Israel Law Review (2024), **57**, 135–174
doi:10.1017/S0021223722000255

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses

Vera Rusinova[1] and Ekaterina Martynova[2]

[1] Doctor of Legal Sciences, LL.M (Goettingen); Professor, Head of the School of International Law of the Law Faculty, National Research University Higher School of Economics (HSE University), Moscow (Russia); Leader of the Research and Study Group 'International Law in the Age of Cyber'; and [2] PhD candidate, National Research University Higher School of Economics (HSE University), Moscow (Russia); Member of the Research and Study Group 'International Law in the Age of Cyber'
Corresponding author: Ekaterina Martynova; Email: eamartynova@hse.ru

(First published online 9 May 2023)

Abstract

This article contributes to the understanding of why states resort to targeted, or smart, sanctions to meet the 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 the article are legal positivism and political theories, including Mancur Olson's theory of groups and Francesco Giumelli's analytical framework for assessment of sanctions. The authors address the effectiveness of sanctions as a reaction to cyber-enabled activities through the lens of regulation introduced in the United States, the European Union and the United Kingdom, which are the most developed counter-cyber sanction regimes, analysing publicly known cases of cyber-related sanctions.

Keywords: cyber attacks; cyber security; economic sanctions

1. Introduction

Cyber incidents have become daily events; moreover, the coronavirus pandemic of 2020 triggered a significant growth in malicious cyber operations. For instance, the FBI reported about a 300 per cent increase in cyber security complaints just in the wake of the pandemic.[1] Only some of the cyber

[1] Maggie Miller, 'FBI Sees Spike in Cyber Crime Reports during Coronavirus Pandemic', *The Hill*, 16 April 2020, https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic.

operations taking place around the world are suspected of being state-sponsored. In 2020 about 88 allegedly interstate operations, mostly espionage, were reported.[2] According to the Council of Foreign Relations, which has tracked significant cyber operations since 2005, 36 states are suspected of sponsoring cyber operations; in this list China, Russia, Iran and North Korea are designated as responsible for 77 per cent of all cyber operations of this type.[3]

Responses from states that suffer from cyber operations include sanctions, the expulsion of diplomats, criminal indictments under domestic law and, rarely, openly announced 'hacking back'. The timeline of sanctions following alleged interstate cyber operations contains at least 20 episodes.[4] It starts with the sanctioning by the US of North Korean entities and individuals arising from the cyber attack on Sony Pictures in January 2015,[5] and concludes with the US sanctions imposed against virtual currency mixer Tornado Cash in August 2022.[6]

Apart from these episodes, the United States imposed sanctions on North Korea for an attack against crypto-currency exchanges in March 2020;[7] six Nigerians were sanctioned by the US for business email and romance fraud in June 2020;[8] the Iranian cyber group APT39, 45 associated individuals, and a front company, Rana Intelligence – which were designated as backed by the Iranian Ministry of Intelligence and Security – were sanctioned by the US for a series of cyber attacks in September 2020.[9] In addition, the US imposed sanctions against six Iranian individuals and one Iranian entity for alleged attempts to influence the 2020 US presidential election in November 2021.[10] That said, the greatest number of designations relates to sanctioning Russian individuals and entities, or actors in other jurisdictions (in particular,

[2] Council on Foreign Relations, Cyber Operation Tracker, https://www.cfr.org/cyber-operations.

[3] ibid.

[4] Certain limitations of case selection for this study should be noted. First, this study is concerned only with cases in which sanctions were actually imposed (threats to implement sanctions remained outside this research). Second, we reviewed cases where sanctions or a combination of sanctions and other means of response were implemented; cases of solely diplomatic reaction or criminal indictment without sanctions imposition were excluded. Finally, our dataset included only cases of alleged interstate cyber attacks, leaving aside designation of cyber criminals as individuals without any links to the government.

[5] John Kerry, US Secretary of State, 'Condemning Cyber-Attack by North Korea', 19 December 2014, https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm.

[6] US Department of the Treasury, 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash', 8 August 2022, https://home.treasury.gov/news/press-releases/jy0916.

[7] US Department of the Treasury, 'Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group', 2 March 2020, https://home.treasury.gov/news/press-releases/sm924.

[8] US Department of the Treasury, 'Treasury Sanctions Nigerian Cyber Actors for Targeting U.S. Businesses and Individuals', 16 June 2020, https://home.treasury.gov/news/press-releases/sm1034.

[9] US Department of State, 'The United States Sanctions Cyber Actors Backed by Iranian Intelligence Ministry', 17 September 2020, https://2017-2021.state.gov/the-united-states-sanctions-cyber-actors-backed-by-iranian-intelligence-ministry/index.html.

[10] US Department of the Treasury, 'Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election', 18 November 2021, https://home.treasury.gov/news/press-releases/jy0494.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

China), for their involvement in malicious activities conducted by Russian-based actors. US sanctions against Russian 'cyber actors' were imposed for the meddling in the US presidential elections in 2016,[11] the development and distribution of the Dridex malware by Evil Corp in 2019,[12] phishing campaigns against crypto-currency exchanges in September 2020,[13] cyber attacks that used Triton malware in October 2020,[14] the SolarWinds cyber attack and other malicious cyber activities in April 2021,[15] and the Kaseya incident in November 2021.[16] US President Biden considers cyber security to be the top priority[17] and declared in April 2021 a national emergency to deal with the 'unusual and extraordinary' threat of malicious cyber-enabled activities against the US and its allies and partners.[18] Later, in September 2021, the Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments was released as a part of broader US counter-ransomware strategy,[19] followed by sanctions imposed on the SUEX virtual currency exchange,[20] the darknet market Hydra Market, and the Garantex virtual currency exchange, all such entities allegedly being operated out of Russia.[21]

[11] US Department of the Treasury, 'Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks', 15 March 2018, https://home.treasury.gov/news/press-releases/sm0312.

[12] US Department of the Treasury, 'Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware', 5 December 2019, https://home.treasury.gov/news/press-releases/sm845.

[13] US Department of the Treasury, 'Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft', 16 September 2020, https://home.treasury.gov/news/press-releases/sm1123.

[14] US Department of the Treasury, 'Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware', 23 October 2020, https://home.treasury.gov/news/press-releases/sm1162.

[15] US Department of the Treasury, 'Treasury Sanctions Russia with Sweeping New Sanctions Authority', 15 April 2021, https://home.treasury.gov/news/press-releases/jy0127.

[16] US Department of the Treasury, 'Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange', 8 November 2021, https://home.treasury.gov/news/press-releases/jy0471.

[17] Eric Geller, 'Biden Pledges Robust Response to Cyber Crisis "From the Moment We Take Office"', *Politico*, 17 December 2020, https://www.politico.com/news/2020/12/17/biden-cyber-crisis-response-447858; Richard Luscombe, 'Biden Mulls Punishments for Russia over Suspected Role in Government Hack', *The Guardian*, 20 December 2020, https://www.theguardian.com/world/2020/dec/20/russian-hack-suspected-role-biden-mulls-punishment.

[18] The White House, 'A Letter on Blocking Property with respect to Specified Harmful Foreign Activities of the Government of the Russian Federation', 15 April 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/a-letter-on-blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the-russian-federation.

[19] US Department of the Treasury, 'Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments', 21 September 2021, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[20] US Department of the Treasury, 'Treasury Takes Robust Actions to Counter Ransomware', 21 September 2021, https://home.treasury.gov/news/press-releases/jy0364.

[21] US Department of the Treasury, 'Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex', 5 April 2022, https://home.treasury.gov/news/press-releases/jy0701.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

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,[22] and North Korean and Chinese citizens for the WannaCry virus.[23] 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[24] and the alleged cyber attack on the Bundestag in October 2020,[25] and against two Chinese citizens and one legal entity for Operation Cloud Hopper in July 2020.[26] The UK applied the EU sanctions until the exit date, and implemented its own regime at least twice in March 2022, against (i) eight Russian individuals and one legal entity designated under the urgent procedure by means of a reference to the US decision to sanction these persons for the cyber attack on the Bundestag and spreading disinformation;[27] and (ii) a Russian-based research institution which was also earlier sanctioned by the US for an alleged cyber attack on a petro-chemical company in August 2017.[28] Even taking into consideration the average percentage of espionage operations, which are usually not followed by economic sanctions,[29] 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 where states that suffered from alleged interstate 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. The concept of targeted or 'smart' sanctions, which substituted the 'comprehensive' sanctions, was operationalised by the United Nations, as well as by the

[22] Council Implementing Regulation (EU) 2020/1125 of 30 July 2020, Implementing Regulation 2019/796 concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States, [2020] OJ L246/4; US Department of the Treasury, 'Treasury Sanctions Russian Federal Security Service Enablers', 11 June 2018, https://home.treasury.gov/news/press-releases/sm0410.

[23] EU Regulation 2020/1125 (n 22); US Department of the Treasury, 'Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups', 13 September 2019, https://home.treasury.gov/index.php/news/press-releases/sm774.

[24] EU Regulation 2020/1125 (n 22).

[25] 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, [2020] OJ L 351 I/1; UK Foreign, Commonwealth and Development Office, 'UK Enforces New Sanctions against Russia for Cyber Attack on German Parliament', 22 October 2020, https://www.gov.uk/government/news/uk-enforces-new-sanctions-against-russia-for-cyber-attack-on-german-parliament.

[26] EU Regulation 2020/1125 (n 22).

[27] HM Treasury, Office of Financial Sanctions Implementation, 'Financial Sanctions Notice: Cyber', 15 March 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060768/Notice_Cyber_150322.pdf.

[28] HM Treasury, Office of Financial Sanctions Implementation, 'Financial Sanctions Notice: Cyber', 24 March 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1063154/Notice_Cyber_240322.pdf.

[29] The imposition of sanctions for the cyber-espionage operation Cloud Hopper by the EU is the sole example: EU Regulation 2020/1125 (n 22).

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

United States and later by other states, by 2010.[30] Targeted sanctions were used with varying degrees of success for different purposes, including 'fight with terror', compliance with the nuclear non-proliferation regime, non-constitutional changes of government, and respect for human rights. However, the question is why states resort to targeted sanctions to meet the 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' generally refers 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).[31] Alongside traditional forms of sanctions such as 'trade-restricting policies between sovereign nations'[32] – which include boycotts, embargoes, tariffs and non-tariff barriers, export and/or import restriction such as quotas[33] – states may 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 that imposes sanctions.[34] Although sanctions can also take the form of restriction of movement of particular individuals (travel ban), they are predominantly of an economic or financial nature. Contemporary studies typically 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.[35] Sanctions are considered to be 'politically motivated'[36] and can be imposed on private actors either working for or having strong ties with the government with the purpose of influencing the decision making of state authorities.[37]

Economic sanctions are common in international politics, and the question of the effectiveness of this tool has been studied for decades. The most authoritative methodological basis for the assessment of the effectiveness of sanctions

[30] Daniel W Drezner, 'Sanctions Sometimes Smart: Targeted Sanctions in Theory and Practice' (2011) 13(1) *International Studies Review* 96, 97.

[31] Gary Clyde Hufbauer and others, *Economic Sanctions Reconsidered* (3rd edn, Peterson Institute for International Economics 2007) 3.

[32] Maarten Smeets, 'Can Economic Sanctions Be Effective?', WTO Economic Research and Statistics Division, Staff Working Paper ERSD-2018-03, 15 March 2018, 4.

[33] For a discussion of the compatibility of economic sanctions with World Trade Organization obligations see Rostam J Neuwirth and Alexandr Svetlicinii, 'The Economic Sanctions over the Ukraine Conflict and the WTO: "Catch-XXI" and the Revival of the Debate on Security Exceptions' (2015) 5 *Journal of World Trade* 891, 894.

[34] Hufbauer and others (n 31) 63.

[35] David A Baldwin and Robert A Pape, 'Evaluating Economic Sanctions' (1998) 23(2) *International Security* 189, 191.

