2019).

[104] Israel (OEWG, first session, 11 September 2019).

[105] The UK (OEWG, first session, 12 September 2019).

[106] The USA (OEWG, first session, 12 September 2019); Singapur, UK, Australia (OEWG, second session, 11 February 2020).

[107] A necessity of law making was expressed by the Algeria, CARICOM group, Nigeria, Russia and the Syrian Arab Republic (OEWG, first session, 9-11 September 2019).

[108] South Africa and Chile (OEWG, first session, 9 and 12 September 2019); Brazil (OEWG, second session, 12 February 2020).

[109] The GGE Report of 2015 contains 11 'norms, rules and principles for the responsible behaviour of states', which were endorsed by consensus by the UN General Assembly (UN GA resolution 70/237 Developments in the field of information and telecommunications in the context of international security, 23 December 2015, para. 2 (a)) and their content was almost not disputed at the substantial meetings of the OEWG in 2019-2020.

[110] The UN General Assembly in the Resolution on creation of the OEWG in 2018 added three new norms to the existing list and altered few aspects in the GGE formulations. However, it was adopted by vote, not by consensus, with 119 votes in favour, 46 – against and 14 abstentions. UN General Assembly in the Resolution 73/27 on creation of the OEWG. The UN General Assembly Resolution 73/27 of 5 December 2018, available at: https://www.un.org/press/en/2018/ga12099.doc.htm (accessed on 1 November 2020).

value' to the qualification of malicious cyber acts compared with existing rules.[111] This standard-setting track may be important and justified as a political instrument to reaffirm the applicability of international law to cyber specific inter-state relations, but by its substance, it is legally tautological in the sense that it does not change anything in the assessment of the legality of inter-state cyber operations. Standards that may be relevant for setting the boundaries of outlawed cyber activities are constrained by the reference to *lex lata* international law and, as a general safeguard, these 'norms do not seek to limit or prohibit action that is otherwise consistent with international law'.[112]

Thirdly, in interstate relations, states suffering from cyber attacks tend not to use the language of international law even in situations which could have been qualified as a breach of its rules. States employ either political rhetoric, calling them a 'cyberwar',[113] 'cyber attacks with a significant effect which constitute an external threat to the [European] Union or its Member States'[114] or by mentioning international law in general terms—terms that are far from being a concrete legal qualification, e.g., designating them as a 'flagrant disregard of international law'[115] or 'international norms';[116] or pointing out that they undermine 'established international norms of behavior'.[117] The example of Georgia, which designated the cyber attacks of 2019 as a infringing on its sovereignty,[118] can be regarded as an exception to the rule.

B. The Attribution of Cyber Operations to States: a Cautious Mode

Although the applicability of the secondary rules of international law on the responsibility of states for cyber operations does not meet principal objections from states, the challenge lies in the necessity to attribute malicious cyber acts committed by individuals to a particular state under international customary rules, which also goes in conjunction with a duty to reach any of the standards of proof applicable in international law.[119] Taking into account the specificity of cyber infrastructure,[120] it might be of no surprise that states hastened to safeguard that 'states should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences' at least as a non-binding 'norm of responsible State behavior'.[121]

---

[111] Against this background it is revealing that during the OEWG sessions only Egypt explicitly suggested transforming the recommendations of the GGE to legally binging, and Philippines expressed concern about non-binding character of their nature and reduced options for compliance and enforcement.

[112] GGE Report of 2015, para. 10.

[113] The Segodnya, *Poroshenko: Russia Unleashed Cyber War against Ukraine* (Poroshenko: Rossiya razvyazala kibervoynu protiv Ukrainy), 29 December 2016, available at: https://politics.segodnya.ua/politics/poroshenko-rossiya-razvyazala-kibervoynu-protiv-ukrainy-784445.html (accessed on 1 November 2020).

[114] EU Regulation of 22 October 2020.

[115] UK National Cyber Security Centre, press release *UK exposes Russian cyber attacks*, 4 October 2018, available at: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks (accessed on 1 November 2020).

[116] Press Statement of John Kerry, Secretary of State, 'Condemning Cyber-Attack by North Korea', 19 December 2014, available at: https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm (accessed on 1 November 2020).

[117] The White House, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, 29 December 2016, available at: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity (accessed on 1 November 2020).

[118] Statement of the Ministry of Foreign Affairs of Georgia, 20 February 2020, available at: https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5 (accessed on 1 November 2020).

[119] See Roscini M., Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, *Texas International Law Journal*, 2015, vol. 50, No. 2, pp. 248-254.

[120] See Chircop L., A Due Diligence Standard of Attribution in Cyberspace, *International and Comparative Law Quarterly*, 2018, Vol. 67, Issue 3, p. 645-648; Henriksen A. Lawful State Responses to Low-Level Cyber-Attacks, *Nordic Journal of International Law*, 2015, Vol. 84, p. 340-342.

[121] GGE Report of 2015, para. 13(b), endorsed by the General Assembly (Resolution of the General Assembly 70/237, Developments in the field of information and telecommunications in the context of international security, 23 December 2015).

After the publicly articulated, although later disavowed, allegations of Russian involvement in the Estonian cyber attacks of 2007,[122] it was only in 2014 that states started to officially link malicious cyber acts with agencies or officials of particular states and these allegations have recently become more frequent. These official statements or acts imposing sanctions pointed at three states: North Korea,[123] Russia[124] and Iran.[125] Although the EU also imposed sanctions against Chinese nationals for 'Operation Cloud Hopper' in 2020, it did not officially link them to the state.[126]

Until now no state has ever officially called another state responsible for an international cyber operation. The approach taken by states in respect of the attribution of cyber operations is usually formulated very cautiously. Let us take an example of the recent condemnation of cyber attacks, allegedly committed by Russia against Georgia. Both Georgia and the UK framed their statement as exposing the author of the attacks and as a condemnation of this behavior without using the language of the law of international responsibility.[127] Although the US and Canada called

---

[122] The New York Times, *Estonian Links Moscow to Internet Attack*, 18 May 2007, available at: https://www.nytimes.com/2007/05/18/world/europe/18estonia.html (accessed on 1 November 2020).

[123] North Korea was designated by the US as a state that organized the cyber attack at 'Sony Pictures' (Press Statement of John Kerry, 19 December 2014, *Op. cit*.) and by the UK, the US, Australia, Canada, New Zealand, and Japan as responsible for the WannaCry ransom ware (Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, 19 December 2017, available at: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ (accessed on 1 November 2020); US Department of the Treasury, press-release *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, 13 September 2019, available at: https://home.treasury.gov/index.php/news/press-releases/sm774 (accessed on 10 August 2020).

[124] Russian intelligence agencies or state officials were blamed for a number of attacks, including: the hacking against German Bundestag in 2015 (EU Regulation of 22 October 2020 and Press release *UK Enforces New Sanctions against Russia for Cyber Attack on German Parliament* of 22 October 2020, available at: https://www.gov.uk/government/news/uk-enforces-new-sanctions-against-russia-for-cyber-attack-on-german-parliament#:~:text=The%20UK%20has%20announced%20it,cyber%20attacks%20on%20Germany's%20Parliament (accessed on 24 October 2020)), meddling into the US Presidential elections in 2016 (Executive Order 13757, Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 28 December 2016, available at: https://www.govinfo.gov/app/details/CFR-2017-title3-vol1/CFR-2017-title3-vol1-eo13757/summary (accessed on 10 November 2020); US Department of the Treasury, press-release *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 US Elections and Malicious Cyber-Attacks*, 15 March 2018, available at: https://home.treasury.gov/news/press-releases/sm0312 (accessed on 10 August 2020)), Petya and NotPetya ransom wares (US Department of the Treasury, press-release *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 US Elections and Malicious Cyber-Attacks*, 15 March 2018, available at: https://home.treasury.gov/news/press-releases/sm0312 (accessed on 10 August 2020); US Department of the Treasury, press-release *Treasury Sanctions Russian Federal Security Service Enablers*, 11 June 2018, available at: https://home.treasury.gov/news/press-releases/sm0410 (accessed on 10 August 2020); EU Regulation of 30 July 2020. In addition to this, in October 2018 the UK National Cyber Security Centre officially claimed that a number of cyber actors widely known to have been conducting cyber attacks around the world are in fact the Russian Military Intelligence Service (the GRU): the 2017 BadRabbit ransom ware, hacking and release of the medical files of the WADA in 2016, attack against the Ukrainian financial, energy and government sectors in 2017, an attempt to gain access to the UK defence and science Technology laboratory computer systems in 2018 and spearphishing the UK Foreign and Commonwealth office, which happened the same year; the attack against OPCW in 2018 (the UK National Cyber Security Centre, press release, *Op.cit.*). In 2020 Georgia, the US and the UK have exposed that Russia (or, precisely, the GRU) is responsible for a number of significant cyber attacks against Georgia in October 2019 that disrupted operations of several thousand Georgian government and privately-run websites and interrupted the broadcast of at least two major television stations (Georgia: Statement of the Ministry of Foreign Affairs of Georgia, 20 February 2020, available at: https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5 (accessed on 1 November 2020); the US Secretary of State Michael R. Pompeo, press statement *The United States Condemns Russian Cyber Attack Against the Country of Georgia*, 20 February 2020, available at: https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/ (accessed on 1 November 2020); Press release *UK condemns Russia's GRU over Georgia cyber attacks*, 20 February 2020, available at: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (accessed on 1 November 2020).

[125] Kingdom of Saudi Arabia Ministry of Foreign Affairs stated that 'in October 2012, Iranian pirates affiliated with the Iranian Revolutionary Guards launched electronic attacks against oil and gas companies in Saudi Arabia and the Gulf' (Kingdom of Saudi Arabia Ministry of Foreign Affairs, The Kingdom's position on Iranian policy, 27 March 2016, para. 31, available at: https://www.mofa.gov.sa/KingdomForeignPolicy/KingdomPosition/Pages/17637623.aspx, accessed on 1 November 2020).

[126] EU Regulation of 30 July 2020.

[127] Statement of the Ministry of Foreign Affairs of Georgia, 20 February 2020, available at: https://mfa.gov.ge/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5 (accessed on 1 November 2020); Press

on Russia to cease such behavior, they did not legally qualify this behavior as a breach of international law.[128] The EU, joining the condemnation campaign, expressed its and its Member States' concern about the cyber attack, without saying a word on Russian involvement.[129]

The current trend of 'cautious attribution' is characterized by two main features. First, public exposure of the organizer of a malicious cyber act is not linked to a breach of a particular rule of international law. Secondly, these acts are not accompanied by the disclosure of evidence meeting at least one of the standards that may be applicable under international law. For instance, whereas the National Cyber Security Centre relies on the assessment 'with high confidence' that GRU was 'almost certainly responsible', which is '95%+' for a list of cyber operations,[130] this evidence remained undisclosed.[131] Thus, 'cautious attribution' is only a 'name and shame' mode and does not represent an attribution for the purposes of calling a particular state responsible.

To sum up, the legal considerations outlined in this part of the paper expose the necessity for victim states to walk a line between the difficulties connected with the proof and legal qualification of cyber operations, on the one hand, and their desire to punish perpetrators and sponsors and deter further intrusions, on the other. Whilst the instruments provided by international law either cannot or can hardly be used, unilateral sanctions taking the form of retorsion remain one of the accessible instruments for victim states. Applying a national or supranational imposition of sanctions, states are not bound by the standards of proof and the duty to reveal evidence set forth by international law.[132] The scope of cyber acts triggering sanctions can be extended to operations which are not necessary linked to particular foreign states and lie below the threshold of behavior outlawed at the international level.[133] Finally, sanctions can be taken in respect of malicious cyber operations which did not necessarily affect the state-target, which significantly extends opportunities for a reaction in

---

release, *UK condemns Russia's GRU over Georgia cyber attacks*, 20 February 2020, available at: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (accessed on 1 November 2020).

[128] US Secretary of State Michael R. Pompeo, Press Statement *The United States Condemns Russian Cyber Attack Against the Country of Georgia*, available at: https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/ (accessed on 1 November 2020); Statement *Canada condemns Russia's malicious cyber-activity targeting Georgia*, 20 February 2020, available at: https://www.canada.ca/en/global-affairs/news/2020/02/canada-condemns-russias-malicious-cyber-activity-targeting-georgia.html (accessed on 1 November 2020).

[129] Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behavior in cyberspace, 21 February 2020, available at: https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/ (accessed on 1 November 2020).

[130] UK National Cyber Security Centre, press release *UK exposes Russian cyber attacks*, 4 October 2018, available at: https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks (accessed on 1 November 2020); or Press release *UK condemns Russia's GRU over Georgia cyber attacks*, 20 February 2020, available at: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (accessed on 1 November 2020).

[131] Ministry for Foreign Affairs of the Russian Federations, *Comment by the Information and Press Department on accusations against Russia of carrying out large-scale cyberattacks on Georgian websites*, 20 February 2020, available at: https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4050783 (accessed on 1 November 2020).

[132] EU Regulation of 17 May 2019 requires to 'give grounds' for listing in the sanctions list (Art. 14), but neither identify the standard of proof, nor require to disclose the evidence; the burden of proof is placed on the sanctioned person or entity, which can present 'observations' *post factum*; should the Council find that it contain new evidence, the decision can be reviewed (Council Regulation 2019/796 concerning restrictive measures against cyber attacks threatening the Union or its Member States, 17 May 2019, Art. 14, Art. 13 (1-3), O.J. L 129I, 17.5.2019, p. 1–12, available at: http://data.europa.eu/eli/reg/2019/796/oj (accessed on 15 October 2020) (hereinafter*: EU Regulation of 17 May 2019*)). The (US) Countering America's Adversaries Through Sanctions Act does not mention any such standard or duty in respect of the cyber-related sanctions at all (Countering America's Adversaries Through Sanctions Act, 2 August 2017 (Public Law 115-44), available at: https://www.congress.gov/115/plaws/publ44/PLAW-115publ44.pdf (accessed on 15 October 2020) (hereinafter*: CAATSA*).

[133] The cyber-related sanctions regime under CAATSA can be introduced for 'significant activities undermining cybersecurity against any person, including a democratic institution, or government…'; the scope of the EU regime according to the EU Regulation is narrower, but also goes beyond the acts outlawed by international law, extending to 'cyber attacks' that 'have (or potentially may have) a significant effect on the EU or its Member States, in particular to their critical infrastructure, public services (transportation, banking, healthcare, drinking water supply and others), critical state functions such as defence and governance' (CAATSA, Section 224(a)(1); EU Regulation of 17 May 2019, Art. 1(1),(3),(4)).

comparison with the *locus standi* under the law of international responsibility, providing for the right to react to not-injured states only in the case of a violation of obligations of an *erga omnes* or *erga omnes partes* character.[134]

II. The US and EU Counter-Cyber Sanction Regimes and their Implementation

The very first episode of cyber-related sanctions occurred in January 2015, when 10 individuals and three entities associated with the North Korean government were sanctioned by the US due to the Sony Pictures hacking attack under Executive Order 13687.[135] Three months later on 1 April 2015, President Obama issued Executive Order 13694, which declared a national emergency to deal with the 'unusual and extraordinary threat to the national security, foreign policy, and economy of the United States' constituted by the 'increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States'.[136] This act provided for blocking the property located in the US which belongs to persons engaged in or responsible for significant malicious cyber activities; the denial of access to the US financial markets; the prohibition to provide funds, goods or services to the sanctioned persons; and the denial of entry to the US.[137] This Executive Order was amended in 2016 to impose sanctions for the meddling into the 2016 US presidential elections on two Russian intelligence services, four members thereof, and three companies.[138]

The US cyber-related sanction regime was further codified and supplemented by the Countering America's Adversaries Through Sanctions Act (CAATSA) of 2017.[139] CAATSA imposes new sanctions with respect to Iran, Russia and North Korea and provides for sanctions related to Russian 'activities undermining cybersecurity'.[140] The scope of sanctions contemplated by CAATSA is similar to those authorized in the Executive Orders, although the wording of these acts differs as CAATSA contains a more detailed description of possible sanctions. The Executive Order sanctions imposed by the Obama administration also remained in effect after CAATSA came into force.

The EU cyber-related sanctions[141] regime is based on a Council Decision[142] and the corresponding Council Regulation[143] (hereinafter: *EU Regulation of 17 May 2019*), which is an act

---

[134] See: Haataja S., Cyber Operations and Collective Countermeasures under International Law, *Journal of Conflict & Security Law*, 2020, p. 33-51.