[36] Francesco Giumelli, *Coercing, Constraining and Signaling: Explaining UN and EU Sanctions after the Cold War* (ECPR Press 2011) 3.

[37] For instance, between 22 February and 20 October 2022, Australia, Canada, the EU, France, Japan, Switzerland, the UK and the US imposed sanctions on 8,330 individuals and 1,543 entities from Russia: Statista, 'Sanctions Imposed on Russia 2022, by Target', November 2022, https://www.statista.com/statistics/1293531/western-sanctions-imposed-on-russia-by-target.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

in general was by Hufbauer and co-authors,[38] who proposed guidelines for estimating the potential success of sanctions based on indicators that include policy goals and the security, as well as the political or other costs incurred by the sender.[39] A legal strand of sanction research is represented by inquiries that focus on the legal nature and legality of unilateral sanctions.[40] The legality of sanctions not authorised by the UN Security Council remains a grey area of international law,[41] dividing scholars into

[38] In 1985 Hufbauer and co-authors published the 1st edition of *Economic Sanctions Reconsidered: History and Current Policy* (Peterson Institute for International Economics 1985) based on case studies of 103 sanctions episodes and analysis of sanctions-related public policies. The 2nd edition of *Economic Sanctions Reconsidered* (Peterson Institute for International Economics 1990) and the 3rd edition of 2007 (n 31) remain among the most cited studies on the subject. A number of quantitative studies followed the work of Hufbauer and others, most of which demonstrated that while sanctions sometimes make targets change their behaviour, some identifiable factors do contribute to the success of sanctions: eg, Jaleh Dashti-Gibson, Patricia Davis and Benjamin Radcliff, 'On the Determinants of the Success of Economic Sanctions: An Empirical Analysis' (1997) 41 *American Journal of Political Science* 608; Daniel W Drezner, 'Conflict Expectations and the Paradox of Economic Coercion' (1998) 42 *International Studies Quarterly* 709. Nonetheless, this approach of Hufbauer and co-authors is not free from critique: see Robert A Pape, 'Why Economic Sanctions Do Not Work' (1997) 22(2) *International Security* 90. A turn towards the study of targeted sanctions is seen since the early 2000s, when the voices of those who oppose comprehensive sanctions based on their negative externalities sound more convincing: eg, David Cortright and George Lopez, *Smart Sanctions: Targeting Economic Statecraft* (Rowman & Littlefield 2002); Michael Brzoska, 'From Dumb to Smart? Recent Reforms of UN Sanctions' (2003) 9 *Global Governance* 519; Ella Shagabutdinova and Jeffrey Berejikian, 'Deploying Sanctions while Protecting Human Rights: Are Humanitarian "Smart" Sanctions Effective?' (2007) 6 *Journal of Human Rights* 59. The UN Targeted Sanctions database by Biersteker and co-authors (Thomas J Biersteker, Sue E Eckert and Marcos Tourinho (eds), *Targeted Sanctions* (Cambridge University Press 2016)) is another heavily cited data source for research on whether economic sanctions work. Based on analysis of 23 episodes of UN-targeted sanctions, Biersteker and co-authors assess only 22 per cent of sanctioning cases to be successful, which is lower than the overall success rate reported by Hufbauer and others (34 per cent). Elizabeth Rosenberg and co-authors in *The New Tools of Economic Warfare: Effects and Effectiveness of Contemporary U.S. Financial Sanctions* (Center for a New American Security 2016) examine the effectiveness of financial sanctions particularly, and conclude that this type of sanction is relatively more effective (in up to 40 per cent of cases) than other types of sanction. Lektzian and Patterson (David Lektzian and Dennis Patterson, 'Political Cleavages and Economic Sanctions: The Economic and Political Winners and Losers of Sanctions' (2015) 59 *International Studies Quarterly* 46), and Pond (Amy Pond, 'Economic Sanctions and Demand for Protection' (2017) 61 *Journal of Conflict Resolution* 1073) study economic and political costs incurred by senders and targets as well as micro-dynamics of the success rate of sanctions. For a detailed and critical review of literature on the effectiveness of economic sanctions refer to Dursun Peksen, 'When Do Imposed Economic Sanctions Work? A Critical Review of the Sanctions Effectiveness Literature' (2019) 30 *Defence and Peace Economics* 635.

[39] Hufbauer and others (n 31) 158–59.

[40] On these issues see Stanley J Marcuss and Stephen D Mathias, 'U.S. Foreign Policy Export Controls: Do They Pass Muster under International Law?' (1984) 2 *Berkeley Journal of International Law* 1; Bradley A Curtis and Jack L Goldsmith, 'Customary International Law as Federal Common Law: A Critique of the Modern Position' (1997) 10 *Harvard Law Review* 815.

[41] Alexandra Hofer, 'The Developed/Developing Divide on Unilateral Coercive Measures: Legitimate Enforcement or Illegitimate Intervention?' (2017) 16 *Chinese Journal of International Law* 175.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

those who support[42] and those who challenge it.[43] Studies have also been conducted on improving the legal regime and regulatory policies concerning sanctions.[44] However, sanctions taken in response to malicious cyber operations, although mentioned in general in a number of publications[45] or with respect to particular cases,[46] have not yet been discussed in detail in the legal literature.

This article contributes to the understanding of how the resort to and effectiveness of economic sanctions implemented in response to cyber operations can be assessed. The research is characterised by two key features. First, the analysis is informed by legal and political theories. The legal analysis represents a positivistic explanation of resorting 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 states with regard to the legal qualification of cyber operations expressed at meetings of the UN Open-Ended Working Group (OEWG) held in 2019 and 2020, and written statements made at those meetings[47] or articulated in other official documents. The political methods applied in this research

[42] The first general justification for the legality of economic coercive measures is the *Lotus* principle (PCIJ, *SS Lotus case* (*France v Turkey*) (1927) PCIJ Rep (Ser A, No 10) 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 recognised as customary international law. In the light of this principle, economic sanctions are prima facie legal; see Hofer (n 41) 180 para 9. The second justification is based on the law of countermeasures. In this respect Gestri has described the EU as 'a trailblazer' in implementing the doctrine of 'collective countermeasures': Marco Gestri, 'Sanctions Imposed by the European Union: Legal and Institutional Aspects' in Natalino Ronzitti (ed), *Coercive Diplomacy, Sanctions and International Law* (Brill/Nijhoff 2016) 70, 99. See also Daniel H Joyner, 'UN Counter-Proliferation Sanctions and International Law' in Larissa van den Herik (ed), *Research Handbook on U.N. Sanctions and International Law* (Edward Elgar 2017) 105; and Devika Hovel, 'Unfinished Business of International Law: The Questionable Legality of Autonomous Sanctions' (2019) 113 *American Journal of International Law Unbound* 140.

[43] Rahmat Mohamad, 'Unilateral Sanctions in International Law: A Quest for Legality' in Ali Z Marossi and Marisa R Bassett (eds), *Economic Sanctions under International Law: Unilateralism, Multilateralism, Legitimacy, and Consequences* (Asser Press/Springer 2015) 71. See also Matthew Happold, 'Economic Sanctions and International Law: An Introduction' in Matthew Happold and Paul Eden (eds), *Economic Sanctions and International Law* (Hart 2016) 1.

[44] Carter's work on reforming the US sanctions regime can be distinguished as particularly comprehensive: Barry E Carter, 'International Economic Sanctions: Improving the Haphazard U.S. Legal Regime' (1987) 75 *California Law Review* 1163. See also Sarabeth Egle, 'The Learning Curve of Sanctions – Have Three Decades of Sanctions Reform Taught Us Anything?' (2010) 19 *Currents: International Trade Law Journal* 34; Anthonius W de Vries, Clara Portela and Borjia Guijarro-Usobiaga, 'Improving the Effectiveness of Sanctions: A Checklist for the EU', *CEPS Special Reports*, No 95, November 2014, https://core.ac.uk/download/pdf/76796051.pdf.

[45] François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020); Anders Henriksen, 'Lawful State Responses to Low-Level Cyber-Attacks' (2015) 84 *Nordic Journal of International Law* 323.

[46] Christina Lam, 'A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election' (2018) 59 *Boston College Law Review* 2167.

[47] The Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security held two substantive sessions: 9–13 September 2019 and 10–14 February 2020.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

include Mancur Olson's theory of groups and Francesco Giumelli's analytical framework for sanction assessment. Secondly, we address the question of the effectiveness of sanctions as a reaction to cyber activities using examples of the regulation introduced in the United States, the European Union and the United Kingdom, which are the most developed counter-cyber sanction regimes assisted with state practice of sanctions imposition.[48] The analysis is empirically based on a poll of 20 cases, when sanctions were imposed by the US, the EU and/or the UK in response to alleged interstate 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. Finally, we conclude by outlining the prospects for cyber-related sanctions on the basis of the interaction between the legal and extra-legal layers of their assessment.

2. 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 the wrongful act to comply with its obligations;[49] it presupposes that a cyber operation, as an initial act of injury, breaches international law and is subject to requirements, which include the proportionality and reversibility of the response, the ongoing character of the initial wrongful act, and a duty of notification.[50] 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,[51] it does not necessitate the qualification of the cyber operation as violating any international legal obligation.

Sanctions taken by the US, the EU and the UK in response to cyber operations point to a clear tendency to shape them as acts of retorsion rather than 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 primary 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

[48] Apart from the US, the EU and the UK, Australia introduced a cyber-specific sanctions regime in December 2021: Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Regulations 2021, F2021L01855, https://www.legislation.gov.au/Details/F2021L01855. The Australian regulation contemplates targeted financial sanctions and a travel ban on the persons designated as responsible for 'significant cyber incidents'. The power of designation is vested in the Minister for Foreign Affairs. Our examination of the Consolidated List as of 24 October 2022 (https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list) did not reveal any designations under the counter-cyber sanctions regime.

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

[50] ibid arts 49–53.

[51] International Law Commission, Articles on the Responsibility of States for Internationally Wrongful Acts, with Commentaries (2001), UN Doc A/56/10 (ARSIWA with Commentaries).

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

to a particular state – a duty that has a requirement to reach the standard of proof applicable in international law.

2.1. 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, interstate 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 against using 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'[52] – is still in a nascent form and, despite the positions of some states,[53] is widely considered *lex ferenda*.[54] The *lex lata* scope of obligations is constrained to the general duty of a state 'not to allow knowingly its territory to be used for acts contrary to the rights of other States', as formulated by the International Court of Justice (ICJ) in the *Corfu Channel* case[55] and other positive obligations stemming from the no harm principle, international humanitarian law and international human rights law.[56] In comparison with this 'patchwork' of existing duties,[57] the application of the 'cyber due diligence' norm would have extended the

[52] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 30–50.

[53] The Netherlands: Ministry of Foreign Affairs, 'Letter to the Parliament on the International Legal Order in Cyberspace', 5 July 2019, 4–5, 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; France: Ministère des Armées, 'International Law Applied to Operations in Cyberspace', October 2019, 6, 9–10, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-oninternational-law-applied-to-cyberspace.pdf.

[54] The GGE Report of 2015 envisages a negative obligation of states to 'not knowingly allow their territory to be used for internationally wrongful acts using ICTs' as 'voluntary, non-binding norms, rules or principles of responsible behaviour of States': UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General (26 June 2015), UN Doc A/70/174, para 13(c) (GGE Report 2015). See The White House, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World', May 2011, 10, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; see also Scott J Shackelford, Scott Russell and Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' (2016) 17 *Chicago Journal of International Law*, article 1, 22–23; François Delerue, 'Cyber Operations and the Principle of Due Diligence' in François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 353.

[55] ICJ, *Corfu Channel (United Kingdom v Albania)*, Judgment [1949] ICJ Rep 4.

[56] Antonio Coco, Talita de Souza Dias, "Cyber Due Diligence': A Patchwork of Protective Obligations in International Law' (2021) 32 *European Journal of International Law* 804.

[57] ibid.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

scope of primary behaviour beyond the internationally wrongful acts to cover cyber operations with 'serious adverse consequences'.