[135] Executive Order 13687 (available at: https://home.treasury.gov/system/files/126/13687.pdf, accessed on 1 November 2020) which forms a part of comprehensive sanctions package against North Korea alongside with, *inter alia*, Executive Order 13722 of 15 March 2016 issued in relation to North Korean nuclear and missile programs (available at: https://home.treasury.gov/system/files/126/nk_eo_20160316.pdf, accessed on 1 November 2020). Executive Order 13722 was also employed to designate North Korean hacking groups with respect to WannaCry attack, although this Executive Order is comprised in the North Korea-related sanctions program (aimed at prevention of weapons of mass destruction proliferation) rather than the cyber-related sanction program.

[136] Executive Order 13694 of 1 April 2015, available at: https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m (accessed on 10 October 2020) (hereinafter: *Executive Order 13694*).

[137] Executive Order 13694, Sections 1-4.

[138] Executive Order 13757 of 28 December 2016, available at: https://home.treasury.gov/system/files/126/cyber2_eo.pdf (accessed on October 10, 2020) (hereinafter: *Executive Order 13757*).

[139] CAATSA.

[140] Alongside with the 'cyber-related' sanctions CAATSA contains provisions on the sanctions related to (1) crude oil projects, (2) financial institutions, (3) corruption, (4) human rights abuses, (5) evasion of sanctions, (6) transactions with Russian defense or intelligence sectors, (7) export pipelines, (8) privatization of state-owned assets by government officials, and (9) arms transfers to Syria.

[141] Although the EU legislation employs the term 'restrictive measures' but not 'sanctions', in their economic nature the former are identical to the latter; therefore, in this paper these terms are used as synonyms.

[142] Council Decision (CFSP) 2019/797 of 17 May 2019, concerning restrictive measures against cyber attacks threatening the Union or its Member States, art. 1(1), O.J. L 129I, 17.5.2019, p. 13–19, available at: http://data.europa.eu/eli/dec/2019/797/oj (accessed on 15 October 2020).

of a direct application to all Member States.[144] The designation and delisting of persons under sanctions is exercised by the Council[145] in order 'to ensure consistency with the process for establishing, amending and reviewing'[146] the annex where the sanctioned persons are named. The Council is to review the sanction list at least once a year.[147] Member States specify national authorities that are entitled to authorize, under certain conditions, the release of certain frozen funds and economic resources,[148] and exchange information related to the implementation of the Regulation with each other and the EU Commission.[149] Member States stipulate penalties for infringement of the EU Regulation of 17 May 2019 in such a manner that such penalties were 'effective, proportionate and dissuasive'.[150] The legal nature of these penalties can be administrative, civil or criminal, with a range of measures from fines to imprisonment.[151]

The adoption of the EU Regulation of 17 May 2019 was specifically promoted by the UK[152] and the Netherlands,[153] who were reported to have suffered from significant cyber-hacking. The introduction of the regulation expanded the sanctions toolkit available to the EU and constituted a move from the 'Cyber Diplomacy Toolbox' of 2017 to a legally binding instrument.[154] The measures that the EU can impose are restricted to the prevention of the entry of the sanctioned persons into territories of EU Member States and the freezing of assets.

The US and the EU cyber-related sanction regimes have a number of common features. They are based on the use of 'targeted', or 'smart', sanctions as opposed to 'comprehensive' sanctions, and are a response to external threats. Both regimes contain rather vague and broad definitions of cyber activities that trigger sanctions and of the criteria for assigning persons on whom sanctions should be imposed. However, the approach used in CAATSA, designating 'significant activities undermining cybersecurity against any person, including a democratic institution, or government…' or are 'owned or controlled by, or act or purport to act for or on behalf of, directly or indirectly' by such person[155] is wider than 'cyber attacks' under the EU Regulation of 17 May 2019 confining them to those that 'have (or potentially may have) a significant effect on the EU or its Member

---

[143] Council Regulation 2019/796 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States, O.J. L 129I, 17.5.2019, p. 1–12, available at: http://data.europa.eu/eli/reg/2019/796/oj (accessed on 15 October 2020).

[144] In accordance with Article 288, *Consolidated version of the Treaty on the Functioning of the European Union*, 26 October 2012, OJ L. 326/47-326/390; 26.10.2012, available at: https://www.refworld.org/docid/52303e8d4.html (accessed on 4 November 2020).

[145] EU Regulation of 17 May 2019, Article 13(1).

[146] *Ibid*, paragraph (4) of Preamble.

[147] *Ibid*, Article 13(4).

[148] *Ibid*, Articles 4(1), 5(1) and 6(1).

[149] *Ibid*, Article 12(1).

[150] *Ibid*, Article 15(1).

[151] Savage D., *EU Sanctions Enforcement* in *The Guide to Sanctions - First Edition*, available at: https://globalinvestigationsreview.com/benchmarking/the-guide-to-sanctions-first-edition/1230031/eu-sanctions-enforcement (accessed on 15 October 2020).

[152] On application of the EU sanction regime after Brexit see, e.g.: Moret E., Pothier F., Sanctions After Brexit, *Survival*, 2018, 60:2, pp. 179-200.

[153] See, e.g.: *Cyber Security Assessment Netherlands 2019*, available at: https://www.thehaguesecuritydelta.com/media/com_hsd/report/255/document/CSBN2019-EN-def-Web-01-tcm32-405804.pdf (accessed on 10 August 2020); or Cyberscoop, *Dutch intelligence warns of escalating Russian, Chinese cyberattacks in the Netherlands*, dated 1 May 2019, available at: https://www.cyberscoop.com/dutch-intelligence-warns-escalating-russian-chinese-cyberattacks-netherlands/ (accessed on 10 August 2020). With respect to the UK see, e.g.: *Cyber Security Breaches Survey 2019*, available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019 (accessed on 10 August 2020); or BBC, *More than half of British firms 'report cyber attacks in 2019'* dated 23 April 2019, available at: https://www.bbc.com/news/business-48017943 (accessed on 10 August 2020); BBC, *Russia Cyber-Plots: US, UK and Netherlands Allege Hacking* dated 4 October 2018, available at: https://www.bbc.com/news/world-europe-45746837 (accessed on 15 October 2020).

[154] Moret E., Pawlak P., European Union Institute for Security Studies, Brief, *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?*, p. 1 (12 July 2017), available at: https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime (accessed on 15 October 2020).

[155] CAATSA, Section 224(a)(1).

States, in particular to their critical infrastructure, public services (transportation, banking, healthcare, drinking water supply and others), critical state functions such as defense and governance'.[156] What differs remarkably is the imposition procedure of the US and EU cyber-related sanctions. The US sanctions can be enabled by the stroke of a pen of the US President under CAATSA, and the designation of persons sanctioned under Executive Orders falls into the competence of the Secretary of the Treasury. In the EU, listing and delisting of persons and entities lies within the exclusive jurisdiction of the Council, which should act on the basis of unanimity.[157] The requirement of unanimity seems to be the main reason why decisions to impose cyber-related sanctions have been taken only twice so far—the objection of particular Member States to imposition of sanctions, considering their political significance, is often motivated by economic ties with the state from which malicious cyber-enabled actions allegedly originate.

The timeline of sanctions following alleged inter-state cyber operations contains 12 episodes. It starts with a sanctioning by the US of North Korean entities and individuals due to the cyber attack on Sony Pictures in January 2015,[158] and concludes with the US sanctions imposed against the Russian research centre 'Central Scientific Research Institute of Chemistry and Mechanics' in October 2020 as a reaction to a cyber attack using Triton malware.[159] Certain limitations should be noted. First, this study deals only with cases in which sanctions were actually imposed (threats to implement sanctions remained outside this research). Second, we include cases when sanctions or a combination of sanctions and other means of response were implemented, i.e. cases of solely diplomatic reaction or criminal indictment without sanctions imposition were excluded. Finally, the dataset includes only the cases of alleged inter-state cyber attacks.

III. How to Measure the Effectiveness of Sanctions

Since January 2015, the US and later the EU have sanctioned almost 200 individuals and legal entities from North Korea, Russia, Nigeria, Iran and China for cyber-hacking. The scale of cyber threats (including presumably those emanating from these countries) has not diminished over the past five years. However, it would be premature to suggest that cyber-related sanctions are not effective as such, without having established how to measure their effectiveness. Sanctions, although having primarily economic content, have always been a political issue.[160] Realizing the danger of a biased approach to their assessment caused by the political beliefs of the researchers, we suggest looking at the effectiveness of cyber-related sanctions, namely their ability to reach the goals of their imposition, from four different approaches: Mancur Olson's theory of groups, Francesco Giumelli's comprehensive analytical framework for sanction assessment, cost-benefit analysis and game theory.

---

[156] EU Regulation of 17 May 2019, Article 1(1),(3),(4).

[157] Council Decision (CFSP) 2019/797 of 17 May 2019, concerning restrictive measures against cyber attacks threatening the Union or its Member States, art. 1(1), O.J. L 129I, 17.5.2019, p. 13–19, available at: http://data.europa.eu/eli/dec/2019/797/oj (accessed on 15 October 2020), Article 6(1).

[158] US Secretary of State John Kerry, press statement *Condemning Cyber-Attack by North Korea*, 19 December 2014, available at: https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm (accessed on 10 August 2020).

[159] US Department of the Treasury, press-release *Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware*, 23 October 2020, available at: https://home.treasury.gov/news/press-releases/sm1162 (accessed on 4 November 2020).

[160] See, e.g.: Chesterman S., Pouligny B., Are Sanctions Meant to Work? The Politics of Creating and Implementing Sanctions Through the United Nations, *Global Governance*, 2003, Vol. 9, No. 4, pp. 503-518; Kaempfer W.H., Lowenberg A.D., The Political Economy of Economic Sanctions, *Handbook of Defense Economics*, 2007, Vol. 2, pp. 868-911; Allen S.H., The Domestic Political Costs of Economic Sanctions, *Journal of Conflict Resolution*, 2008, Vol. 52 issue 6, pp. 916-944. A separate strand of the literature examines the target states' political regime and potential correlation between the type of the regime and effectiveness of sanctions against the target. See, e.g.: Escribà-Folch A., Wright J., *Foreign Pressure and the Politics of Autocratic Survival*, UK: Oxford University Press, 2015; Peksen D., Autocracies and Economic Sanctions: The Divergent Impact of Authoritarian Regime Type on Sanctions Success, *Defense and Peace Economics*, 2019, 30 (3), pp. 253-268.

A. Identifying the Goals of the Imposition of Cyber-Related Sanctions

Before proceeding to the evaluation of sanction effectiveness as a response to cyber operations, it is instructive to address the goals of sanctions. There are three generally acknowledged goals of sanctions: *coercion* (modifying the target's behavior), *constraint* (reducing the target's capacity to take discretionary actions), and *signalling* and/or *stigmatizing* (notifying the target and in some cases third parties of the sender's intended course of action if the target continues the objectionable behavior).[161] The assessment of their effectiveness consists in the analysis of how they achieve the goal(s) intended by the sender.

Although coercion could be among the major reasons for the imposition of sanctions, travel restrictions of particular individuals or limitations on commercial relations with them cannot have a significant coercive impact on the states that are accused of orchestrating cyber operations. It is doubtful that North Korean citizens or Russian intelligence officers have substantial assets in the US or the EU or participate in commercial activities with the relevant counterparties. It is questionable, whether Russia, China, Iran or North Korea (even if we presume that these states actually stood behind the discussed cyber operations) would abstain from further acts of that nature because of targeted sanctions imposed on a number of individuals.

The goal of constraining the targets in their capacity to engage in further malicious cyber-enabled activities is also unlikely to be the principal motive of applying sanctions. None of the analyzed episodes of sanctions contemplates the seizure of computers or server systems for obvious reasons—in case of external cyber attacks, they can be located on the territory of a third party state or their location might not be established at all. Another aspect of constraining—the limitation of sources of financing by denying access to the US capital markets and financial institutions—also has a limited impact. North Korean hacking groups or Russian security services are unlikely to use sources of funding from abroad (in particular, due to restrictions in national legislation). The denial of access to foreign capital, therefore, would not raise the costs of the targets' activities in cyberspace.

The sanctions associated with cyber operations send certain signals to the targeted actors and the states of their residency, and to third parties. The signals can differ: from 'naming and shaming' to the articulation of a principal position on the inviolability of international norms in cyberspace. The rhetoric around sanctions also enhances the significance of the signaling and stigmatizing role of the sanctions. As an example, the imposition of sanctions on the Russian intelligence agencies GRU and FSB, and a number of their officers and affiliated companies, was accompanied by evaluative, often quite harsh, statements at different levels. The republican senators John McCain and Lindsey Graham in their joint statement said: 'Ultimately, [the sanctions] are a small price for Russia to pay for its brazen attack on American democracy',[162] while the then President Obama pointed out that '[t]he United States and friends and allies around the world must work together to oppose Russia's efforts to undermine established international norms of behavior, and interfere with democratic governance.'[163]

The coercive and constraining effects of cyber-related sanctions are limited which does not mean by itself that the policy of sanctions in response to cyber attacks is a failure. Neither does the primary signaling role make sanctions a symbolic gesture. It is essential, however, that the assessment of sanction effectiveness is conducted with a consideration of their goals. Research

---

[161] Dreyer I., Luengo-Cabrera J., Introduction to *On target? EU Sanctions as Security Policy Tools*, EU Institute for Security Studies. Reports, No. 25, p. 13, available at: https://doi.org/10.2815/710375 (accessed on 10 August 2020).

[162] The Guardian, *Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking*, available at: https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack (accessed on 10 August 2020).

[163] Euronews, *Obama Expels 35 Russian Diplomats, Accuses Russia of Meddling in Election*, available at: https://www.euronews.com/2016/12/29/washington-gives-35-russian-diplomats-72-hours-to-leave-the-us-in-response-to (accessed on 10 August 2020).

carried out by the Targeted Sanctions Consortium (TSC) headed by Prof. Thomas Biersteker with respect to general (not cyber-related) sanctions indicates that 'sanctions intended to constrain or to signal targets are nearly three times as effective (27%) as sanctions intended to coerce a change in behavior (10%).'[164] In the absence of statistically significant data on cyber-related sanctions it does not seem possible to conduct a similar calculation in relation to them. Still, as the studies on general sanctions show, the significance of the goals of the sanctions should not be underestimated.

B. Mancur Olson's Theory of Groups

Mancur Olson's theory of collective action and group behavior can be used in the context of cyber-sanctions. Among 12 cases of cyber-related sanctions, there is a special group of US sanctions imposed not against perpetrators, legal entities or institutions, but an elite group. Following adoption of CAATSA in August 2017, the US Congress instructed the Trump administration to prepare and deliver a list of Russia's 'most significant senior foreign political figures and oligarchs […] as determined by their closeness to the Russian regime and their net worth' with an obligatory 'assessment of the relationship between individuals' and 'President Vladimir Putin or other members of the Russian ruling elite', and the measurement of their corruption.[165] The list was intended to become the basis for a new package of sanctions against Russia for alleged election meddling and interference in Ukraine's internal affairs. As a result of the administration efforts, the notorious 'Kremlin Report' was released in January 2018. It included the names of the top officials of the Russian government and the presidential administration (almost all top officials except for the President himself) and 96 billionaires on the Forbes list. The imposition of sanctions against the entire political and economic elite of Russia was neither possible nor reasonable, and sanctioning under the 'Kremlin Report' remained an idle threat until April 2018 when sanctions were imposed against six Russian oligarchs 'with ties to Putin as well as to the Russian government'.[166] The sanctioning was accompanied with harsh rhetoric. 'The Russian government operates for the disproportionate benefit of oligarchs and government elites,' said in March 2018 the US treasury secretary, Steven Mnuchin, 'Russian oligarchs and elites who profit from this corrupt system will no longer be insulated from the consequences of their government's destabilizing activities.'[167] It was openly admitted that the sanctions aimed to reach President Putin's inner circle. 'Today's sanctions send a clear message to Putin and his cronies that there will be a high price to pay for Russia's […] attempts to undermine Western democracies, including our own,' McCain said.[168]

The upper echelons of the targeted state's political elite could be viewed in line with the theory of Mancur Olson as a small group with a properly defined stimulus system punishing those deviating from group profit-maximizing behavior.[169] Participants of a small group have common interests, economic and social incentives, and each of them is aware of this commonality of interests and of the degree of their contribution towards their achievement. When the number of

---

[164] Biersteker T., van Bergeijk P., How and When Do Sanctions Work? The Evidence in Dreyer I., Luengo-Cabrera J. (Eds.), *On Target? EU Sanctions as Security Policy Tools*. EU Institute for Security Studies. Reports, No. 25, p. 19, available at: https://doi.org/10.2815/710375 (accessed on 10 August 2020).

[165] The Atlantic, *How Not to Design Russia Sanctions*, 31 January 2018, available at: https://www.theatlantic.com/international/archive/2018/01/kremlin-report-sanctions-policy/551921/ (accessed on 10 August 2020).