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 United Nations,[58] is well represented in legal scholarship[59] and – at least, as a matter of principle – affirmed by states.[60] However, even this level of abstraction is not free from disagreement.[61] The Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security was unable to adopt final reports in 2016–2017 because of the position articulated by Cuba,[62] and backed by Russia[63] and China.[64] According to this, the 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 [information and communication technologies] and the concept of "armed attack"'[65] under Article 51 of the UN Charter, and thereby militarise the use of and the response to information and communication technologies (ICTs). The same divergence was found in the positions of states expressed at the OEWG meetings in 2019 and 2020.[66] While the majority of states confirmed the applicability of international law in its

[58] Charter of the United Nations (entered into force 24 October 1945) 1 UNTS XVI (UN Charter).

[59] See, inter alia, Schmitt (n 52); James Gow and others (eds), *Routledge Handbook of War, Law and Technology* (Routledge 2019); Yoram Dinstein and Arne Willy Dahl, *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary* (Springer Nature 2020).

[60] The UN General Assembly welcomed this affirmation of the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security on numerous occasions: see UNGA Res 70/237, Developments in the Field of Information and Telecommunications in the Context of International Security (23 December 2015), UN Doc A/RES/70/237. A significant number of states confirmed this applicability during the sessions of the OEWG.

[61] See also Michele G Markoff, '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', 23 June 2017, https://2017-2021.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/index.html.

[62] Declaration by Cuba, at the Final Session of GGE on Developments in the Field of Information and Telecommunications in the Context of International Security, 23 June 2017, http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.

[63] Ministry of Foreign Affairs of the Russian Federation, '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, http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288.

[64] China did not publicly share its position; see Elaine Korzak, 'UN GGE on Cybersecurity: The End of an Era?', *The Diplomat*, 31 July 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe.

[65] Declaration by Cuba (n 62).

[66] For instance, Pakistan, Russia, the Syrian Arab Republic: OEWG, 11 September 2019, 11 February 2020 (n 47).

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

entirety to cyberspace,[67] it was contested by a group of states that used 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.[68] Some states took an intermediate position by appealing to the need to adopt new legally binding instruments.[69] In its report of 2021 the GGE finally acknowledged the applicability of international humanitarian law, but highlighted that these norms apply 'only in situations of armed conflict'.[70] This acknowledgement is ambivalent, as the question of whether a particular operation with the use of ICTs can be qualified as 'an armed conflict' remains outside the brackets; hence this issue will continue to raise controversies in the future.

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,[71] or originates from state behaviour in shaping either the lawmaking path or that of the interpretation of law (as the subsequent application of the relevant rules). 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 interstate cyber operations,[72] or in the contested applicability of general, non-cyber-specific rules in a cyber context. Taking into account recently articulated positions of states expressed officially 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[73] in cyberspace encounters not only the problem of the indeterminacy of its threshold and the scope of protected infrastructure,[74] but also a split in the official positions of different states with regard 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

[67] Austria, Brazil, Canada, Chile, Czech Republic, European Union, Italy, Lichtenstein, New Zealand, Pacific Islands Forum, Sweden, Switzerland, United Kingdom, and others: OEWG, 11 February 2020 (n 47).

[68] Russia raised a question of how the application of international law in cyberspace correlates with voluntary principle: OEWG, 11 February 2020 (n 47).

[69] Cuba, Egypt, Jordan, Pakistan, Singapore, Syria: OEWG, 11 February 2020 (n 47).

[70] Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (14 July 2021), UN Doc A/76/135, para 71(f),

[71] Schmitt (n 52); Dinstein and Dahl (n 59).

[72] Jean D'Aspremont, 'Cyber Operations and International Law: An Interventionist Legal Thought' (2016) 21 *Journal of Conflict and Security Law* 580.

[73] *Corfu Channel* (n 55); ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)* Merits, Judgment [1986] ICJ Rep 14; 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 [2015] ICJ Rep 665.

[74] Experts on *Tallinn 2.0* were strongly divided in respect of this issue: Schmitt (n 52) 20–27.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

sovereignty is merely a principle, not a rule.[75] In contrast, France reserved a maximal wide approach, claiming that its sovereignty would be violated by 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'.[76] 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 for a minimal threshold.[77] Finland expressed a comparable position at the first OEWG.[78]

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 intervention, 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 judgment in the *Nicaragua* case of 1986[79] (which consisted of the element of coercion and an interference into *domaine réservé*) and apply a very broad grid to outlawed behaviour. Therefore, the non-interference principle, which was underinclusive in non-cyber operations, became extremely underinclusive in cyber operations.

There is a strong tendency in the legal literature to problematise the element of coercion as making the non-interference principle almost unworkable in the cyber context (for attacks having malicious or retaliatory aims cannot be qualified as coercive),[80] but there are also reasons to claim that the first

[75] Jennifer M O'Connor, 'Memorandum "International Law Framework for Employing Cyber Capabilities in Military Operations"', 19 January 2017 (quoted in Harriet Moynihan, 'The Application of International Law to State Cyberattacks Sovereignty and Non-intervention', Chatham House, Research Paper, December 2019, fn 36, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf; Jeremy Wright, Attorney-General (UK), 'Cyber and International Law in the 21st Century', MP Speech on the UK's Position on Applying International Law to Cyberspace, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[76] Ministère des Armées (France) (n 53) 6, 9–10.

[77] Government of the Netherlands, Ministry of Foreign Affairs, Letter to the Parliament on the International Legal Order in Cyberspace, 26 September 2019, 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; Michael Schmitt, 'The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis', *Just Security*, 14 October 2019, https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis.

[78] International Law and Cyberspace: Finland's National Positions, October 2020, https://front.un-arm.org/wp-content/uploads/2020/10/finland-views-cyber-and-international-law-oct-2020.pdf.

[79] *Nicaragua* (n 73) para 205.

[80] The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations provides that

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

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'.[81] The notion of *domaine réservé* was and remains bound with realisation by the state of its powers and competences, but cannot be regarded as a 'shelter, fully covering entire areas of politics'.[82] For instance, although the election process falls within *domaine réservé*, this does not mean that all activities related thereto are protected by the non-interference principle. Elections belong to *domaine réservé*, but this covers only governmental functions related to this process. If we take US election meddling 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,[83] fall within *domaine réservé*. Other acts, arguably, do not. Among them are hacking by the so-called Cozy Bear and Fancy Bear hacking groups, the subsequent publication on WikiLeaks of the Democratic National Committee emails, hacking the account of John Podesta, chairman of Hillary Clinton's campaign, and a massive informational operation in social networks, based on the 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 'armed attack',[84] which was further supported by the 'scale and effects' doctrine elaborated by the ICJ in the *Nicaragua* case.[85] Although the military paradigm to treat interstate cyber operations received the bulk of attention,[86] the application of these norms to cyberspace is not free from controversy. The reason for this is not only the ever-used indeterminacy argument in respect of the threshold of 'use of force' and 'armed attack'.[87] The commonly used logic of applying *jus ad bellum* to cyber operations is based on the acknowledgement that the prohibition of the use of force may be violated by any use of force, regardless of the type of weapon,[88] and is underpinned

'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 its advantages of any kind': UNGA Res 2625 (XXV) (24 October 1970).

[81] *Nicaragua* (n 73) para 205.

[82] Katja S Ziegler, 'Domaine Réservé' in Rüdiger Wolfrum and Anne Peters (eds), *Max Planck Encyclopedia of Public International Law* (online edn, April 2013) 213, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1398.

[83] David E Sanger and Catie Edmondson, 'Russia Targeted Election Systems in All 50 States, Report Finds', *The New York Times*, 25 July 2019, https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html.

[84] UN Charter (n 58) art 2, art 51; *Nicaragua v US* (n 73) [191].

[85] *Nicaragua* (n 73) [195].

[86] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 48–51; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 53–60.

[87] Olivier Corten, *The Law Against War* (Hart 2012) 5–27.

[88] ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion [1966] ICJ Rep 226, [39].

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

by the permissibility of the consequential use of the analogy with kinetic attacks (causing death, injury or the destruction of physical objects). However, the problem arises from the fact that the chain of consequences launched by a cyber operation might be significantly longer in comparison with the conventional use of force. Not challenging the fact that some cyber operations can take a military form, the use of that analogy can be overstretched to produce results that contrast the well-known refusal of the drafters of the Charter to understand 'economic coercion' as falling within the scope of prohibited behaviour.[89]

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 mainstream.[90] 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; 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.[91] Should one not doubt the soundness of the consequentialist approach, the majority of publicly known cyber operations[92] do not reach the threshold of 'use of force' because of their low intensity.[93]

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 – that is,[94]

> 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

[89] Oliver Dörr and Albrecht Randelzhofer, 'Article 2(4)' in Bruno Simma (ed), *The Charter of the United Nations: A Commentary* (3rd edn, Oxford University Press 2012) 17, 18, 21.

[90] OEWG (n 47) 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, 'Krieg im "Cyber-Raum" – offensive und defensive Cyberstrategie des Bundesministeriums der Verteidigung', *Drucksache* 18/6989, 10 December 2015, 10; UK: Wright (n 75); US: Harald Hongju Koh, 'International Law in Cyberspace' (2012) 54 *Harvard International Law Journal Online*.

[91] ibid.

[92] Center for Strategic and International Studies, 'Significant Cyber Incidents since 2006', https://csis-website-prod.s3.amazonaws.com/s3fs-public/200901_Significant_Cyber_Events_List.pdf.

[93] Sean Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention' in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015) 249, 249–50.

[94] Ministère des Armées (France) (n 53) 7.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

extent of intrusion, the actual or intended effects of the operation or the nature of the intended target.

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'.[95] 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 included 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'.[96]

Turning to the applicability of *jus in bello* norms to cyber operations, can we truly celebrate that the states answer this question in the affirmative? To begin with, in almost all cases when the application of international humanitarian law is confirmed, we do not know in which source. For instance, 79 states have supported the Paris Call for Trust and Security in Cyber Space, which states laconically that international humanitarian law 'is applicable to the use of information and communication technologies by States'.[97] A more or less detailed position has been represented by only a few states, which so far include Australia,[98] Germany,[99] the Netherlands,[100] the UK,[101] the US,[102] France,[103] Finland,[104] and Israel.[105]

The argument of opponents is that the applicability of international humanitarian law will legitimise militarisation of cyberspace if taken per se, and seems to go against the whole history of the development of *jus in bello* norms. However, this rebuttal is convincing only if it implies a superficial meaning for the argument of militarisation. Another way is to read it as exposing that without a clear determination of borderlines between cyber operations as a 'use of force' or an 'armed attack' in *jus ad bellum* terms and an

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

[96] UK Ministry of Defence, *Cyber Primer* (2nd edn, 2016) Annex 1A: International Law Aspects, 12.

[97] Paris Call for Trust and Security in Cyber Space, 11 December 2018, https://pariscall.international/en/call.

[98] 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.

[99] Antwort der Bundesregierung (Germany) (n 90) 4, 5, 7.

[100] Ministry of Foreign Affairs (The Netherlands) (n 77).

[101] Wright (n 75).

[102] Koh (n 90).

[103] Ministère des Armées (France) (n 53).

[104] International Law and Cyberspace: Finland's National Positions (n 78).

[105] Roy Schondorf, 'Israel's Perspective on Key Legal and Practical Issues concerning the Application of International Law to Cyber Operations', *EJIL:Talk!*, 9 December 2020, https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

'attack' or a 'military operation' in *jus in bello* terms, on the one hand, and cyber operations as (ordinary) malicious acts which may take place also during armed conflicts, on the other hand, the shift to international humanitarian law can lead to a misuse of a military legal paradigm of international law. So, at the end of the day it would be *jus in bello* instead of international human rights law, or national criminal law, which may be well based on numerous international treaties in this respect, as it is not something new when states are sheltering their activities and, on the basis of *lex specialis*, exclude the application of other regimes.