[166] Reuters, *US Plans to Sanction Russian Oligarchs This Week: Sources*, 5 April 2018, available at: https://www.reuters.com/article/us-usa-russia-sanctions/u-s-plans-to-sanction-russian-oligarchs-this-week-sources-idUSKCN1HB34U (accessed on 10 August 2020).

[167] The Guardian, *Trump Administration Hits 24 Russians with Sanctions over 'Malign Activity'*, available at: https://www.theguardian.com/us-news/2018/apr/06/trump-russia-sanctions-election-meddling-latest (accessed on 10 August 2020).

[168] *Ibid*.

[169] See Olson M., *The Logic of Collective Action: Public Goods and the Theory of Groups*, Harvard University Press, 1971, p. 29: 'Where small groups with common interests are concerned, then, there is a systematic tendency for "exploitation" of the great by the small'. Economic incentives, as well as higher degree of consensus in a small (or 'privileged') group enable its member to expect that their collective needs will be met one way or another (Olson M., *Op. cit*, p. 58).

participants is large, and the group obtains the features of a latent group, its typical participant recognizes that she cannot make a noticeable contribution to any group effort or anyhow influence the outcome.[170] Consequently, she has little incentive to contribute (which constitutes the 'free rider' problem). On the contrary, there is no free rider problem in small and well-organized groups where the members, at less cost, can observe whether any individual contributes or deviates and put sanctions on the deviating party. It is empirically proven that in a variety of constituencies, either private or public, including national states, 'action taking' groups and subgroups tend to be much smaller than 'non-action taking' groups and subgroups.[171] These well-organized action-taking groups and subgroups have a significant advantage over the poorly organized, latent masses and have a better negotiating position.

The economic sanctions with respect to the key businesspeople of Russia can be viewed in light of Olson's theory as an attempt of the US administration to use financial leverage against Russian political and business elites to alter their incentives in the communication with the Russian government. Based on the belief that sanctioned persons have 'ties' with the government and personally with the president, the US sanctions aim to influence the decision-making process in the Russian upper echelons through economic pressure on persons close to those echelons. There are publicly available calculations of the economic impact of sanctions on the targeted persons' business and wealth. The losses of Oleg Deripaska, a major shareholder of United Co RUSAL PLC (Rusal), one of the world's largest aluminum producers, are calculated by Forbes as $3.1 billion,[172] while Deripaska himself indicated losses in the amount more than $7.5 billion, or approximately 81% of his net wealth, in the lawsuit against the US Department of Treasury.[173] That said, the assessment of sanction effectiveness should not be narrowed down to numbers. The question is to what extent the circle of businesspeople that have come under the sanctions actually represents a part of the 'action taking' subgroup and influences the decision-making process.

C. Francesco Giumelli's Four-Step Analysis

The four-step process of sanction impact evaluation designed by Francesco Giumelli[174] represents a comprehensive analytical framework suitable for the assessment of cyber-related sanctions.[175] Understanding the logic of sanctions is at the heart of Giumelli's approach. Considering the potential goals of sanction implementation (coercion, constraint and signaling, as discussed above), the assessment of sanctions' success is built on the determination of whether imposing sanctions adds value to the sender in these three dimensions.

The first step of the analysis is to identify the position of sanctions in the sender's overall foreign policy context.[176] As sanctions are implemented alongside other political tools, the objective

---

[170] Olson M. *Op. cit.*, p. 50.

[171] *Ibid*, p. 53.

[172] Forbes, '*For Me, This Is a Total Crisis': Vekselberg Told how his Life Changed due to US Sanctions* ("Dlya menya eto total'nyy krizis": Veksel'berg rasskazal, kak yego zhizn' izmenilas' iz-za sanktsiy SSHA), 3 June 2019, available at: https://www.forbes.ru/milliardery/377121-dlya-menya-eto-totalnyy-krizis-vekselberg-rasskazal-kak-ego-zhizn-izmenilas-iz-za?photo=1 (accessed on 10 August 2020).

[173] The lawsuit is available at: https://www.courtlistener.com/recap/gov.uscourts.dcd.205241/gov.uscourts.dcd.205241.1.0.pdf (accessed on 10 August 2020).

[174] See Giumelli F., *The Success of Sanctions: Lessons Learned from the EU Experience*. London: Taylor & Francis Group, 2013.

[175] The methodological approach of Francesco Giumelli has been employed in a series of recent studies on sanctions' effectiveness, see, e.g.: Jones L., *Societies Under Siege: Exploring how International Economic Sanctions (do Not) Work*, Oxford University Press, 2015; Veebel V., Markus R., Lessons from the EU-Russia Sanctions 2014-2015, *Baltic Journal of Law & Politics*, 2015, 8(1), pp. 165-194. An instructive report of 2015 prepared by the Task Force on sanctions within the EU Institute for Security Studies was built 'on the framework presented by Francesco Giumelli' to adopt 'a "new narrative" on how sanctions effectiveness can be conceptualized' (*On Target? EU Sanctions as Security Policy Tools*. EU Institute for Security Studies. Reports, No. 25, p. 12, available at: https://doi.org/10.2815/710375 (accessed on 1 November 2020).

[176] Giumelli F., *Op. cit*., p. 7.

of the first step is to determine their relative significance in the entire foreign policy of the sender. The study of episodes of cyber-related restrictive measures shows that sanctions are integrated into the overall political response. In the episode related to the meddling in the US 2016 presidential elections, the US alongside implementing sanctions also designated 35 Russian intelligence operatives located in the Russian embassy in Washington and the consulate in San Francisco as *personae non gratae* and ordered them to leave the country within 72 hours; access to Russian compounds in New York and Maryland was denied as they were claimed to be used 'for intelligence-related purposes'.[177] When sanctions are considered in the overall context of the sender's reaction to cyber-enabled actions, it creates obstacles to separating the effect caused by sanctions and to evaluating their contribution to the achievement of the sender's objectives.

The second step is to educe the logic of sanctions.[178] Two indicators of *ex-ante* analysis are taken into consideration: the expected direct impact of the sanctions and the feasibility of demands. If the sender's goal is to impose material costs on the target (e.g., to make any line of behavior that differs from the line required by the sender too costly for the target), then coercive and constraining sanctions would be more efficient than signaling ones. Otherwise, if the sender does not expect to have material impact on the sender, signaling sanctions are the choice. Travel bans, one of the two common restrictive cyber-related measures in the US and EU regimes, do not entail any significant material costs on the targets. Asset freezes might have material impacts if the sanctioned persons actually possess assets or economic resources under the jurisdiction of the sender (which is presumably not the case of most cyber-related sanctions applied to date, except for the sanctions against six Russian oligarchs). The constraint of business operations between the sanctioned persons and US residents might entail either direct costs for the targets (e.g., when they had effective commercial contracts at the time of sanction imposition) and indirect costs, i.e. the loss of expected profits, but again, this is rarely relevant for the known episodes of sanctioning in response to cyber-hacking. The second factor, the feasibility of demands, indicates the possibility of the target's compliance with the sender's demands. The feasibility of demands in Giumelli's concept appears to be a distinctive feature of coercive sanctions as opposed to constraining: imposing coercive measures means that the target has freedom to decide whether to comply with the sender's demands, and 'this voluntary decision that does not affect their [targets'] political existence.'[179] When sanctions are imposed in the constraining logic, the targets generally do not have this freedom of choice—they have to change their behavior as prescribed by the sender. In case of the cyber-related sanctions, the feasibility of demands seems to be a secondary factor of the *ex-ante* analysis as cyber-related sanctions tend to be mostly signaling and stigmatizing rather than coercive or constraining.

The third step of the analysis is an *ex-post* estimation of the sanctions' impact and effects,[180] the assessment of the sanctions factual consequences—intended or not. This evaluation often includes a cost-benefit analysis, which will be discussed in more detail in section D, but should not be limited to it. Although sanctions can have a calculable material impact, the assessment of their effectiveness should also include an analysis of effects other than economic costs, first of all the political consequences of sanctions. Thus, President Trump, who openly opposed the adoption of CAATSA, argued that the US Congress was making a mistake introducing new sanctions against Russia. 'Our relationship with Russia is at an all-time & very dangerous low', he wrote on

[177] BBC news, *US Expels Russian Diplomats over Cyber Attack Allegations*, 29 December 2016, available at: https://www.bbc.com/news/world-us-canada-38463025 (accessed on 10 August 2020).

[178] Giumelli F. *Op cit*., p. 7.

[179] Giumelli F. *Op cit*., p. 8.

[180] *Ibid*.

Twitter.[181] The Russian leader also spoke strongly on the preparation of new sanctions under CAATSA. 'What we are seeing is just growing anti-Russian hysteria, more likely this is the use of anti-Russian instruments in domestic political fight—of President Trump and his political rivals inside the United States,' Putin said.[182] 'As you know, we are behaving very composedly and patiently but we will have to respond at a certain point. It is impossible to constantly tolerate loutish behavior towards our country,' he added.[183] The authoritative Carnegie Endowment for International Peace estimates US-Russian relations are 'at the lowest point since the Cold War' with no 'signs that the relationship will improve in the near future'.[184] The US sanction policy, in particular the episode related to Russia's alleged meddling in 2016 presidential elections, has undoubtedly contributed to growing tension in relations between the two states.

Finally, the fourth step is to consider possible alternative tools to sanctions taking into account the specifics of the situation in which they have been applied.[185] This analysis estimates whether sanctions were the sender's best choice in the particular circumstances. It seeks to understand whether 'sanctions bring about effects that could not have been caused by other foreign policy tools and at a minor cost'.[186] The imposition of cyber-related sanctions, as discussed further in section D, can be associated with certain costs for the sender (both, in a strictly economic sense, meaning losses incurred by the sender, and in political sense, that is weakening of power positions and/or the increase of political risks). Still, sanctions remain a readily accessible instrument, however the widespread practice of imposing sanctions can limit the further use of this measure: according to the US National Security Advisor Robert O'Brien, the US has imposed so many sanctions against Russia and Iran that is has little opportunity left to impose new sanctions and has to look at other possible deterrents.[187]

The analytical framework developed by Giumelli represents a nuanced approach to the assessment of sanction effectiveness in comparison with the mainstream assessment. Although changing the target's behavior can be among the sender's objectives, but it is not the only one. An estimation of the sanctions' impact through the lens of their goal(s) might provide a clearer understanding of the position of sanctions amid other foreign policy tools and their relative, as opposed to absolute, impact.

D. Cost-Benefit Analysis

Designing, discussing, evaluating, implementing, monitoring, reflecting and correcting sanctions require a great deal of effort on the part of the sender, and coordinating that process is itself a challenge. The existence and amount of these costs in our real (non-Coase) world determines the fact that only significant trespassing and cyber-threats are punished, although the total burden of all threats is felt by society, so imposing sanctions for the most significant attacks may be attributed *de facto* to the number of attacks thus redistributing the costs for the most prominent violators or alleged violators. The estimation of the costs incurred by the sender and the benefits it gains due to sanctions can also be used to assess sanction efficiency. This approach

---

[181] Trump D.J. on Twitter, 3 August 2017, available at: https://twitter.com/realDonaldTrump/status/893083735633129472 (accessed on 10 August 2020).

[182] The Tass, *New US Anti-Russia Sanctions Way to Pursue Its Economic Interests with Cynicism — Putin*, 27 July 2017, available at: https://tass.com/politics/958037 (accessed on 10 August 2020).

[183] *Ibid*.

[184] Sokolsky R., Rumer E., *US-Russian Relations in 2030*, 15 June 2020. Available at: https://carnegieendowment.org/2020/06/15/u.s.-russian-relations-in-2030-pub-82056 (accessed on 10 August 2020).

[185] Giumelli F. *Op. cit*, p. 10.

[186] *Ibid*.

[187] TehranTimes, *Few New Sanctions Left to Impose on Iran, Russia: Robert O'Brien*, dated 26 October 2020, available at: https://www.tehrantimes.com/news/453901/Few-new-sanctions-left-to-impose-on-Iran-Russia-Robert-O-Brien (accessed on 1 November 2020).

evaluates the strengths and weaknesses of alternatives to determine which options provide the most benefits at the least cost. To put it simply, we should sum the benefits of sanctions and subtract the costs associated with their implementation.

Cost-benefit analysis is an economic assessment tool going back to welfare economics of the 19th century,[188] particularly to an 1848 article by Jules Dupuit, where he discusses the social profitability of a construction project from a mathematical standpoint.[189] Alfred Marshall further elaborated the concept. In his major work *Principles of Economics* first published in 1890,[190] he laid out the foundations of what is now called the cost-benefit analysis, particularly designing his famous scissors analysis comparing utility obtained and costs incurred. The application of cost-benefit analysis is required for assessment of a wide variety of regulatory practices and policy changes.[191]

The costs associated with the imposition of sanctions can be classified as direct costs and indirect costs. The first include costs incurred due to designing the proposed sanctions by in-house specialists or external professionals, the time legislators spend on discussing and adopting sanctions, the preparation of expert conclusions in parliamentary committees, securing infrastructure to introduce sanctions, wages for those monitoring their implementation and other related costs. Indirect costs refer to any losses occurring to the sender's national parties resulting from sanctions implementation (breaches or termination of contracts, loss of contractors, destroying production chains and losses from actual or expected retaliation by the sanctioned party).

The costs for the sender can be considerable and undermine both the economic rationale and the political willingness to impose sanctions. This appears to hold for comprehensive sanctions particularly. When the sanctions are wide-reaching, the *ex-ante* analysis of the costs that the sender is ready to incur and their correlation with the goals the sender intends to achieve is especially important prior to taking political decisions.

Estimations of costs that targets and senders suffer from vary (these refer mostly to comprehensive rather than smart sanctions, and present significantly different results). The western financial sanctions imposed on Russia in the Ukraine crisis were particularly subject to calculations. In November 2014, Anton Siluanov, the then Russia's Finance Minister, estimated Russia's annual losses because of geopolitical sanctions at around $40 billion; meanwhile, losses caused by falling oil prices reached as much as $90 billion to $100 billion per year.[192] The agri-food embargo introduced by Russia as a 'counter-sanction' and the decline in volume of Russian-European trade caused sufficient damages to the EU and the economies of some of its Member States: the estimation carried out by WIFO in 2016 indicates sanction-induced decline of EU exports to Russia in 2015 of about EUR 20 billion, or a 0.2 % loss in total value added (EUR 17.6 billion) and

[188] Pearce D.W., The Origins of Cost-Benefit Analysis. In: *Cost-Benefit Analysis. Studies in Economics*, London: Palgrave, 1983, p. 14.

[189] Detailed discussion can be found in Ekelund R. B. and Hebert R.F., Dupuit and Marginal Utility: Context of the Discovery, *History of Political Economy*, 1976, 8, pp. 266-73.

[190] Marshall A., *Principles of Economics*, Eighth Edition. London: Macmillan, 1920.

[191] For recent theoretical and empirical developments of this method refer, e.g. to the 2nd edition of classical *Cost-Benefit Analysis* by Pearce D. W. (Macmillan International Higher Education, 2016); and also Johansson P.-O., Kriström B., *Cost–Benefit Analysis*, Cambridge University Press, 2018. For a multifold scholarly debate on implications of cost-benefit analysis see, e.g.: Adler M.D., Posner E.A. (Eds.), *Cost-Benefit Analysis: Legal, Economic, and Philosophical Perspectives*, University of Chicago Press, 2001. See also the paper by Richard Allan Posner (Posner R.A., Cost-Benefit Analysis: Definition, Justification, and Comment on Conference Papers, *The Journal of Legal Studies*, 2000, Vol. 29, No. S2, pp. 1153-1177) for his reflections on application of cost-benefit analysis to antitrust law and risk regulation.

[192] Reuters, *Russia Puts Losses from Sanctions, Cheaper Oil at up to $140 Billion per Year*, 24 November 2014, available at: https://www.reuters.com/article/us-russia-siluanov/russia-puts-losses-from-sanctions-cheaper-oil-at-up-to-140-billion-per-year-idUSKCN0J80GC20141124 (accessed on 10 August 2020).

employment (400 000 jobs) for the EU as a whole.[193] Estimating the impact of the economic sanctions on the sender's and target's economies is challenging, as it requires distinguishing the sanction-induced economic costs from those caused by other factors (such as oil prices).

Similar difficulties are inherent to estimating the costs and benefits related to smart sanctions, and sanctions imposed in response to cyber operations in particular. The EU cyber-related sanctions introduced in July 2020 appear to be cost-effective instruments: considering that the sanctions target a limited number of Chinese and Russian individuals and legal entities and constitute asset freezes and travel bans, their imposition is hardly a material drain on the EU budget. Although the impact of the US cyber-related sanctions cannot be calculated to the accuracy of the dollar, the main clues to the application of a cost-benefit analysis can be illustrated as follows. Sanctioning Russian oligarchs in April 2018 related to accusations of Russian interference in the US presidential elections which had far-reaching implications for financial markets, affected the interests of investors around the world, including residents of the US and the EU, and a number of enterprises in the real sectors of the economy. An example is Rusal controlled by Oleg Deripaska. The shares of Rusal are listed on the Moscow and Hong Kong Stock Exchanges. Figure 1 shows the stock quotes of Rusal over a 5-year period. The chart portrays a dramatic drop in April 2018 when the sanctions were announced. The market closed with a 50.4% fall in the Rusal share price.