Finally, the affirmative approach – which is widely endorsed as progressive and pro-humanitarian – can serve to ignore the necessity to adopt cyber-specific norms of international law, although the international humanitarian law regime is full of loose ends and general notions that cannot be seen as self-executing in the cyber context. Hence, the application of international humanitarian law can overstretch such norms, for their material content and design are not tailored for cyberspace.

A collective affirmation of the applicability of international humanitarian law to cyber operations can also lead to disappointment as, besides applicability *in abstracto*, what deserve close scrutiny are the questions of whether international humanitarian law norms are relevant, adequate and sufficient to deal with military types of cyber operation. There can be identified, at least, three problematic issues. First, what can be highlighted is the scarcity of international humanitarian law provisions applicable to 'military operations', even in international armed conflicts. It forms a problem as the majority of cyber operations will not reach the threshold of the international humanitarian law notion of 'an attack', and will be qualified as 'military operations', if at all. Under Articles 51(1) and 57(1) of the First Additional Protocol the duties of the parties to international armed conflicts are too general and laconic in imposing the general protection of the civilian population and constant care. Let us use France as an example, once again. The French Ministry of Defence has articulated a broad approach to the 'use of force' and considered cyber operations without physical damage as falling within this notion, but in the end it had nothing more to do than to admit that 'most operations, including offensive cyberwarfare operations carried out by France in an armed conflict situation, remain below the attack threshold' and 'they remain governed by general principles of IHL'.[106]

The second problem arises when states try to circumvent the limitations of the scope of 'an attack' under *jus in bello* by stretching this notion to embrace more types of cyber operation. For instance, in his remarks of 10 November 2016, US legal adviser Brian Egan opined that, although 'not all cyber operations rise to the level of an "attack" as a legal matter under the law of armed conflict', it is still possible to determine such cyber operation as an attack, 'considering, among other things, whether a cyber activity results in kinetic or non-kinetic effects, and the nature and scope of those effects, as well as the nature of the connection, if any, between the cyber activity and

[106] Ministère des Armées (France) (n 53) 13.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

the particular armed conflict in question'.[107] The use of this method will result in an objective inapplicability of international humanitarian law provisions dedicated to 'attacks', simply because they are thought and designed to govern kinetic operations.

The third problem connected with the applicability of international humanitarian law to cyber operations originates from the fact that perpetrators of cyber attacks can be in different densities of alliance with the state or a non-governmental party to the armed conflict. Combined with the different nature of cyber operations, this fact can render the rules and concept of 'direct participation of hostilities' in its different incarnations reflected in legal scholarship and jurisprudence[108] underinclusive. This outcome results from either a very strict connection with the party to the conflict with regard to classification as a combatant or member of the armed forces, or groups in non-international armed conflicts, or from the requirement of the kinetic-like harm, direct causation, or in some cases a belligerent nexus.

The application of another set of norms – international human rights law – to alleged interstate cyber operations is also theoretically possible in respect of cyber operations, which, inter alia, can intrude into privacy, freedom of expression and association (following the concept of 'human rights online').[109] However, this is dependent on the extent to which the norms of the human rights treaties[110] can be applied extraterritorially.[111] Since the UN Human Rights Committee[112] and later the ICJ[113] 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[114] and the European Court of Human Rights (ECtHR) has elaborated spatial (control over the territory or a limited space[115]) and personal approaches (control

[107] Brian J Egan, 'Remarks on International Law and Stability in Cyberspace', speech at Berkeley Law School, 10 November 2016, https://2009-2017.state.gov/s/l/releases/remarks/264303.htm.

[108] International Committee of the Red Cross, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law', 46–64, https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf; another view of the number of key elements of the 'direct participation in hostilities' is represented in HCJ 769/02 *Public Committee Against Torture in Israel and Palestinian Society for the Protection of Human Rights and the Environment v Israel and Others*, ILDC 597 (IL 2006) [2006] (*Targeted Killing*) para 39.

[109] UNGA Res 68/167, The Right to Privacy in the Digital Age (18 December 2013), UN Doc A/RES/68/167.

[110] International Covenant on Civil and Political Rights (entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17; European Convention for the Protection of Human Rights and Fundamental Freedoms (entered into force 3 September 1953) 213 UNTS 222 (ECHR) art 8.

[111] Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 *Harvard International Law Journal* 81, 120–30.

[112] UN Commission on Human Rights, General Comment No 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant (26 May 2004), UN Doc CCPR/C/21/Rev.1/Add.13, para 10.

[113] ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion [2004] ICJ Rep 136, [108], [111].

[114] ICCPR (n 110) art 2(1).

[115] ECtHR, *Loizidou v Turkey*, App No 15318/89, 23 March 1995, para 62; ECtHR, *Al-Saadoon and Mufdhi v United Kingdom*, App No 61498/08, 4 October 2010, paras 86–89.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

and authority over the individuals[116]) to the notion of 'jurisdiction',[117] contained in the Convention on the Protection of Human Rights and Fundamental Freedoms (ECHR), it is possible to extend the application of these treaties to extraterritorial modes of data interception.[118] At least three cases adjudicated by the ECtHR prove that this is not a purely hypothetical scenario: *Weber and Saravia v Germany*,[119] *Liberty v United Kingdom*,[120] and *Big Brother Watch and Others v United Kingdom*.[121]

Nonetheless, extending 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 given by the ECtHR Chambers in 2018 in two cases – *Centrum för Rättvisa v Sweden*[122] and *Big Brother Watch and Others v United Kingdom*[123] – acknowledged that mass surveillance per se does not violate the ECHR. 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' that states enjoy in choosing 'how best to achieve the legitimate aim of protecting national security'.[124] 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 regulation of the mass interception of data.[125] On 6 October 2020 the Grand Chamber of the Court of Justice of the European Union (CJEU) delivered two judgments on requests for preliminary rulings in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* and *La Quadrature du Net and Others v Premier Ministre and Others*. The Court in these cases found that the general and indiscriminate retention and transmission of traffic data by providers of electronic communications services to a state authority violated EU law.[126]

[116] ECtHR, *Al-Skeini and Others v United Kingdom*, App No 55721/07, 7 July 2011, paras 138–140; ECtHR, *Jaloud v The Netherlands*, App No 47708/08, 20 November 2014.

[117] ECHR (n 110) art 1.

[118] Milanovic (n 111) 129.

[119] ECtHR, *Weber and Saravia v Germany*, App No 54934/00, 29 June 2006.

[120] ECtHR, *Liberty and Others v United Kingdom*, App No 58243/00, 1 July 2008.

[121] ECtHR, *Big Brother Watch and Others v United Kingdom*, App Nos 58170/13, 62322/14 and 24960/15, Grand Chamber, 25 May 2021.

[122] ECtHR, *Centrum för Rättvisa v Sweden*, App No 35252/08, 19 June 2018, para 112. See also Asaf Lubin, 'Legitimizing Foreign Mass Surveillance in the European Court of Human Rights', *Just Security*, 2 August 2018, https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights.

[123] *Big Brother Watch and Others v United Kingdom* (n 121) para 340.

[124] ibid.

[125] At the request of the applicants, the judgments in *Centrum för Rättvisa* and *Big Brother Watch* have been referred to the Grand Chamber, https://hudoc.echr.coe.int/eng-press?i=003-6321717-8260093.

[126] CJEU, Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, Request for a Preliminary Ruling from the Investigatory Powers Tribunal

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

However, according on the judgment of the ECtHR Grand Chamber, the enhanced level of international protection of privacy can remain applicable only for the 27 member states of the EU.

Against the backdrop of the problematic application of the *lex lata* non-cyber-specific provisions, the lawmaking path to concretise how international law applies to cyberspace does not currently play a significant role. First, the overwhelming majority of states at present prefer not to create any new legally binding instruments.[127] Explicitly articulated grounds for this include references to the sufficiency of the current 'strategic framework' for regulating the cyber sphere[128] or to the danger that the creation of new legally binding instruments will undermine or create uncertainty in respect of existing instruments,[129] lack of state practice[130] or consensus among states,[131] or the lengthy character of international lawmaking, which contrasts with the speed of technological developments.[132] Only a minority of states preferred lawmaking,[133] some of which did so with the reservation that they consider the development of new binding norms as a medium to long-term objective.[134]

Secondly, standard setting – which is a mainstream track at this stage should we consider the content of the standards endorsed by the UN General Assembly, both in its initial (11 non-binding norms of responsible state behaviour)[135] and in its extended (13 norms)[136] version – has not brought any 'added value' to the qualification of malicious cyber acts compared with existing rules.[137] This standard-setting track may be important and justified

(London), Judgment, 6 October 2020, ECLI:EU:C:2020:790; CJEU, Joined Cases C-511/18, C-512/18 and C-520/18 *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, ECLI:EU:C:2020:791.

[127] François Delerue, 'Reinterpretation or Contestation of International Law in Cyberspace?' (2019) 52 *Israel Law Review* 295, 315–16.

[128] EU statement, Portugal joined: OEWG (n 47) 9 and 10 September 2019.

[129] Bulgaria; Italy: OEWG (n 47) 9 September 2019.

[130] Israel: OEWG (n 47) 11 September 2019.

[131] UK: OEWG (n 47) 12 September 2019.

[132] US: OEWG (n 47) 12 September 2019, 1st subs Session; Singapore, UK, Australia: OEWG (n 47) 11 February 2020.

[133] The necessity for lawmaking was expressed by Algeria, the CARICOM group, Nigeria, Russia and the Syrian Arab Republic: OEWG (n 47) 9–11 September 2019.

[134] South Africa and Chile: OEWG (n 47) 9 and 12 September 2019; Brazil: OEWG (n 47) 12 February 2020.

[135] The GGE Report of 2015 (n 54) contains 11 'norms, rules and principles for the responsible behaviour of states', which were endorsed by consensus by the UN General Assembly (UNGA Res 70/237 (n 60) para 2(a)) and their content was almost not disputed at the substantial meetings of the OEWG in 2019 and 2020.

[136] The UN General Assembly in the resolution on the creation of the OEWG in 2018 added three new norms to the existing list and altered a few aspects of the GGE formulations. However, it was adopted by vote, not by consensus, with 119 votes in favour, 46 against and 14 abstentions: UNGA Res 73/27, Developments in the Field of Information and Telecommunications in the Context of International Security (5 December 2018), UN Doc A/RES/73/27.

[137] Against this background it is revealing that during the OEWG sessions only Egypt explicitly suggested transforming the GGE recommendations to legally binding provisions, and the Philippines

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

as a political instrument to reaffirm the applicability of international law to cyber-specific interstate 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 interstate 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'.[138]

Thirdly, in interstate relations, states that suffer 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',[139] 'cyberattacks with a significant effect which constitute an external threat to the [European] Union or its Member States'[140] or by referring to international law in general terms. These terms are far from being a concrete legal qualification – for example, by designating such incidents as a 'flagrant disregard of international law'[141] or 'international norms';[142] or pointing out that they undermine 'established international norms of behavior'.[143] Two cases can be regarded as exceptions to the rule: (i) Georgia alleged that the cyber attacks of 2019 infringed its sovereignty,[144] and (ii) the US declared in April 2021 that cyber operations allegedly conducted by the Russian government were 'efforts' 'to violate well-established principles of international law, including respect for the territorial integrity of states'.[145]

2.2. 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, in contrast to the primary rules, does not encounter any principal objections from states, the challenge lies in the necessity to attribute malicious cyber acts committed by individuals to a particular state under international rules of customary law, which also goes in conjunction with a duty to reach any of the standards of proof

expressed concern about the non-binding character of their nature and reduced options for compliance and enforcement.

[138] GGE Report 2015 (n 54) para 10.

[139] 'Poroshenko: Russia Unleashed Cyber War against Ukraine', *The Segodnya*, 29 December 2016 (in Russian), https://politics.segodnya.ua/politics/poroshenko-rossiya-razvyazala-kibervoynu-protiv-ukrainy-784445.html.

[140] Council Implementing Regulation 2020/1536 (n 25).