Fig. 1. United Co RUSAL PLC 5Y (August 2016 – August 2020) stock quotes, Hong Kong Stock Exchange (stock code: 486)

Source: https://www.bloomberg.com/quote/486:HK

[193] European Parliament, Directorate-general for external policies policy department. *Russia's and the EU's Sanctions: Economic and Trade Effects, Compliance and the Way Forward*, October 2017, document EP/EXPO/B/INTA/2017/11, P.40, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603847/EXPO_STU(2017)603847_EN.pdf (accessed on 10 August 2020).

Unsurprisingly, global depositary receipts of En+ Group, the company that was holding a 48% stake in Rusal (and was also controlled by Deripaska) underwent a similar drop in price on the London Stock Exchange amid news of the sanctions.

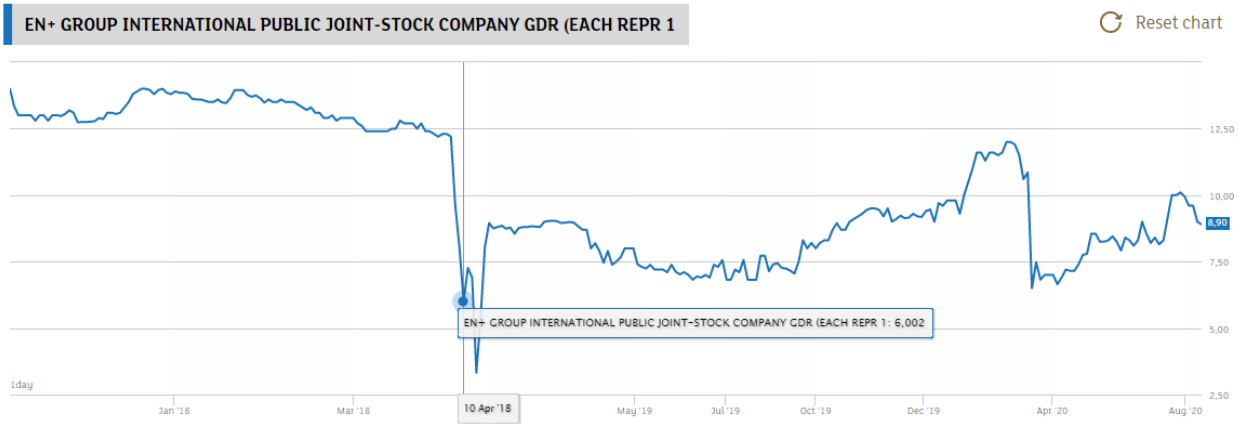

Fig. 2. En+ Group 5Y (August 2016 – August 2020) GDR quotes, London Stock Exchange (ticker: ENPL)

Source: https://www.londonstockexchange.com/stock/ENPL/en-group-international-public-joint-stock-company/company-page

Aluminum prices, meanwhile, soared. Benchmark aluminum on the London Metal Exchange hit its highest level gaining around 7% shortly after the sanctions were announced.[194] The sharp rise in aluminum prices resulted in contingent losses for companies on both sides of the Atlantic. Not only Rusal's US counterparties, but also legal entities registered in other jurisdictions and having ties with the US, for example, through shareholder control, were banned from doing business with Rusal. Thus, the sanctions caused losses not only for Rusal and its group companies, but also to many players in the non-ferrous metallurgy industry around the world, including national and foreign investors. According to the head of the American Chamber of Commerce in Russia, potential losses for German entities doing business with Rusal (especially automakers) could reach €10 billion, while the biggest losses were probably inflicted to the US aircraft industry which is highly dependent on aluminum supplies.[195] A managing director at TS Lombard, a global independent research and investment consulting firm, set forth in a note to clients: 'The new US sanctions against Russia are a negative game-changer for three reasons: they directly affect portfolio investments; they are de-linked from clear conditionality; and they will be applied "extra-territorially"'.[196] This is also true for companies affiliated with other persons on the sanctions list and their counterparties and investors. Although in-depth calculation of all losses caused to various actors by the imposition of sanctions against Russian oligarchs and their companies in the midst of accusations of Russian interference in the US elections is not the main purpose of this paper, the examples provided demonstrate the importance of the *ex-ante* calculation of costs and the potential circle of affected parties of the imposition of any restrictive measures.

The methodology of cost-benefit analysis requires the assessment of not only the sender's costs associated with sanctions' implementation, but also benefits received. When sanctions are imposed in the coercive logic, the key benefit for the sender is a change in the target's behavior in

[194] CNBC, *Russian Stocks Crash on New Sanctions; Aluminum Prices Soar on Penalties to Global Producer Rusal*, 9 April 2018, available at: https://www.cnbc.com/2018/04/09/russian-stocks-crash-on-new-sanctions-aluminum-prices-soar-on-penalties-to-global-producer-rusal.html (accessed on 10 August 2020).

[195] RT, *Anti-Russia Sanctions are Punishing the US Economy – AmCham President*, 7 May 2018, available at: https://www.rt.com/business/426018-us-sanctions-business-russia/ (accessed on 10 August 2020).

[196] CNBC, *Op. cit.*

line with the sender's demands (the target's 'costs', i.e. economic losses, are not necessary 'benefits' for the sender). In the case of constraining sanctions, the costs that the target incurs to carry on the opposed actions might be considered benefits for the sender. The example of sanctions against Russian individuals and their affiliate companies, however, raises concerns about whether the measures employed actually influence the behavior of Russia in cyberspace. The absence of any evidential signs of such an influential role of cyber-related sanctions inclines towards a conclusion of their predominantly signaling function.

E. Game Theory

Game theory is among the most interesting and promising assessments of sanctions effectiveness.

Game theory, according to the definition of Roger Myerson is the 'study of mathematical models of conflict and cooperation between intelligent rational decision-makers'.[197] Game-theoretical analysis has been widely addressed in the international relations literature and, more recently, in the literature of international law.[198] The tools of game theory are employed as a part of a beyond-positivistic approach to answering the question of why states obey international law.[199] Presuming that states are rational decision-makers allocating resources to maximize benefits, game theory provides various avenues for the analysis of sanctions as strategic interaction. Situations of strategic interaction between the players, or 'games', are divided in a number of classes.[200]

One of the classes that can be considered here is the class of zero-sum/non-zero-sum games. A zero-sum game is a mathematical representation of a situation in which each game player's gain or loss of utility is exactly balanced by the losses or gains of the utility of the other players. If the total gains of the players are added up and the total losses are subtracted, they will sum to zero. If we consider the interaction 'cyber attack-sanction' as a zero-sum game, it means that the gains of the state imposing sanctions amount to the losses of the state or entity with respect to which the sanctions are imposed. Most sanctions do not qualify as zero-sum games as the total distribution of wealth (or gains and losses) does not sum to zero. As illustrated by the example of sanctions against Rusal and En+ Group, both the sender and the target bear losses caused by implementation of restrictive measures. Game theory tells us that the sender, being a rational agent, still decides to impose cost-bearing sanctions because of its belief that the expected net benefits of sanctions exceed the net benefits from abstaining from sanctioning or applying another strategy.

The interaction 'cyber attack-sanction' can be qualified as a cooperative game. States as game players are bound, at least in theory, with commitments enforced under international law, including the principles of sovereignty and non-interference in the internal affairs of other states. As these

---

[197] Myerson R. B., *Game Theory: Analysis of Conflict*, Harvard University Press, 1991, p. 1. See also: Osborne M.J. *An Introduction to Game Theory*, Oxford University Press, 2009; Tadelis S., *Game Theory: An Introduction*, Princeton University Press, 2013; Lambertini L., *Game Theory in the Social Sciences: A Reader-friendly Guide*, Taylor & Francis, 2011.

[198] Ohlin J.D., Nash Equilibrium and International Law, *Cornell L. Rev*., 2011, Vol. 96, p. 869.