[141] UK National Cyber Security Centre, 'UK Exposes Russian Cyber Attacks', 4 October 2018, https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks.

[142] Kerry (n 5).

[143] The White House, 'Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment', 29 December 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

[144] Statement of the Ministry of Foreign Affairs of Georgia, 20 February 2020, @MFAgovge, Twitter, 20 February 2020, https://twitter.com/MFAgovge/status/1230479514431631363?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1230479514431631363%7Ctwgr%5E7028efa2532a3132db27d25535179e56c5bc4434%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fcivil.ge%2Farchives%2F339589.

[145] Executive Order No 14024, 86 FR 20249, 15 April 2021.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

applicable in international law.[146] Taking into account the specificity of cyber infrastructure,[147] it might be of no surprise that states hastened to safeguard the notion that '[they] 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'.[148]

After publicly articulated, although later disavowed, allegations of Russian involvement in the Estonian cyber attacks of 2007,[149] 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 that imposed sanctions pointed to three states: North Korea,[150] Russia[151] and

[146] Marco Roscini, 'Evidentiary Issues in International Disputes related to State Responsibility for Cyber Operations' (2015) 50 *Texas International Law Journal* 233, 248–54.

[147] See Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace' (2018) 67 *International & Comparative Law Quarterly* 645, 648; Anders Henriksen, 'Lawful State Responses to Low-Level Cyber-Attacks' (2015) 84 *Nordic Journal of International Law* 323, 340–42.

[148] GGE Report 2015 (n 54) para 13(b), endorsed by the General Assembly: UNGA Res 70/237 (23 December 2015) (n 60).

[149] 'Estonian Links Moscow to Internet Attack', *The New York Times*, 18 May 2007, https://www.nytimes.com/2007/05/18/world/europe/18estonia.html.

[150] North Korea was designated by the US as a state that organised the cyber attack on Sony Pictures (press statement of John Kerry (n 5)) and by the UK, the US, Australia, Canada, New Zealand, and Japan as responsible for the WannaCry ransomware (The White House, 'Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea', 19 December 2017, https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917; US Department of the Treasury (n 23).

[151] Russian intelligence agencies or state officials were blamed for a number of attacks, including the cyber operation against SolarWinds Co and its clients, which included US state agencies (US Department of the Treasury (n 15)), the hacking of the German Bundestag in 2015 (Council Implementing Regulation 2020/1536 (n 25), UK Foreign, Commonwealth and Development Office (n 25)), meddling in the US presidential elections in 2016 (US Department of the Treasury (n 11)), Petya and NotPetya ransomwares (US Department of the Treasury (n 22), EU Regulation 2020/1125 (n 22)). 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 (GRU): the 2017 BadRabbit ransomware, hacking and release of the medical files of the WADA in 2016, the 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 in the same year. In 2020 Georgia, the US and the UK exposed Russia (or, precisely, the GRU) as being responsible for a number of significant cyber attacks against Georgia in October 2019, which disrupted the operations of several thousand Georgian government and privately run websites and interrupted the broadcast of at least two major television stations (Statement of the Ministry of Foreign Affairs of Georgia (n 144); Michael R Pompeo, US Secretary of State, 'The United States Condemns Russian Cyber Attack Against the Country of Georgia', 20 February 2020, https://ge.usembassy.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia-february-20; UK Foreign and Commonwealth Office, 'UK Condemns Russia's GRU over Georgia Cyber Attacks', 20 February 2020, https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks). Finally, the US claimed that '[b]etween approximately August 2020 and November 2020, state-sponsored Iranian cyber actors executed an online operation to intimidate and influence American voters, and to undermine voter confidence

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

Iran.[152] Although the EU also imposed sanctions against Chinese nationals for Operation Cloud Hopper in 2020, it did not officially link them to the state.[153]

Until now no state has ever officially called another state responsible for an international cyber operation. The approach taken by states regarding the attribution of cyber operations is typically formulated very cautiously. Let us take an example of the 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 behaviour without using the language of the law of international responsibility.[154] Although the United States and Canada called on Russia to cease such behaviour, they did not qualify such behaviour legally as a breach of international law.[155] The US pointed to the Russian Foreign Intelligence Service (SVR) in one of the recent cases of sanctions, calling it 'the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures'.[156] The EU, joining the condemnation campaign, expressed its concern and that of its Member States about the cyber attack, without saying a word about Russian involvement,[157] or, without its own assessment, carefully expressed solidarity with the US on the impact of the 'the SolarWinds cyber operation, which, the United States assesses, has been conducted by the Russian Federation'.[158]

The current trend of 'cautious attribution' is characterised by two main features. First, public exposure of the organiser 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 that meets at least one of the standards that may be applicable under international law. For

and sow discord, in connection with the 2020 U.S. presidential election' (US Department of the Treasury (n 10)).

[152] 'In October 2012, hackers from Iran's Revolutionary Guard carried out cyber-attacks against oil and gas companies in Saudi Arabia and the Gulf': The Embassy of the Kingdom of Saudi Arabia, 'Fact Sheet: Iran's Record in Supporting Terrorism and Extremism', 19 January 2016, https://www.saudiembassy.net/news/fact-sheet-irans-record-supporting-terrorism-and-extremism.

[153] EU Regulation 2020/1125 (n 22).

[154] Statement of the Ministry of Foreign Affairs of Georgia (n 144); UK Foreign and Commonwealth Office (n 151).

[155] Pompeo (n 151); Global Affairs Canada, 'Canada Condemns Russia's Malicious Cyber-Activity Targeting Georgia', 20 February 2020, https://www.canada.ca/en/global-affairs/news/2020/02/canada-condemns-russias-malicious-cyber-activity-targeting-georgia.html.

[156] The White House, 'Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government', 15 April 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government.

[157] Council of the EU, 'Declaration by the High Representative on behalf of the European Union: Call to Promote and Conduct Responsible Behavior in Cyberspace', 21 February 2020, 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.

[158] Council of the EU, 'Declaration by the High Representative on behalf of the European Union Expressing Solidarity with the United States on the Impact of the SolarWinds Cyber Operation', 15 April 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

instance, whereas the UK National Cyber Security Centre relied on the assessment 'with high confidence' that the GRU was 'almost certainly responsible', which is '95%+' for a list of cyber operations,[159] this evidence remained undisclosed.[160] Thus, 'cautious attribution' reflected a 'name and shame' mode and did not represent attribution for the purposes of calling a particular state responsible.

To sum up, the legal considerations outlined in this part of the article 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. While the instruments provided by international law either cannot be used at all or can hardly be used, unilateral sanctions taking the form of retorsion remain one of the accessible instruments for victim states. When imposing national or supranational sanctions, states are not bound by the standards of proof and the duty to reveal evidence set forth by international law.[161] The scope of cyber acts that trigger sanctions can be extended to operations which are not necessarily linked to particular foreign states and lie below the threshold of behaviour outlawed at the international level.[162] Finally, sanctions can be taken in respect of malicious cyber operations that did not necessarily affect the target state; this significantly extends opportunities for a reaction in comparison with the *locus standi* under the law of international responsibility, providing non-injured states with the right to react only in the case of a violation of obligations of an *erga omnes* or *erga omnes partes* character.[163]

[159] UK National Cyber Security Centre (n 141).

[160] Ministry for Foreign Affairs of the Russian Federation, 'Comment by the Information and Press Department on Accusations against Russia of Carrying Out Large-Scale Cyberattacks on Georgian Websites', 20 February 2020, https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4050783.

[161] Council Regulation (EU) 2019/796 requires grounds to be given for listing in the sanctions list (art 14), but does not identify the standard of proof or require the disclosure of evidence; the burden of proof is placed on the sanctioned person or entity, which can present 'observations' post factum; should the Council find that there is new evidence, the decision can be reviewed: Council Regulation (EU) 2019/796 of 17 May 2019 concerning Restrictive Measures against Cyber Attacks Threatening the Union or its Member States [2019] OJ L 129 I/1, arts 14, 13(1)–(3)). The (US) Countering America's Adversaries Through Sanctions Act (HR 3364, Pub L 115–44 (2017)) (CAATSA) does not mention any such standard or duty in respect of cyber-related sanctions at all.

[162] The cyber-related sanctions regime under CAATSA (ibid s 224(a)(1)) 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 Council Regulation (EU) 2019/796 (ibid arts 1(1), (3), (4)), 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'.

[163] See Samuli Haataja, 'Cyber Operations and Collective Countermeasures under International Law' (2020) *Journal of Conflict and Security Law* 33.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

3. The US, the EU and the UK 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 United States under Executive Order 13687 as a result of the Sony Pictures hacking attack.[164] Three months later, on 1 April 2015, President Obama issued Executive Order 13694, which declared a national emergency to address 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'.[165] This Order provided for blocking property located in the US which belongs to persons engaged in or responsible for significant malicious cyber activities; denial of access to US financial markets; prohibiting the provision of funds, goods or services to the sanctioned persons; and denial of entry into the US.[166] This Executive Order was amended in 2016 to impose sanctions for meddling in the 2016 US presidential elections on two Russian intelligence services, four members thereof, and three companies.[167]

The US cyber-related sanction regime was further codified and supplemented by the Countering America's Adversaries Through Sanctions Act (CAATSA) of 2017. CAATSA imposes new sanctions in respect of Iran, Russia and North Korea, and provides for sanctions related to Russian 'activities undermining cybersecurity'.[168] The scope of sanctions contemplated by CAATSA is similar to those authorised in the Executive Orders, although the wording of these enactments 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 Biden administration tightened the cyber-related sanctions regime with regard to Russia. Executive Order 14024 and the relevant directive of the Treasury's Office of Foreign Assets Control[169] provide for the new sanctions designations and the new prohibitions alongside traditional property blocking

[164] Executive Order No 13687 (80 FR 817, 2 January 2015), which forms part of a comprehensive sanctions package against North Korea in conjunction with, inter alia, Executive Order No 13722 (81 FR 14941, 15 March 2016) issued in relation to North Korean nuclear and missile programmes. Executive Order No 13722 was also employed to designate North Korean hacking groups with regard to the WannaCry attack, although this Order is included in the North Korea-related sanctions programme (aimed at preventing the proliferation of weapons of mass destruction) rather than the cyber-related sanctions programme.

[165] Executive Order No 13694, 80 FR 18077, 1 April 2015.

[166] ibid ss 1–4.

[167] Executive Order No 13757, 82 FR 1, 28 December 2016.

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

[169] US Department of the Treasury, Office of Foreign Assets Control, Directive 1 under Executive Order of 15 April 2021 'Blocking Property with respect to Specified Harmful Foreign Activities of

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

and travel bans. US financial institutions are prohibited from (i) participating in the primary market for ruble or non-ruble denominated bonds issued after 14 June 2021 by Russia's Central Bank, National Wealth Fund, and Ministry of Finance; and (ii) lending ruble or non-ruble denominated funds to these three Russian entities.[170] The measure, however, does not restrict transactions on the secondary market with bonds issued by the named Russian entities.[171]

The EU cyber-related sanctions[172] regime is based on a Council Decision[173] and the corresponding EU Regulation of 17 May 2019,[174] which is an act of direct application for all member states. The designation and delisting of persons under sanctions is exercised by the Council[175] in order 'to ensure consistency with the process for establishing, amending and reviewing'[176] the annex in which the sanctioned persons are named. The Council is to review the sanction list at least once a year.[177] Member states specify national authorities that are entitled to authorise, under certain conditions, the release of certain frozen funds and economic resources,[178] and exchange information related to the implementation of the Regulation with each other and with the EU Commission.[179] 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'.[180] The legal nature of these penalties can be administrative, civil or criminal, with a range of measures from fines to imprisonment.[181]

---

the Government of the Russian Federation', https://home.treasury.gov/system/files/126/sovereign_debt_prohibition_directive_1.pdf.

[170] ibid.

[171] US Department of the Treasury, 'Frequently Asked Question, Russian Harmful Foreign Activities Sanctions, FAQ 889', https://home.treasury.gov/policy-issues/financial-sanctions/faqs/889.

[172] Although the EU legislation employs the term 'restrictive measures' rather than 'sanctions', in their economic nature the former are identical to the latter; therefore, in this article these terms are used as synonyms.

[173] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning Restrictive Measures against Cyber Attacks Threatening the Union or its Member States [2019] OJ L 129 I/13, art 1(1). In May 2020 the Council decided to extend the cyber sanctions regime for a year (Council of the EU, 'Council Extends Cyber Sanctions Regime until 18 May 2021', 14 May 2020, https://europa.eu/!jP36Mf) and, in May 2021, for another year until May 2022 (Council of the EU, 'Cyber-Attacks: Council Prolongs Framework for Sanctions for Another Year, 17 May 2021, https://europa.eu/!CK67uW). In May 2022 the cyber sanctions regime was extended for three years with immediate effect to indicate 'the strong EU commitment to enhance its resilience and ability to prevent, discourage, deter and respond to cyber threats and malicious cyber activities in order to safeguard European security and interests' (Council of the EU, 'Cyber-Attacks: Council Extends Sanctions Regime until 18 May 2025', https://europa.eu/!qfDkPr).

[174] Council Regulation (EU) 2019/796 (n 161)

[175] ibid art 13(1).

[176] ibid preambular para (4).

[177] ibid art 13(4).

[178] ibid arts 4(1), 5(1), 6(1).

[179] ibid art 12(1).

[180] ibid art 15(1).

[181] David Savage, 'EU Sanctions Enforcement', in *The Guide to Sanctions – First Edition*, https://globalinvestigationsreview.com/benchmarking/the-guide-to-sanctions-first-edition/1230031/eu-sanctions-enforcement.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

The adoption of EU Regulation 2019/796 of 17 May 2019 was specifically promoted by the UK[182] and the Netherlands,[183] 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.[184] The measures that the EU may impose are restricted to preventing the entry of the sanctioned persons into territories of EU member states and the freezing of assets.

The UK implemented the EU sanctions until Brexit, and replaced the EU sanctions regime with its own regime on the exit date when the Cyber (Sanctions) (EU Exit) Regulations 2020 fully came into force.[185] The power to designate persons involved in cyber activities is vested in the Secretary of State.[186] Similar to the EU regime, the UK Cyber Regulations 2020 contemplate financial sanctions (asset freezing, prohibiting dealing with sanctioned persons and making funds available to them),[187] as well as immigration sanctions (travel bans and the cancellation of effective permission to stay in the UK).[188]

All three 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. The regimes contain rather vague and broad definitions of the cyber activities that trigger sanctions and of the criteria for designating persons on whom sanctions should be imposed. At the same time, 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[189] – is wider than the European approach. EU Regulation 2019/796 confines 'cyber-attacks' to those that 'have (or potentially may have) a significant effect on the EU or its member states, in

[182] On the application of the EU sanctions regime after Brexit see Erica Moret and Fabrice Pothier, 'Sanctions After Brexit' (2018) 60(2) *Survival* 179.

[183] See Ministry of Justice and Security, 'Cyber Security Assessment Netherlands 2019', https://www.thehaguesecuritydelta.com/media/com_hsd/report/255/document/CSBN2019-EN-def-Web-01-tcm32-405804.pdf; or Shannon Vavra, 'Dutch Intelligence Warns of Escalating Russian, Chinese Cyberattacks in the Netherlands', *Cyberscoop*, 1 May 2019, https://www.cyberscoop.com/dutch-intelligence-warns-escalating-russian-chinese-cyberattacks-netherlands. With regard to the UK see Department for Digital, Culture, Media and Sport, 'Cyber Security Breaches Survey 2019', https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019; or 'More than Half of British Firms "Report Cyber Attacks in 2019"', *BBC News*, 23 April 2019, https://www.bbc.com/news/business-48017943; 'Russia Cyber-Plots: US, UK and Netherlands Allege Hacking', *BBC News*, 4 October 2018, https://www.bbc.com/news/world-europe-45746837.

[184] Erica Moret and Patryk Pawlak, 'The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?', 12 July 2017, 1, https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime.

[185] Cyber (Sanctions) (EU Exit) Regulations 2020, SI 2020/597 (UK Cyber Regulations 2020); and Sanctions (EU Exit) (Miscellaneous Amendments) (No 4) Regulations 2020, SI 2020/951.

[186] UK Cyber Regulations 2020, ibid reg 5.

[187] ibid regs 11–15.

[188] ibid reg 17.

[189] CAATSA (n 161) s 224(a)(1).

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

particular to their critical infrastructure, public services (transportation, banking, healthcare, drinking water supply and others), critical state functions such as defence and governance'.[190] The understanding of cyber-enabled actions is very close in EU Regulation 2019/796 and the UK Cyber Regulations 2020 (access to information systems, interference with information systems, data interference, and data interception).[191] However, the EU regulation qualifies such actions as cyber attacks if they originate or are carried out from outside the EU and harm the EU or its member states,[192] while the UK regulations adopt a broader approach: cyber activities are considered a cyber attack if they have consequences not only in the UK but also in any other country, or affect 'a significant number of persons in an indiscriminate manner'.[193] Contrary to the US and the EU regimes, the UK Cyber Regulations 2020 do not respond explicitly to external threats and do not focus on the condition that the malicious activities should be conducted or controlled from outside the country.

What differentiates the EU cyber-related sanctions is the procedure for imposing sanctions. US sanctions can be enabled by a stroke of the US President's pen under CAATSA, and the designation of persons sanctioned under Executive Orders falls within the competence of the Secretary of the Treasury. UK sanctions are imposed by the relevant Secretary of State. 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.[194] 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 the imposition of sanctions, considering their political significance, is often motivated by economic ties with the state from which the malicious cyber-enabled actions allegedly originate.

A comparison of cyber-related sanctions with other multilateral and unilateral sanction regimes reveals a number of similarities, as well as a few differences. The econometric studies of smart sanctions reveal that the key determinants of their effectiveness are the target's costs of imposing the sanction, the salience of the issue at stake for the target, the multilateral or unilateral nature of the sanctions regime, endorsement of the sanctions by an international institution, and the institutional structure of the target state and political vulnerability of its regime.[195] According to these parameters, sanctions in response to cyber attacks possess a combination of features that distinguish them from other regimes. In particular, the existence and amount

[190] Council Regulation (EU) 2019/796 (n 161) arts 1(1), (3), (4).

[191] ibid art 1(3); UK Cyber Regulations 2020 (n 185) reg 4(3).

[192] Council Regulation (EU) 2019/796 (n 161) arts 1(1), (2).

[193] UK Cyber Regulations 2020 (n 185) reg 4(2).

[194] Council Decision (CFSP) 2019/797 (n 173) 13–19.

[195] See Daniel W Drezner, 'Sanctions Sometimes Smart: Targeted Sanctions in Theory and Practice' (2011) 13 *International Studies Review* 99; Navin A Bapat and T Clifton Morgan, 'Multilateral versus Unilateral Sanctions Reconsidered' (2009) 53 *International Studies Quarterly* 1092; Sean M Bolks and Dina Al-Sowayel, 'How Long Do Economic Sanctions Last? Examining the Sanctioning Process through Duration' (2000) 53(2) *Political Research Quarterly* 241.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

of costs associated with designing, implementing, monitoring, reflecting and correcting sanctions determine the fact that only significant trespassing and cyber threats are penalised, although the total burden of all threats is felt by society. Therefore, 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.

Estimations of costs incurred by targets and senders vary (they refer mostly to comprehensive rather than smart sanctions, and present significantly different results). The western economic sanctions imposed on Russia as a result of the Ukraine crisis were particularly subject to calculation. In November 2014, Anton Siluanov, Russia's Finance Minister at the time, estimated Russia's annual losses as a result 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.[196] The agrifood embargo introduced by Russia as a 'counter-sanction' and the decline in volume of Russian–European trade caused sufficient damage to the EU and the economies of some of its member states: the estimation carried out by WIFO in 2016 indicates a sanction-induced decline of EU exports to Russia in 2015 of about EUR 20 billion, or a 0.2 per cent loss in total value added (EUR 17.6 billion) and employment (400,000 jobs) for the EU as a whole.[197] Estimating the impact of the economic sanctions on the economies of the sender and target is challenging, as it requires distinguishing the sanction-induced economic costs from those caused by other factors (such as oil prices).

At the same time, the imposition of sanctions in response to cyber attacks so far seems not to have led to substantial costs for the target states. When sanctions are imposed in the coercive logic, the key benefit for the sender is a change in the target's behaviour in line with the sender's demands (the target's 'costs' – economic losses – are not necessary 'benefits' for the sender). In the case of constraining sanctions, the costs that the target incurs in carrying 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 behaviour of Russia in cyberspace. The absence of any evidential signs of such an influential role of cyber-related sanctions inclines towards the conclusion of their predominantly signalling function, as will be discussed below.

There are some similarities between cyber-related sanctions and other sanctions regimes. By their nature, the US and UK regimes are unilateral; the EU regime represents one of a multilateral, institutionalised nature. At the same time, the possibility of the US imposing secondary sanctions on those who violate the primary sanctions (even if this is a purely hypothetical

[196] 'Russia Puts Losses from Sanctions, Cheaper Oil at up to $140 Billion per Year', *Reuters*, 24 November 2014, https://www.reuters.com/article/uk-russia-economy-oil-sanctions-idUKKCN0J80P720141124.

[197] 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, EP/EXPO/B/INTA/2017/11, 40, https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603847/EXPO_STU(2017)603847_EN.pdf.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

scenario), together with an overlap between the US and the EU sanctions regimes in response to cyber attacks, allows the former to benefit from the advantages of both unilateral and multilateral formats. What also significantly distinguishes this type of targeted sanction is the salience of the issue at stake. The ability of target states to conduct covert cyber operations, taking into account their low costs and significant effects, makes the salience extremely high.

4. How to measure the effectiveness of sanctions

Since January 2015, the US, and later the EU and the UK, have sanctioned more than 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 six 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.[198] Realising 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 two different approaches: Mancur Olson's theory of groups, and Francesco Giumelli's comprehensive analytical framework for the assessment of sanctions.

4.1. Identifying the goals of the imposition of cyber-related sanctions

Before proceeding to the evaluation of the effectiveness of sanctions as a response to cyber operations, it is instructive to address the objectives of sanctions, of which there are three generally acknowledged goals: (i) *coercion* (modifying the target's behaviour); (ii) *constraint* (reducing the target's capacity to take discretionary action); and (iii) *signalling* and/or *stigmatising* (notifying the target and, in some cases, third parties of the sender's intended course of action if the target continues the objectionable behaviour).[199] The

[198] Simon Chesterman and Béatrice Pouligny, 'Are Sanctions Meant to Work? The Politics of Creating and Implementing Sanctions through the United Nations' (2003) 9 *Global Governance* 503; William Kaempfer and Anton D Lowenberg, 'The Political Economy of Economic Sanctions' (2007) 2 *Handbook of Defense Economics* 868; Susan Hannah Allen, 'The Domestic Political Costs of Economic Sanctions' (2008) 52 *Journal of Conflict Resolution* 916. A separate strand of the literature examines the target states' political regime and potential correlation between the type of regime and effectiveness of sanctions against the target; see Abel Escribà-Folch and Joseph Wright, *Foreign Pressure and the Politics of Autocratic Survival* (Oxford University Press 2015); Dursun Peksen, 'Autocracies and Economic Sanctions: The Divergent Impact of Authoritarian Regime Type on Sanctions Success' (2019) 30 *Defence and Peace Economics* 253.

[199] Iana Dreyer and José Luengo-Cabrera, 'Introduction' in Iana Dreyer and José Luengo-Cabrera (eds), *On Target? EU Sanctions as Security Policy Tools*, Report No 25 (EU Institute for Security Studies 2015) 7, https://doi.org/10.2815/710375.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

assessment of their effectiveness consists of the analysis of how they achieve the goal(s) intended by the sender.