[199] Teson F. *A Philosophy of International Law*, Routledge, 2018, pp. 74-76. On application of game theory to international relations and international law see also: Chinen M. A., Game Theory and Customary International Law: A Response to Professors Goldsmith and Posner, *Michigan Journal of International Law*, 2001, 23, pp. 143-189; McAdams R.H., Beyond the Prisoners' Dilemma: Coordination, Game Theory, and Law, *Southern California Law Review*, 2009, Vol. 82, pp. 209-268; Konyukhovskiy P., Holodkova V., Application of Game Theory in the Analysis of Economic and Political Interaction at the International Level, *Contributions to Game Theory and Management*, 2017, 10, pp. 143–161; Rapoport A. International Relations and Game Theory, in: Foradori P., Giacomello G., Pascolini A. (Eds), *Arms Control and Disarmament*, Palgrave Macmillan, 2018.

[200] Analysis of cyber-related sanctions in the context of all applicable classes of games falls outside the scope of the present paper which aim is rather to present game theory as an appropriate methodological framework. For more detailed analysis of economic sanctions in the light of game theory, an interested reader may refer, e.g., to the book by Eyler R., *Economic Sanctions: International Policy and Political Economy at Work*, US: Palgrave Macmillan, 2008.

commitments can be enforced through outside parties, the game is deemed cooperative.[201] In non-cooperative games, although players can cooperate with each other, any cooperation must be self-enforcing.[202] Cooperative game theory contemplates forecasting coalitions that the players will form (in the case of sanctions, coalitions are possible with participation of both states and international organizations), their collective actions and group payoffs. In non-cooperative theory, a game is a detailed model of various moves available to the players, the analysis of individual payoffs and Nash equilibria.[203] In a cooperative game, players other than the original sender and the target can join the game at each decision stage, at their discretion, as 'white knights' in cooperation with the sender or 'black knights' on the side of the target.[204] In the episode of sanctions in response to the WannaCry attack the US initiated sanctions, and the EU joined later as a 'white knight'.

Although these examples of game theory application to sanctions analysis are quite simplistic, they demonstrate that the analysis of sanctions effectiveness should not be reduced to a calculation of loses caused to the target or consider successful only those sanctions that have led to an alteration of the target's behavior. Game theory provides insight as to why sanctions are initiated, continue or end, beyond the calculation of their direct and indirect costs and benefits.

IV. Concluding Remarks: Prospects of the Cyber-Related Sanctions

Starting with the application of a positivistic legal approach to the question of why states make use of the 'good old' tool of sanctions in response to a still relatively new threat of malicious cyber operations, we have demonstrated that states are pushed to resort to self-help and sanctions are one of its forms. States are pushed by the conundrum of problems surrounding the legal basis for the qualification of the initial malicious cyber operation as a breach of international law and, consequently, a possible appeal to the law of international responsibility in response to it. In contrast, national or supranational law on sanctions, like in the two examined cases of the US and the EU, provides the possibility to extend the scope of cyber activities for almost all types of cyber acts without looking back to the issues of the applicability, normativity and thresholds of non-cyber specific rules of international law in cyberspace. The use of sanctions helps to avoid the duty to disclose evidence and connect the perpetrators with a concrete state and provides freedom from the pressure of the standards of proof applicable in international law.

However, the 'comfort' of using this instrument to fight malicious cyber operations allegedly sponsored by other states, being below the threshold of international law, is not unlimited. The scope of measures, which may be used as a response, is restricted, because, once sanctions are themselves breaching the international legal obligations of the sending states, they may be legal only if they either meet all criteria set forth for countermeasures or fall under one of the defenses provided by the law of international responsibility. An abuse of sanctions, which can stream from each of its elements, including the scope of the malicious acts, the designation of the sanctions' targets, and the determination of the volume and length of the restrictions, may involve a spiral of sanctions and counter-sanctions, provided that they can be deployed with comparable speed and volume by the targeted state. Therefore, there is an incentive for the senders not to go too close to the 'red lines' set by international law or exploit its immanent indeterminacy. The increasing popularity of sanctions will, although as a byproduct, raise the inevitable question of the

---

[201] Shor M., *Non-Cooperative Game*, GameTheory.net. Retrieved 15 September 2016, available at: http://www.gametheory.net/dictionary/Non-CooperativeGame.html (accessed on 10 August 2020).

[202] *Ibid*.

[203] Brandenburger A., *Cooperative Game Theory: Characteristic Functions, Allocations, Marginal Contribution*, p.1, available at: https://web.archive.org/web/20160527184131if_/http://www.uib.cat/depart/deeweb/pdi/hdeelbm0/arxius_decisions_and_games/cooperative_game_theory-brandenburger.pdf (accessed on 10 August 2020).

[204] Eyler R., *Op. cit.*, p. 37.

permissibility of the cyber-sanctions, i.e. sanctions consisting in the use of cyber means, and this could motivate states to strive for normativity in cyberspace.[205]

The use of the extra-legal analytical tools in the assessment of the efficiency of cyber-related sanctions has revealed that although their use has not led to any visible changes in the number and intensity of malicious cyber acts, thus, proving its very limited capacity to coerce the target to modify their behavior or to constrain them by reducing their potential to conduct new operations, these restrictive measures are efficient in fulfilling the purpose of signaling the alleged organizer of the cyber operation and third parties of the sender's intended course of action, and stigmatization.

To reach these aims, states should take into consideration a number of general and cyber-specific factors. Among them, first of all, the risk that the economically designed sanctions may inflict economic costs to many states (not only to the sender and target states). Secondly, empirical studies on 'general' (not cyber-related) economic sanctions reveal that they lose much of their effectiveness after the first and second year, which accounts for 55% of successful sanction episodes[206] due to adjustment by the target to the restrictions caused by sanctions. As the process of adjustment and the reallocation of capital requires time, and as targeted states tend to adjust their economies under sanctions irrespective of the grounds for their implementation, the gradual decline of sanction damage is relevant for cyber-related sanctions. Thirdly, the effectiveness of sanctions is contingent on their credibility and consistency. That stresses the impact of due procedure, the sufficiency of evidence, legal certainty and the predictability of the imposition of sanctions, which is a crucial psychological factor.[207] Fourthly, the impact of cyber-related sanctions should be measured in conjunction with the other tools including different acts of reaction in the realm of the diplomacy, the initiation of the criminal cases against individual perpetrators, and political statements. The overall context of the sender's foreign policy and the stance of third party states ('black knights' and 'white knights') are also to be taken into consideration.

[205] Only two cases of hacking-back have been made public so far: in February 2019 the US military blocked Internet access to the 'Internet Research Agency', a Russian 'fabric of trolls', on the day of the 2018-midterm elections (US Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms, Ellen Nakashima, 27 February 2019, available at: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html, accessed on 1 November 2020). Few months later, in June 2019 a new US cyber operation was articulated and reported to consist of deployment of hacking tools at Russian grid systems (NYT, Sanger D.E., Perlroth N., *US Escalates Online Attacks on Russia's Power Grid*, 15 June 2019, available at: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html, accessed on 1 November 2020).

[206] Dizaji S. F., van Bergeijk P. A. G., Potential Early Phase Success and Ultimate Failure of Economic Sanctions: a VAR Approach with an Application to Iran, *Journal of Peace Research*, vol. 50, no. 6, 2013, pp. 721-36.

[207] See EU Best Practices for the effective implementation of restrictive measures, updated, 8519/18, 4 May 2018, available at: https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf (accessed on 4 November 2020); Guidelines on Implementation and Evaluation of Restrictive Measures in the framework of the EU CFSP – update, 5664/18, 4 May 2018, available at: https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf (accessed on 4 November 2020); Hovi J., Huseby R., Sprinz D.F., When Do (Imposed) Economic Sanctions Work?, *World Politics*, 2005, Vol. 57, Issue 4, pp 479 – 499; Giumelli F., Ivan P., The Effectiveness of EU Sanctions, EPC Issue Paper No. 76, 2013, p. 20, available at: http://hdl.handle.net/11370/3fb316d8-d072-4be0-bb66-4fa750d07502 (accessed on 4 November 2020).

Vera N. Rusinova
National Research University Higher School of Economics (Moscow, Russia). School of International Law of the Law Faculty, Faculty of Law. Professor.
E-mail: vrusinova@hse.ru

Ekaterina A. Martynova
National Research University Higher School of Economics. Faculty of Law. Master's student.
E-mail: eamartynova_1@edu.hse.ru

Polina Kurakina
National Research University Higher School of Economics. Faculty of Law. Master's student.
E-mail: pol.kurakina@yandex.ru

Corresponding author
Correspondence to Vera Rusinova.