Both the policymaking on general (non-cyber) sanctions and the scientific discussion around such political responses are based largely on the assumption that the main purpose of sanctions is to change the target's behaviour.[200] While the US cyber-related sanctions instruments (namely, Executive Order 13694, Executive Order 14024, CAATSA) do not indicate any objectives in implementing sanctions, except for the necessity to respond to cyber incidents that threaten national security, political documents issued in relation to sanctions imposition in some cases shed light on the sender's intentions. Thus, the Fact Sheet published by the White House in connection with the adoption of Executive Order 14024 indicates the explicit intention of the Biden administration to '*signal* that the United States will impose costs in a strategic and economically impactful manner on Russia if it continues or escalates its destabilizing international actions'.[201] The EU Council states in its Sanctions Guidelines a different aim: to coerce the target to change its objectionable course of action.[202] According to the Council, the EU imposes restrictive measures 'to bring about a change in policy or activity by the target country, part of the country, government, entities or individuals, in line with the objectives set out in the [Common Foreign and Security Policy] Council Decision'.[203] The particular legal instruments that implement sanctions are intended, in general, to incentivise the required change in the target's policy or activity and, at the same time, clearly indicate the specific objective of the imposed restrictive measures in line with the general goal of coercion.[204] Interestingly, the EU Regulation 2019/796 indicates the necessity 'to deter and respond to cyber-attacks' as the goals of establishing the framework for EU targeted cyber security-restrictive measures.[205] The goals of the EU cyber-related sanctions regime, at least as they are stated in the applicable policy tools, are not limited to coercion but include also constraining and deterrent effects. The UK Cyber Regulations 2020 do not specify the goal of sanctions imposition, while the relevant guidance rather cautiously formulates it as 'prevention of relevant cyber activity'.[206]

Although coercion could be among the major reasons for the imposition of sanctions, travel restrictions imposed on particular individuals or limitations on commercial relations with them have a limited coercive impact on the

[200] Thomas J Biersteker and Peter AG van Bergeijk, 'How and When Do Sanctions Work? The Evidence', in Dreyer and Luengo-Cabrera (n 199) 17, 18.

[201] The White House (n 156) (emphasis added).

[202] Council of the EU, 'Guidelines on Implementation and Evaluation of Restrictive Measures (Sanctions) in the Framework of the EU Common Foreign and Security Policy', Doc 5664/18, 4 May 2018, https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf.

[203] ibid para 4.

[204] ibid paras 4, 5.

[205] Council Regulation (EU) 2019/796 (n 161) preambular paras 1 and 2.

[206] UK Foreign, Commonwealth & Development Office, 'Statutory Guidance – Cyber Sanctions: Guidance', 3 November 2020, https://www.gov.uk/government/publications/cyber-sanctions-guidance/cyber-sanctions-guidance.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

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, the EU or the UK, or participate in commercial activities with the relevant counterparties.[207] It is questionable whether Russia, China, Iran or North Korea (even if we presume that these states actually stood behind the relevant cyber operations) would abstain from further acts of that nature because of targeted sanctions imposed on a number of individuals.

The objective of constraining the targets in their capacity to engage in further malicious cyber-enabled activities can be achieved if the sanctioned persons are deprived of assets required for their activities or continuing their malicious activities becomes too costly for them. Raising awareness of the target's cyber-enabled activities probably contributes to the constraining effect of sanctions. When imposing sanctions on the Iranian cyber threat group APT39 in September 2020, the US Department of the Treasury and FBI advisory released particular sets of malware employed by a front company, allegedly controlled by the Iranian Ministry of Intelligence and Security, to conduct cyber intrusions against foreign citizens, companies, institutions and governments globally.[208] By making the code public, the US authorities aimed to hinder 'the ability [of the Iranian Ministry of Intelligence and Security] to continue their campaign, ending the victimization of thousands of individuals and organizations around the world'.[209] That said, none of the episodes of sanctions analysed contemplates the seizure of computers or server systems for obvious reasons: in the 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 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, because of restrictions in national legislation). The denial of access to foreign capital, therefore, would not significantly 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, as well as 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 signalling and stigmatising 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,

[207] Julia Edwards and Jason Lange, 'US Slaps More Sanctions on North Korea after Sony Hack', *Reuters*, 4 January 2015, https://www.reuters.com/article/us-northkorea-cyberattack-sanctions-idUSKBN0KB16U20150104 ('It's not as if they [the sanctioned North Korean individuals] travel a lot abroad to western Europe or the United States ... They don't have billions of dollars in western banks', said Joel Wit of 38North, part of the US Korea Institute at Johns Hopkins University in Washington).

[208] US Department of State (n 9).

[209] ibid.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

statements at various levels. 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',[210] while 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 behaviour, and interfere with democratic governance'.[211] Moreover, the stigmatising targeted sanctions may precede prosecution, including criminal, under the national law of the state with which the sanctioned individual is associated. Thus, in January 2022 the Russian agency FSB dismantled REvil,[212] a notorious hacking group believed to mastermind ransomware hacks against Colonial Pipeline and Kasey, which caused the imposition of US sanctions.[213] The arrest of 14 members of the hacking group followed several requests by the US administration, and President Biden's appeal to President Putin to cooperate in fighting cyber attacks and ransomware when the two met in Geneva in June 2021.[214]

The coercive and constraining effects of cyber-related sanctions are limited, which in certain cases is acknowledged by the states that impose the sanctions. Following a massive cyber attack against multiple US federal agencies from March to December 2020,[215] allegedly originating from Russia,[216] US President-elect Biden's team called for a 'strong response' that should go 'beyond sanctions'.[217] The choice of the new administration, apart from financial sanctions, could include revenge cyber attacks on Russian institutions and potentially cut off Russia from the SWIFT system of international funds transfers and bank communication.[218]

[210] 'Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking', *The Guardian*, 30 December 2016, https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack.

[211] 'Obama Expels 35 Russian Diplomats, Accuses Russia of Meddling in Election', *Euronews*, 29 December 2016, https://www.euronews.com/2016/12/29/washington-gives-35-russian-diplomats-72-hours-to-leave-the-us-in-response-to.

[212] Ivan Nechepurenko, 'Russia Says It Shut Down Notorious Hacker Group at U.S. Request', *The New York Times*, 14 January 2022, https://www.nytimes.com/2022/01/14/world/europe/revil-ransomware-russia-arrests.html.

[213] US Department of the Treasury (n 16).

[214] Robyn Dixon and Ellen Nakashima, 'Russia Arrests 14 Alleged Members of REvil Ransomware Gang, Including Hacker U.S. Says Conducted Colonial Pipeline Attack', *The Washington Post*, 14 January 2022, https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil.

[215] Kari Paul and Lois Beckett, 'What We Know – and Still Don't – about the Worst-Ever US Government Cyber-Attack', *The Guardian*, 19 December 2020, https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government.

[216] 'Pompeo Says Russia "Pretty Clearly" behind Cyberattack, Prompting Pushback from Trump', *NPR*, 19 December 2020, https://www.npr.org/2020/12/19/948318197/pompeo-russia-pretty-clearly-behind-massive-solarwinds-cyberattack.

[217] Trevor Hunnicutt, David Lawder and Daphne Psaledakis, 'Biden's Options for Russian Hacking Punishment: Sanctions, Cyber Retaliation', *Reuters*, 20 December 2020, https://www.reuters.com/article/usa-cyber-breach-biden/bidens-options-for-russian-hacking-punishment-sanctions-cyber-retaliation-idUSKBN28U0DV.

[218] ibid.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

The limited prospects to coerce and constrain the target by way of sanctions do not mean that the policy of sanctions in response to cyber attacks is itself a failure; nor does the primary signalling role make sanctions a symbolic gesture. It is essential, however, that the assessment of sanction effectiveness is conducted with a consideration of their objectives. Research carried out by the Targeted Sanctions Consortium (TSC), headed by Thomas Biersteker, in respect of general (rather than cyber-related) sanctions, indicates that 'sanctions intended to constrain or to signal targets are nearly three times as effective (27 per cent) as sanctions intended to coerce a change in behaviour (10 per cent)'.[219] 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 objectives of sanctions should not be underestimated.

4.2. Mancur Olson's theory of groups

The theory of collective action and group behaviour developed by Mancur Olson[220] is among the most promising for the assessment of the effectiveness of sanctions. The taxonomy of groups suggested by Olson (including small and large, or 'latent', groups, depending not only on the number of their participants but also the benefit that each member obtains from the collective good and the importance of their contribution to the group objective) can be used in the context of cyber sanctions. Among 20 cases of cyber-related sanctions, there is a special group of US sanctions imposed not on perpetrators, legal entities or institutions, but on an elite group. Following the 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.[221] 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

[219] Biersteker and Van Bergeijk (n 200) 19.

[220] Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Harvard University Press 1971).

[221] Julia Ioffe, 'How Not to Design Russia Sanctions', *Atlantic*, 31 January 2018, https://www.theatlantic.com/international/archive/2018/01/kremlin-report-sanctions-policy/551921.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

the Russian government'[222] for 'profiting from' malicious cyber activities allegedly conducted by the Russian authorities.[223] The sanctioning was accompanied by harsh rhetoric: 'The Russian government operates for the disproportionate benefit of oligarchs and government elites', said US Treasury Secretary, Steven Mnuchin, in March 2018; 'Russian oligarchs and elites who profit from this corrupt system will no longer be insulated from the consequences of their government's destabilizing activities'.[224] It was openly admitted that the sanctions were 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.[225]

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 who deviate from group profit-maximising behaviour.[226] Participants of a small group have common interests, economic and social incentives, and each is aware of this commonality of interests and of the degree of their contribution towards their achievement. When the number of participants is large, and the group obtains the features of a latent group, its typical participants recognise that they cannot make a noticeable contribution to any group effort or influence the outcome in any way.[227] Consequently, they have little incentive to contribute (which constitutes the 'free rider' problem). On the contrary, there is no free rider problem in small and well-organised groups in which the members, at less cost, can observe whether any individual contributes or deviates, and impose 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.[228] These well-organised action-taking groups and subgroups have a significant advantage over the poorly organised, latent masses and have a better negotiating position.

Economic sanctions imposed on key businesspersons of Russia can be viewed in the light of Olson's theory as an attempt by the US administration

[222] John Walcott and Jonathan Landay, 'US Plans to Sanction Russian Oligarchs This Week: Sources', *Reuters*, 4 April 2018, https://www.reuters.com/article/us-usa-russia-sanctions/u-s-plans-to-sanction-russian-oligarchs-this-week-sources-idUSKCN1HB34U.

[223] US Department of the Treasury, 'Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity', 6 April 2018, https://home.treasury.gov/news/press-releases/sm0338.

[224] Lauren Gambino, 'Trump Administration Hits 24 Russians with Sanctions over "Malign Activity"', *The Guardian*, 6 April 2018, https://www.theguardian.com/us-news/2018/apr/06/trump-russia-sanctions-election-meddling-latest.

[225] ibid.

[226] See Olson (n 220) 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 a higher degree of consensus in a small (or 'privileged') group enable its members to expect that their collective needs will be met one way or another: ibid 58.

[227] ibid 50.

[228] ibid 53.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

to use financial leverage against Russian political and business elites to alter their incentives in the communication with the Russian government. The economic pressure on persons close to the Russian upper echelons is presumably based on the beliefs that (i) the sanctioned persons have 'ties' with the government and personally with the President; (ii) they represent an interest group consolidated with common economic incentives; and (iii) they influence the decision-making process in the target country.

Based on the assumption that the group can exert pressure either in favour of or against the continuation of the policy of malicious cyber activities, the sanctioning state might seek to make it more costly to support such a policy. The distinct way is to make the group face the decrease in income resulting from sanctions. There are publicly available calculations of the economic impact of sanctions on the business and wealth of targeted persons. The losses of Oleg Deripaska, a major shareholder of United Co RUSAL PLC (Rusal), one of the world's largest aluminium producers, are calculated by *Forbes* as $3.1 billion,[229] while Deripaska himself indicated losses of more than $7.5 billion, or approximately 81 per cent of his net wealth, in the lawsuit against the US Department of Treasury.[230]

That said, the assessment of the effectiveness of sanctions should not be narrowed down to numbers. Kaempfer and Lowenberg use a threshold model of collective action to examine the ways in which external economic pressure influences the political potency of elites within the target country.[231] One of the mechanisms described is an 'increase in reputational benefits awarded to individuals who support certain domestic interest groups, by increasing the effectiveness of those groups in rewarding their supporters with selective incentives' produced by foreign sanctions.[232] The post factum analysis shows that neither the elite group has rallied around the flag, nor the malicious activity in cyberspace ascribed to Russia has somewhat decreased significantly as a result of sanctioning oligarchs. It questions the extent to which the circle of businesspersons on whom sanctions were imposed actually represents part of the 'action-taking' subgroup and influences the decision-making process, as well as the capacity of sanctions to encourage opposition to the cyber-related policy, either through a decrease in income or reputational costs. Examples of elite reactions to other sanction regimes – including the withdrawal of several of Russia's richest people from Russian citizenship after February 2022 under unprecedented sanctions pressure – suggest that economic sanctions per se have such a potential. However, the introduction of cyber-related sanctions in 2018 did not have such an effect, which leads to the assumption that the degree of establishment

[229] Alexandr Pyatin, '"For Me, This Is a Total Crisis": Vekselberg Told How His Life Changed due to US Sanctions', *Forbes*, 3 June 2019, https://www.forbes.ru/milliardery/377121-dlya-menya-eto-totalnyy-krizis-vekselberg-rasskazal-kak-ego-zhizn-izmenilas-iz-za?photo=1 (in Russian).

[230] *Deripaska v Mnuchin and Others*, US District Court (District of Columbia), Case 1:19-cv-00727, https://www.courtlistener.com/recap/gov.uscourts.dcd.205241/gov.uscourts.dcd.205241.1.0.pdf.

[231] William Kaempfer and Anton D Lowenberg, 'Using Threshold Models to Explain International Relations' (1992) 73 *Public Choice* 419.

[232] William Kaempfer and Anton D Lowenberg, 'The Political Economy of Economic Sanctions' (2007) 2 *Handbook of Defense Economics* 886, n 32.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

of the link between the weakening financial position of Russian oligarchs and the potential limits of alleged Russian malicious cyber activities is insufficient.

4.3. Francesco Giumelli's four-step analysis

The four-step process of evaluating the impact of sanctions designed by Francesco Giumelli[233] represents a comprehensive analytical framework suitable for the assessment of cyber-related sanctions.[234] Understanding the logic of sanctions is at the heart of Giumelli's approach. Considering the potential goals of sanction implementation (coercion, constraint and signalling, as discussed above), assessing their 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 context of the sender's overall foreign policy.[235] As sanctions are implemented alongside other political tools, the objective 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, in conjunction with 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';[236] ten personnel were expelled from the Russian diplomatic mission in Washington following the adoption of Executive Order 14024 in April 2021.[237] Indictments of Korean hackers claimed to be involved in the attack against Sony Pictures not only indicated the willingness of US authorities to prosecute those individuals criminally, but also revealed that North Korean citizens and intelligence groups have become subjects of long-standing and timely FBI forensic analysis.[238] When sanctions are considered in the overall context of the sender's reaction to cyber-enabled actions, it creates obstacles

[233] Francesco Giumelli, *The Success of Sanctions: Lessons Learned from the EU Experience* (Routledge 2013).

[234] Giumelli's methodological approach has been employed in a series of recent studies on the effectiveness of sanctions; see Lee Jones, *Societies under Siege: Exploring How International Economic Sanctions (Do Not) Work* (Oxford University Press 2015); Viljar Veebel and Raul Markus, 'Lessons from the EU-Russia Sanctions 2014-2015' (2015) 8 *Baltic Journal of Law & Politics* 165. An instructive report prepared in 2015 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': Dreyer and Luengo-Cabrera (n 199) 12.

[235] Giumelli (n 233) 7.

[236] 'US Expels Russian Diplomats over Cyber Attack Allegations', *BBC News*, 29 December 2016, https://www.bbc.com/news/world-us-canada-38463025.

[237] The White House (n 156).

[238] A criminal complaint of more than 170 pages against a North Korean citizen accused of conducting the attack against Sony Pictures is available at: https://www.justice.gov/opa/press-release/file/1092091/download.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

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 draw out the logic of sanctions.[239] Two indicators of *ex ante* analysis are taken into consideration: (i) the expected direct impact of the sanctions, and (ii) the feasibility of demands. If the sender's goal is to impose material costs on the target (for instance, to make any line of behaviour that differs from the line required by the sender too costly for the target), then coercive and constraining sanctions would be more efficient than those of a signalling nature. Otherwise, if the sender does not expect to have a material impact on the sender, signalling sanctions are the preferable choice. Travel bans – one of the two most common restrictive cyber-related measures in the US, the EU and the UK regimes – do not entail any significant material costs on the targets. Asset freezes might have material impact if the sanctioned persons actually possess assets or economic resources within the jurisdiction of the sender (which is presumably not the case with most cyber-related sanctions applied to date, except for the sanctions against Russian oligarchs). Constraining business operations between the sanctioned persons and US residents might entail either direct costs for the targets (for example, when they had effective commercial contracts at the time of sanction imposition) or indirect costs (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 sanctions: 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'.[240] When sanctions are imposed in the logic of constraining, the targets generally do not have this freedom of choice: they have to change their behaviour as prescribed by the sender. In the case of 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 of a signalling and stigmatising nature rather than coercive or constraining.

The third step of the analysis is an *ex post* estimation of the sanctions' impact and effects,[241] the assessment of their factual consequences – intended or not. This evaluation often includes a cost-benefit analysis, but should not be limited to this. Although sanctions can have a calculable material impact, the assessment of their effectiveness should also include an analysis of effects other than economic costs, the first of which are the political consequences of sanctions. Thus, President Trump, who openly opposed the adoption of CAATSA, argued that the US Congress was making a mistake in introducing new sanctions against Russia. 'Our relationship with Russia is at an all-time

[239] Giumelli (n 233) 7.
[240] ibid 8.
[241] ibid.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

& very dangerous low', he wrote on Twitter.[242] The authoritative Carnegie Endowment for International Peace estimates US-Russian relations to be 'at the lowest point since the Cold War' with no 'signs that the relationship will improve in the near future'.[243] The US sanctions policy, in particular the episode related to Russia's alleged meddling in the 2016 presidential elections, has undoubtedly contributed to the 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.[244] 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'.[245] The imposition of cyber-related sanctions can be associated with certain costs for the sender (both in a strictly economic sense, meaning losses incurred by the sender, and in a political sense, that is the weakening of power positions and/or an increase in 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 US National Security Advisor Robert O'Brien, the US has imposed so many sanctions against Russia and Iran that it has little opportunity left to impose new sanctions, and must look at other possible deterrents.[246]

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 behaviour can be among the sender's objectives, it is not the only one. An estimation of the impact of sanctions 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.

5. Concluding remarks: Prospects for cyber-related sanctions

Starting with the application of a positivistic legal approach to the question of why states make use of the tool of targeted, or smart, sanctions in response to the threat of malicious cyber operations, we have demonstrated that states are being pushed to resort to self-help, and sanctions represent one of its forms. States are pushed to its application by the conundrum of problems surrounding the legal basis for the qualification of the initial malicious cyber operation

[242] @DonaldTrump, Twitter, 3 August 2017, https://twitter.com/realDonaldTrump/status/893083735633129472 (last visited 10 August 2020).

[243] Richard Sokolsky and Eugene Rumer, 'U.S.-Russian Relations in 2030', Carnegie Endowment for International Peace, 15 June 2020, https://carnegieendowment.org/2020/06/15/u.s.-russian-relations-in-2030-pub-82056.

[244] Giumelli (n 233) 10.

[245] ibid.

[246] 'Few New Sanctions Left to Impose on Iran, Russia: Robert O'Brien', *Tehran Times*, 26 October 2020, https://www.tehrantimes.com/news/453901/Few-new-sanctions-left-to-impose-on-Iran-Russia-Robert-O-Brien.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

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 – as in the cases of the US, the EU and the UK – provides the possibility to extend the scope of cyber activities for almost all types of cyber act 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 themselves breach the international legal obligations of the sending states, they may be legal only if they either meet all criteria set forth for counter measures or fall within one of the defences provided by the law of international responsibility. 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 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 by-product, raise the inevitable question of the permissibility of cyber sanctions (sanctions consisting of the use of cyber means), and this could motivate states to strive for normativity in cyberspace.[247]

The use of extralegal analytical tools in the assessment of the efficiency of cyber-related sanctions has revealed their limited capacity to coerce targets to modify their behaviour or to constrain them by reducing their potential to conduct new operations. Though the use of cyber-related sanctions has not led to any visible changes in the number and intensity of malicious cyber acts, these restrictive measures are efficient in fulfilling the purpose of signalling to the alleged organiser of the cyber operation and third parties of the sender's intended course of action, as well as stigmatisation.

[247] 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; see Ellen Nakashima, 'U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms', *The Washington Post*, 27 February 2019, 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. A few months later, June 2019, a new US cyber operation was articulated and reported to consist of the deployment of hacking tools at Russian grid systems; see David E Sanger and Nicole Perlroth, 'U.S. Escalates Online Attacks on Russia's Power Grid', *The New York Times*, 15 June 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

https://doi.org/10.1017/S0021223722000255 Published online by Cambridge University Press

To achieve these aims, states should take into consideration a number of general and cyber-specific factors. Among them, first of all, is the risk that economically designed sanctions may inflict economic costs on many states (and not only on the sender and target states). Secondly, empirical studies on 'general' (rather than cyber-related) economic sanctions reveal that they lose much of their effectiveness after the first and second year, which accounts for 55 per cent of successful sanction episodes,[248] as a result of adjustment by the target to the restrictions caused by the 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-caused damage is relevant for cyber-related sanctions. Thirdly, the effectiveness of sanctions is contingent on their credibility and consistency; this stresses the impact of due procedure, the sufficiency of evidence, legal certainty and the predictability of imposing sanctions, which is a crucial psychological factor.[249] Fourthly, the impact of cyber-related sanctions should be measured in conjunction with other tools, which include various acts of reaction in the realm of diplomacy, the initiation of criminal cases against individual perpetrators, and political statements. The overall context of the sender's foreign policy and the stance of third-party states are also to be taken into consideration.

Funding statement. The article was prepared within the framework of the Academic Fund Program at the National Research University Higher School of Economics (HSE University), Moscow (Russia) in 2020 (Grant No 20-04-020) and within the framework of the Russian Academic Excellence Project '5-100'.

Competing interests. The authors declare none.

[248] Sajjad Faraji Dizaji and Peter AG van Bergeijk, 'Potential Early Phase Success and Ultimate Failure of Economic Sanctions: A VAR Approach with an Application to Iran' (2013) 50 *Journal of Peace Research* 721.

[249] See Council of the EU, 'EU Best Practices for the Effective Implementation of Restrictive Measures', 8519/18, updated 4 May 2018, https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf; 'Guidelines on Implementation and Evaluation of Restrictive Measures in the Framework of the EU CFSP – update', 5664/18, 4 May 2018, https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf; Jon Hovi, Robert Huseby and Detlef F Sprinz, 'When Do (Imposed) Economic Sanctions Work?' (2005) 57 *World Politics* 479; Francesco Giumelli, 'The Effectiveness of EU Sanctions: An Analysis of Iran, Belarus, Syria and Myanmar (Burma)' (2013), EPC Issue Paper No 76, 20.

Cite this article: Vera Rusinova and Ekaterina Martynova, 'Fighting Cyber Attacks with Sanctions: Digital Threats, Economic Responses' (2024) 57 *Israel Law Review* 135–174, https://doi.org/10.1017/S0021223722000255